2004-03

Monitoring the progress of the Navy Marine Corps Intranet (NMCI) implementation, performance and impact

Dalaklis, Dimitrios

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MONITORING THE PROGRESS OF THE NAVY MARINE CORPS INTRANET (NMCI): IMPLEMENTATION, PERFORMANCE AND IMPACT

by

Dimitrios Dalaklis

March 2004

Thesis Advisor:	Glenn R. Cook
Second Reader:	Dorothy E. Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY	**2. REPORT DATE** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Monitoring the Progress of the Navy Marine Corps Intranet (NMCI): Implementation, Performance and Impact			**5. FUNDING NUMBERS**
6. AUTHOR Dimitrios Dalaklis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Information Superiority is the driver for the creation of the Global Information Grid (GIG) as the mean to provide connectivity between all parts of shore establishments, and with all deployed forces at sea and ashore. The **Navy Marine Corps Intranet (NMCI)** is an information technology (IT) services contract to provide to provide secure universal access to integrated voice, video and data communications; eliminate interoperability problems and remove network impediments to improve productivity and speed of command to the shore-based components of the Navy and Marine Corps.

The NMCI contract is the procurement of IT services based on a commercial model of Service Level Agreements (SLAs). Under this model, the emphasis is placed on the verification, validation, and monitoring of the end-user services and not on the underlying infrastructure of systems.

The research explores the current implementing effort of NMCI and analyzes the way this common network capability is tested and monitored. This thesis will provide a single source of information for managers seeking to quickly understand the impact of NMCI as an enterprise level asset. Security policies related to the project are examined and recommendations to improve this new IT initiative are made.

14. SUBJECT TERMS Navy Marine Corps Intranet, NMCI, Information Assurance, FORCEnet, IT services			**15. NUMBER OF PAGES** 208
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MONITORING THE PROGRESS OF THE NAVY MARINE CORPS INTRANET (NMCI): IMPLEMEMENTATION, PERFORMANCE AND IMPACT

Dimitrios Dalaklis
Lieutenant, Hellenic Navy
B.S., Hellenic Naval Academy, 1992

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGENT

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author: Dimitrios Dalaklis

Approved by: Glenn R. Cook
Thesis Advisor

Dorothy E. Denning
Associate Advisor

Dan Boger
Chairman, Department of Information Science

Gordon McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information Superiority Information Superiority is the driver for the creation of the Global Information Grid (GIG) as the mean to provide connectivity between all parts of shore establishments, and with all deployed forces at sea and ashore. The **Navy Marine Corps Intranet (NMCI)** is an information technology (IT) services contract to provide to provide secure universal access to integrated voice, video and data communications; eliminate interoperability problems and remove network impediments to improve productivity and speed of command to the shore-based components of the Navy and Marine Corps.

The NMCI contract is the procurement of IT services based on a commercial model of Service Level Agreements (SLAs). Under this model, the emphasis is placed on the verification, validation, and monitoring of the end-user services and not on the underlying infrastructure of systems.

The research explores the current implementing effort of NMCI and analyzes the way this common network capability is tested and monitored. This thesis will provide a single source of information for managers seeking to quickly understand the impact of NMCI as an enterprise level asset. Security policies related to the project are examined and recommendations to improve this new IT initiative are made.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Network-centric warfare (NCW) established the idea that networks are becoming increasingly necessary and important to the modern military. Information Superiority is the focus of the transformational concepts outlined in Department of Defense Joint Vision 2020 and is the driver for the creation of the Global Information Grid (GIG). In order to provide the operational environment necessary to promote information superiority, there needs to be connectivity between all parts of shore establishments, and with all deployed forces at sea and ashore.

The **Navy Marine Corps Intranet (NMCI)** is an information technology (IT) services contract to provide reliable, secure, and seamless information services to the shore-based components of the Navy and Marine Corps. The NMCI is a critical component of the Department of the Navy (DoN) vision of a network-centric force, where a single secure, integrated network delivers all voice, video, and data IT services to more than 360,000 seats in more than 300 locations. Through the standardization of hardware and software suites, and employment of common, multi-layered security architecture, the NMCI will greatly improve interoperability and security across the DoN "Enterprise".

The purpose of the analysis that follows was to thoroughly examine the mechanisms involved with monitoring the implementation effort of NMCI, to include testing, and evaluate the Intranet's performance and impact in relation to the end user. A brief introduction of the concepts related to the contract along with snapshots to the implementation numbers were provided in order to demonstrate that the implementation effort still remain behind schedule, no mater of continuously adjusting the associated timeframe. On the other hand, NMCI is the foundation that will enable DoN-wide web-based processes, knowledge management and e-business solutions, making the decision to go ahead with this IT initiative an obvious one. With NMCI and by adapting to the new approach of "IT as a utility", apart from dealing with the "bandwidth-starvation" problem, greater efficiency and effectiveness in all facets of naval operations will be gained.

The research examined the current roughly 200 different criteria and measurements as described by the **Contract Line Item Number (CLINs) and SLAs** used by DoN to monitor the success of the common network capability for the whole Department and concluded that even without DoN's prior experiences of that type of IT acquisition activity, the methodology to describe and frame the NMCI was the result of a sound approach towards a Service-Level Agreement (SLA) contract based on practices already established and followed by the private sector businesses, while enforcing automated tools to monitor the related metrics facilitates objective establishment of the exact services levels.

The NMCI contract is relying on the concept of SLA to ensure mutual government and provider understanding of the services to be provided and to ensure that stakeholders' and users' expectations are satisfactorily defined and executed. However, continuous assessment and adjustment of the SLAs are necessary in this type of contracting environment. The main conclusion is that the DoN and EDS after the completion of the "Operational Evaluation" phase should establish the SLAs at a level that the NMCI project delivers value for both parties and the DoN should continue to receive IT support as an "utility" and take advantage of the outsource idea in order to focus more on its core missions while exploiting IT as a force multiplier.

I. INTRODUCTION

A. THE "GRAND STRATEGY" ENVIROMENT

1. Department of Defense (DoD) Strategic Visions and the Implementation of the Joint Task Force (JTF) Concept

DoD must develop the ability to integrate combat organizations with forces capable of responding rapidly to events that occur with little or no warning. These joint forces must be scalable and task-organized into modular units to allow the combatant commanders to draw on the appropriate forces to deter or defeat an adversary. The forces must be highly networked with joint command and control, and must be better able to integrate into combined operations than the forces of today.

(Abstract from the Quadrennial Defense Review September 2001, included in the *Year 2003 Secretary's of Defense Annual Report for the President and the Congress*, p. 42)

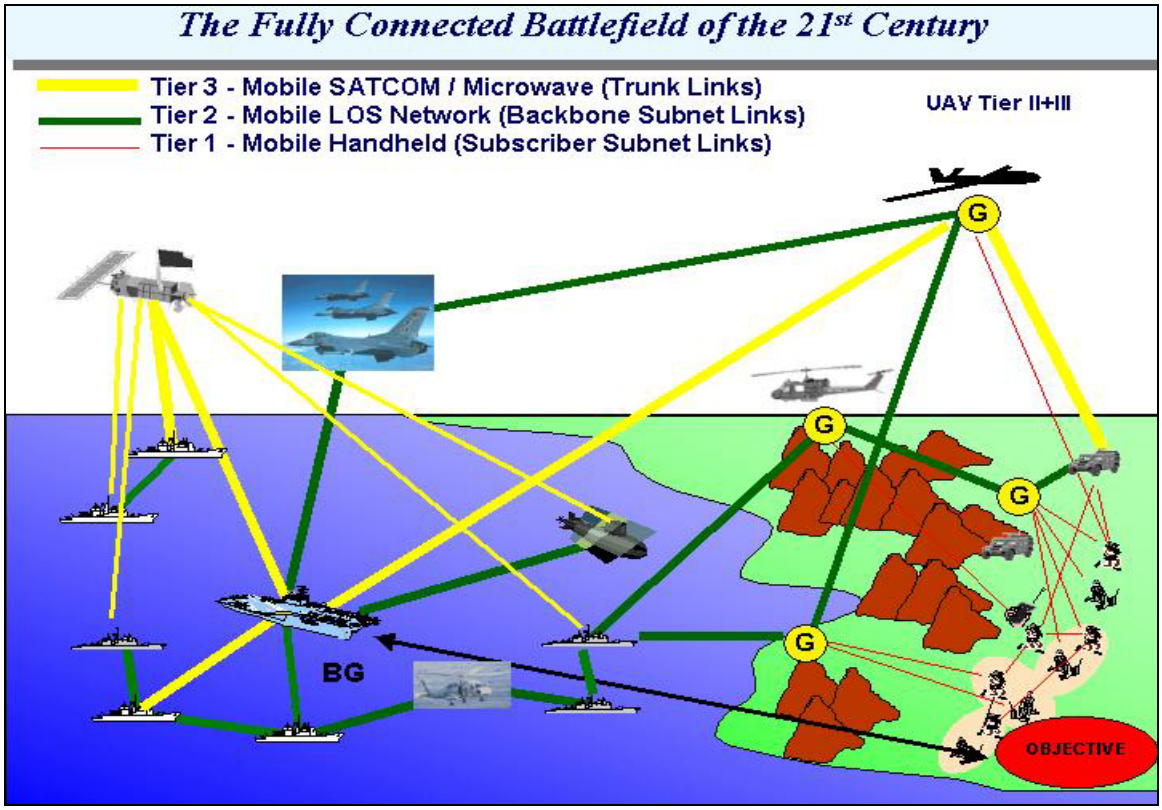


Figure 1: Joint Task Force (JTF) Operating Under the Concept of Networking

Transformation can be defined as the process of changing form, nature or function. Fashioning joint operating concepts to guide the conduct of joint operations and

promote interagency cooperation are DoD leading priorities for transformation. For the United States (U.S.) developing the kind of forces and capabilities that can adapt quickly to new challenges and unexpected circumstances requires changing the form or structure of the military forces and the nature of the military culture and doctrine supporting those forces; and streamlining war-fighting functions to more effectively meet the complexities of any type of threat. The Joint Knowledge Development and Distribution Capability (JKDDC) initiative, for example, is intended to leverage state-of-the-art technology to access knowledge and share information—in the form of education, learning, training, and human expertise—using a networked, knowledge-based, joint architecture that is interoperable within the various military services. The main idea is:

> To provide dynamic, capabilities-based training for the Department of Defense in support of national security requirements across the full spectrum of service, joint, interagency, intergovernmental, and multinational operations
>
> Lt Col Lyndon S. Anderson, Director of Joint Management Office (JMO), Joint *Knowledge Development and Distribution Capability (JKDDC) Briefing*, in the Worldwide Joint Training Conference, USA, September 2003.

The JKDDC is intended to allow on-scene commanders, first responders, and others to seek real-time advice from subject-matter experts in the areas of language, culture, science, strategy, and planning at various sites across the globe. The objectives in mind are:

- Prepare forces for new war-fighting concepts
- Continuously improve joint force readiness
- Develop individuals and organizations that think and act joint
- Develop individuals and organizations that improvise and adapt to emerging crises
- Achieve unity of effort from a diversity of means

The focus of DoD now shifts into enabling joint operations -the ability of land, sea, air, and space forces to be combined under the control of a single combatant commander- and used in ways that are most appropriate to achieving the final objectives. Over the past years, the individual military departments have each proposed their individual models of how they would prefer to fight and DoD is now seeking to integrate

these perspectives into an overarching concept for the employment of the joint force. The importance of implementing the JTF concept is reflected in the priority list included in the 2003 Secretary of Defense Annual Report to the President and the Congress.

Figure 2: DOD's Priorities for the Year 2004, from the Year 2003 Secretary's of Defense Annual Report for the President and the Congress, p. 65)

2. Network-Centric Warfare (NCW)

Network Centric Warfare (NCW) has emerged as the key paradigm for achieving the distributed war-fighting goals outlined in Department of Defense (DoD) Joint Vision 2020 [Note 1] and is the driver for the creation of the **Global Information Grid (GIG)**. [Note2] Each of the military services under the DoD drafted "roadmaps" laying out their respective approaches to acquiring the kinds of capabilities described as leading the way toward a transformed force. The concept of NCW has become the central concept for organizing Department of the Navy (DoN) efforts to change and transform itself. The structural model for the Navy's NCW concept is a high-performance information grid that quickly assimilates and shares battlefield data among Naval Forces worldwide. NCW shifts the emphasis from platform-centered, attrition-style operations to a new methodology based on enhanced speed of command and dynamic, real-time reorganization of sensors and shooters to meet changing mission requirements. This new model of warfare introduces the change from relying solely on the individual platform towards networking units as the medium for the conduct of Naval Operations. (Vice Admiral. Arthur K. Cebrowski, U.S. Navy and John J. Garstka, article *"Network Centric Warfare: Its Origins and Future"* -Naval Institute Proceedings, 1997).

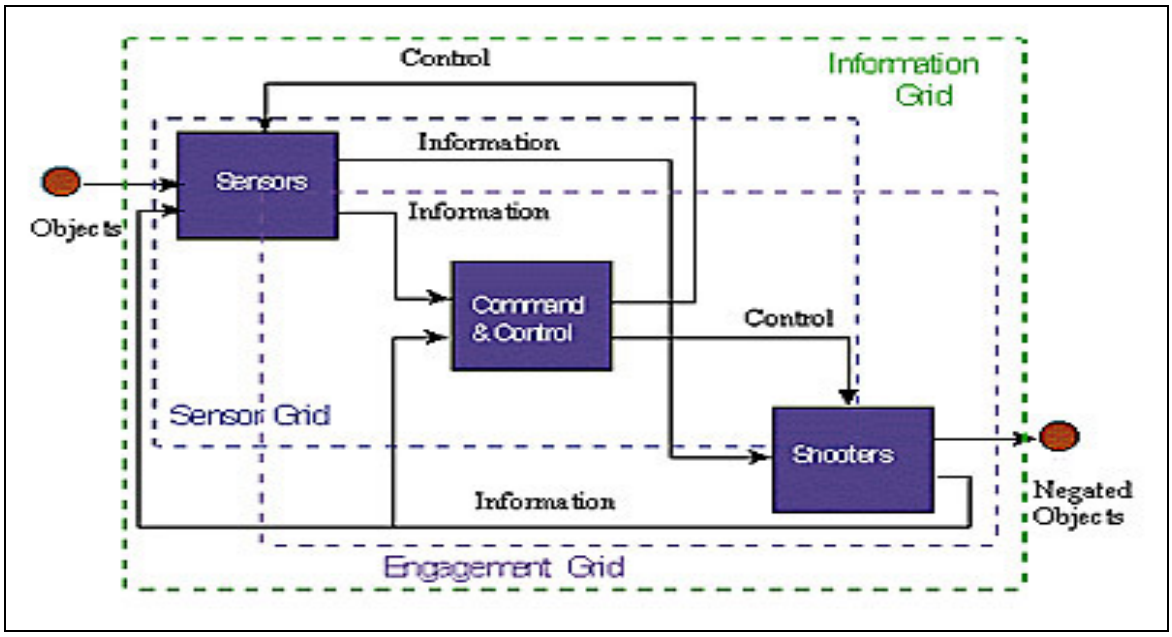


Figure 3: Logical Model for Network-Centric Warfare, from the Cebrowski and Garstka article *"Network Centric Warfare: Its Origins and Future"*

NCW focuses on using advanced information technology (IT) – computers, high-speed data links, and networking software – to link together ships, aircraft, and shore installations into highly integrated computer/telecommunications networks. At the structural level, network-centric warfare requires an operational architecture with three critical elements: sensor grids and transaction (or engagement) grids hosted by a high-quality information backplane. They are supported by value-adding command-and-control processes, many of which must be automated to get required speed. Rapid information collection, analysis, dissemination, decision-making, and execution are critical to achieve increased combat effectiveness. The information grid will provide the necessary backplane for computing and communications, by enabling the operational architectures of sensor grids and engagement grids. The sensor grid rapidly generates engagement quality awareness, and the engagement grid translates this awareness into increased combat power. NCW generates combat power by the fusion of networking sensors, decision-makers and shooters. There are two complementary ways that this is accomplished:

- Network-centric warfare allows participating forces to develop speed of command.

- Network-centric warfare enables forces to organize from the bottom up--or to self-synchronize--to meet the commander's intent.

Information superiority, obtained through NCW, creates combat power by fusing information producers with information consumers at the right time and place across the battlefield. The aim is to produce increased shared situational awareness and accelerated speed of command with a higher tempo of operations, resulting in greater lethal capability and increased survivability for the operational units.

3. The Visions of the Department of the Navy (DoN)

The speed, volume, and diversity of knowledge required to effectively operating within the framework of joint military forces is continuously accelerating. Projected future operating environments strongly emphasize the decisive advantage conferred by superior information management and knowledge dominance and both will probably be the key to operational success in the future. Near-instantaneous collection, analysis, and dissemination of information coupled to advanced computer-driven decision aids aim to unify the battle space of the 21st century.

> Our vision and our way ahead – Naval Power 21 and the Naval Transformation Roadmap – provide the framework to align, organize, and integrate our Naval Forces to meet the wide array of challenges that lie ahead. This will require accelerating operational concepts and technologies to improve war-fighting effectiveness and enhance homeland defense; shaping and educating our force to operate tomorrow's Fleet; sustaining readiness; and harvesting efficiencies to invest in the transformation of our Navy and Marine Corps.
>
> Secretary of the Navy, in his *2003 Annual report for the President and Congress*

The Navy's vision focuses on four fundamental qualities of Naval Forces – decisiveness, sustainability, responsiveness and agility. The Navy and Marine Corps have defined their respective Service strategies in **Sea Power 21 and Marine Corps Strategy 21**. Taken together, these visions begin to prescribe a strategy to concepts to capabilities technology continuum that will result in greatly enhanced power projection, protection and joint operational freedom. In so doing, they provide the framework for organizing, aligning, integrating and transforming the fully networked naval forces to meet the

challenges and risks that lie ahead. (Secretary of the Navy, *Year 2003 Secretary's of Defense Annual Report for the president and Congress*, p. 163)

Swift and effective use of information will be central to the success of **Sea Power 21**. Sea Strike will rely on rich situational awareness provided by persistent intelligence, surveillance, and reconnaissance to sense hostile capabilities and trigger rapid and precise attacks. Sea Shield will use integrated information from joint military, interagency, and coalition sources to identify and neutralize threats far from shores, locate and destroy any type of challenge in littoral waters, and intercept missiles deep over land. Sea Basing will draw on comprehensive data to sustain critical functions afloat, such as joint command and logistics, ensuring operational effectiveness and timely support. (Vice Admiral Richard W. Mayo and Vice Admiral John Nathman, U.S. Navy, article *"FORCEnet: Turning Information into Power"*- Naval Institute Proceedings, February 2003).

Figure 4: The Navy's Vision for the 21st Century, from RADM Mike Sharp, U.S. Navy, Vice Commander Space & Naval Warfare Systems Command Briefing, at the NMCI – Industry Symposium, 19 June 2003

The Navy is turning visions and plans into reality as it chooses which information and communications technologies will be integrated, which ones will be dropped, and which will serve as the foundation for its giant FORCEnet architectural framework.

FORCEnet is a massive, transformational undertaking that will integrate, align and enhance existing networks, sensors, commands, platforms, operations and weapons across the entire Navy. The goal of the project, which went through its first major field test in late September 2003, is faster, better decision-making for intelligent, interoperable, network-centric warfare. (Cheryl Gerber, (MIT Correspondent), article: *"Field Test Highlights FORCEnet Advances"*- Military Information Technology, November 2003)

4. FORCEnet within the JTF Concept

FORCEnet is the enabler of Sea Power 21, turning information into power. It has the aim to provide the advantage of information superiority and increase responsiveness and survivability of participants involved. Sharing information could enable knowledge-based operations, delivering greater power, protection, and operational independence than ever before possible to joint force commanders.

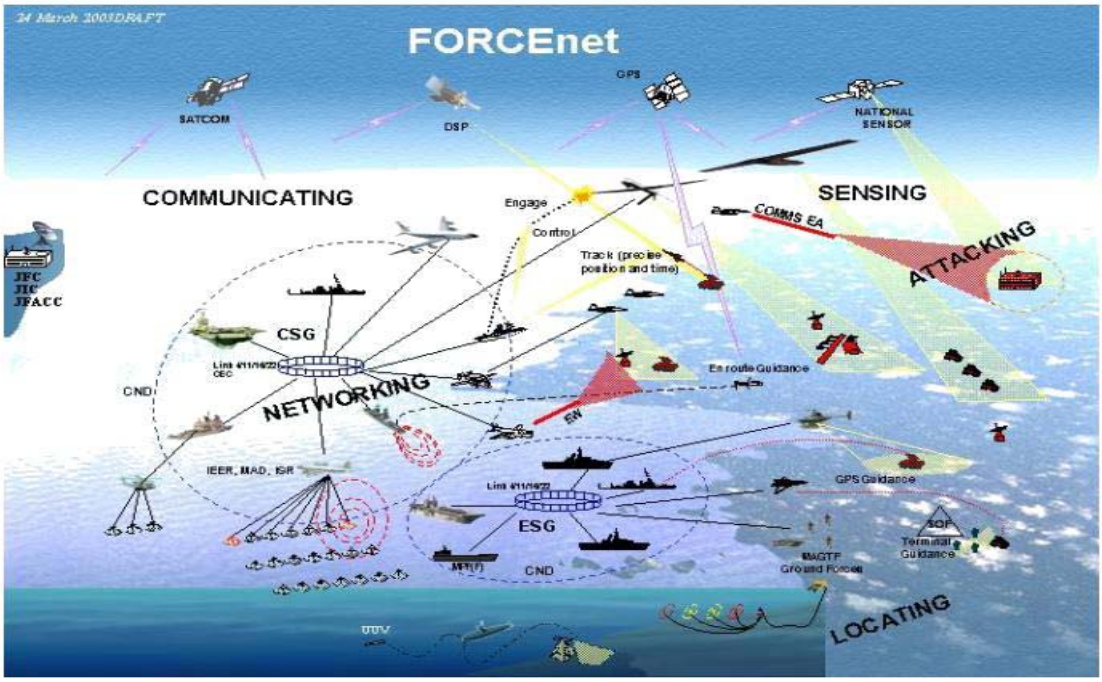


Figure 5: FORCEnet, the New Naval Operational Environment, from RADM Mike Sharp, USN Vice Commander Space & Naval Warfare Systems Command Briefing, at the NMCI – Industry Symposium, 19 June 2003

FORCEnet will be the operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is

scalable across all levels of conflict from seabed to space and sea to land. The goal of FORCEnet is to achieve superior knowledge for deployed forces, leading to increased combat power. A comprehensive network of sensors, analysis tools, and decision aids to support the full array of naval activities, from combat operations to logistics and personnel development will be created. The focused, timely, and accurate data delivered by this type of network will help decision-making at every level by allowing participants to draw on vast amounts of information and share the resultant understanding. This could increase the joint force's ability to synchronize activities throughout the battle space to achieve the greatest impact.

Developing this type of capability will involve designing and implementing a network architecture that includes standard joint protocols, common data packaging, seamless interoperability, and strengthened security. FORCEnet spans across Navy and United States Marines Corps (USMC) mission areas and is Joint from Inception – Naval unique implementations are only by exception. Some key Joint drivers towards the Global Information Grid include: the bandwidth expansion, the Transformational Communications Architecture and the Defense Information System Network [Note 3]. The overall technical architecture will consist of commercial standards with DoD standards imposed only as necessary to conform to unique military requirements.

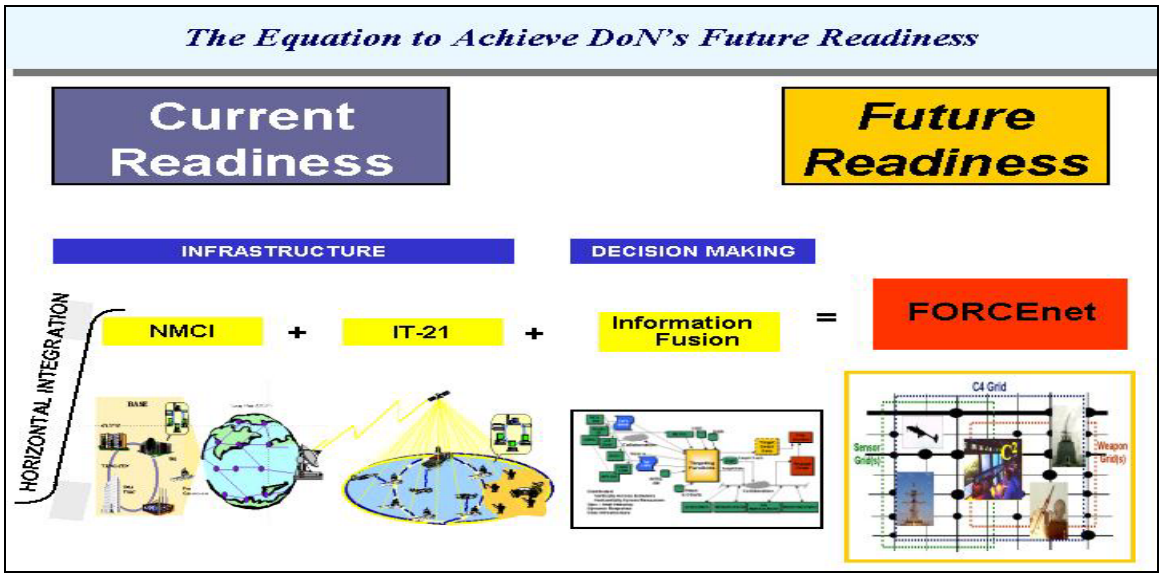


Figure 6: Integration of Systems, Information and Decision Tools towards FORCEnet, from RADM Mike Sharp, USN Vice Commander Space & Naval Warfare Systems Command Briefing, at the NMCI – Industry Symposium, 19 June 2003

Priority actions will include: Web-enabling the Navy; establishing open architecture systems and standards to allow rapid upgrades and integration; building common data bases to widely share information; implementing standard user interfaces to access information; and establishing portals that allow users to pull data from common servers. (Vice Admiral Richard W. Mayo, U.S. Navy and Vice Admiral John Nathman, U.S. Navy, article *"FORCEnet: Turning Information into Power"*, Naval Institute Proceedings, February 2003). As a direct result, a tremendous effort to integrate systems, information and services at the inter-service level is necessary and will require capability investments within and across joint, interagency and international programs.

5. How the Navy Will Achieve Information Superiority

Information superiority will be the key outcome of the transformational concepts outlined in Joint Vision 2020. Information superiority can be defined as providing our forces with the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. In a non-combat situation this means that our forces would have the necessary information to achieve their operational objectives. In order to provide the operational environment necessary to promote information superiority, there needs to be connectivity between all parts of shore establishments, and with all deployed forces at sea and ashore. This connectivity will enable an environment where all members can collaborate freely, share information, and organizational learning can be fostered. (NMCI Report to Congress, 30 June 2000, p. J-5-1)

DoN is building the infrastructure necessary to achieve information superiority and support knowledge superiority at the same time. The Web-enabled framework is designed to ensure mobile, seamless operations for the business and operational process users, and provide support tools for users to access the services and data from any location. Ashore, that infrastructure takes the form of the **Navy-Marine Corps Intranet (NMCI)** project that will ultimately connect all ashore Naval facilities and permit rapid, secure, information transfer, and universal Internet access. At sea, SPAWAR is installing IT-21 capabilities on most fleet units to bring the same capability while afloat. The combination of the two networks could provide universal access and information sharing across the entire department. As web access becomes more available, we will begin

moving to a "Web enabled Navy". The Web-enabled Navy (WEN) will be a web-service based layer riding on top of existing C4ISR architectures and infrastructures including the NMCI, IT-21, the Defense Information System Network (DISN), and commercial services. The combination of these elements begins to move the Navy rapidly toward the goal of knowledge superiority and integrated information—the right information, provided to the right person at the right time.

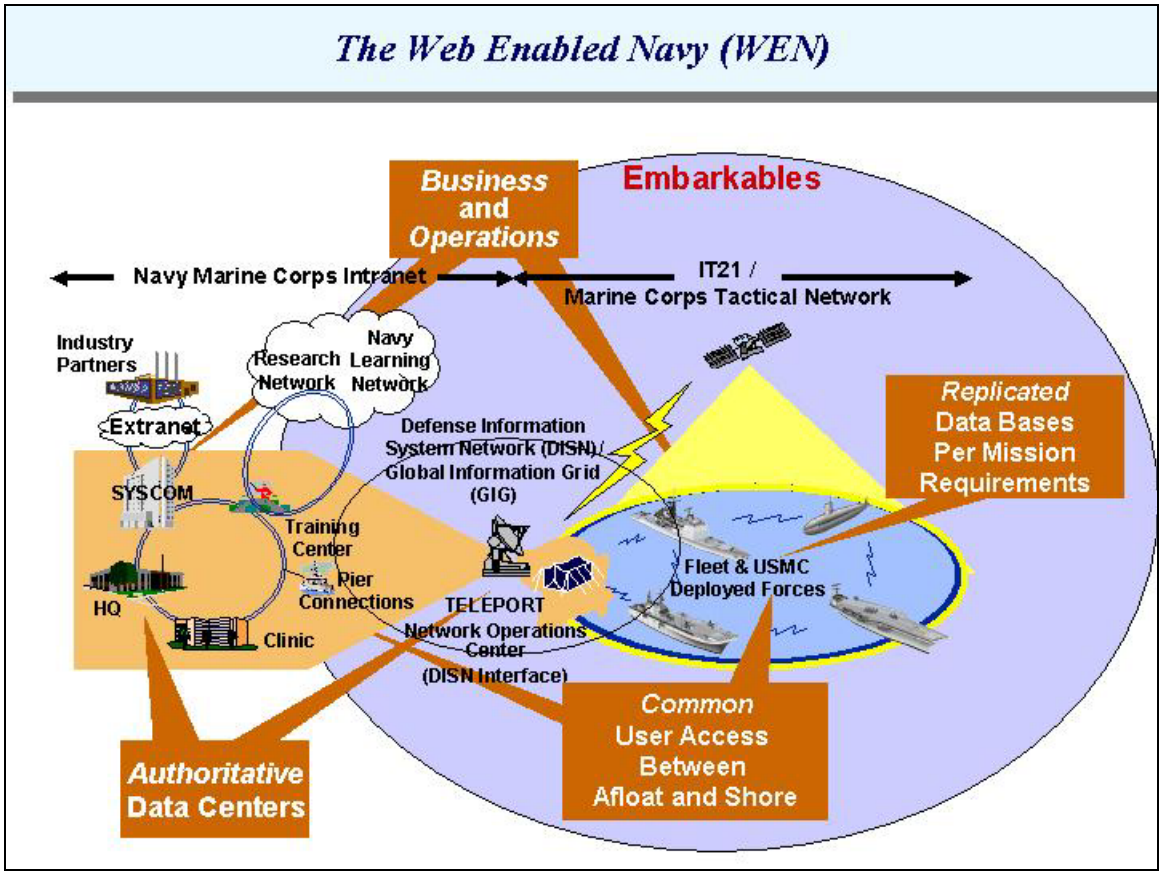


Figure 7: Web-enabled Navy, from RADM Mike Sharp USN Vice Commander Space & Naval Warfare Systems Command Briefing, at the NMCI – Industry Symposium 19 June 2003

Navy and Marine Corps personnel use IT to support DoN's core business, scientific, research, computational activities, and war fighting activities. The Navy's effort to implement the transformational efforts that are promoted by the DoD involves several simultaneous IT procurement efforts, as the necessary building blocks. (Ronald O'Rourke, Congressional Research Service Report: *Navy Network-Centric Warfare*

Concept: Key Programs and Issues for Congress, Order Code RS20557, June 6th of 2001, p. 2) For units afloat, the Cooperative Engagement Capability (CEC) program [Note 4] along with the IT-21 investment strategy [Note 5] are currently underway, while for Naval Installations ashore the **Navy-Marine Corps Intranet (NMCI)** is the concept used to make the full range of network-based information services available to Navy and Marines operators for day-to-day activities, along with war-fighting supportive tasks.

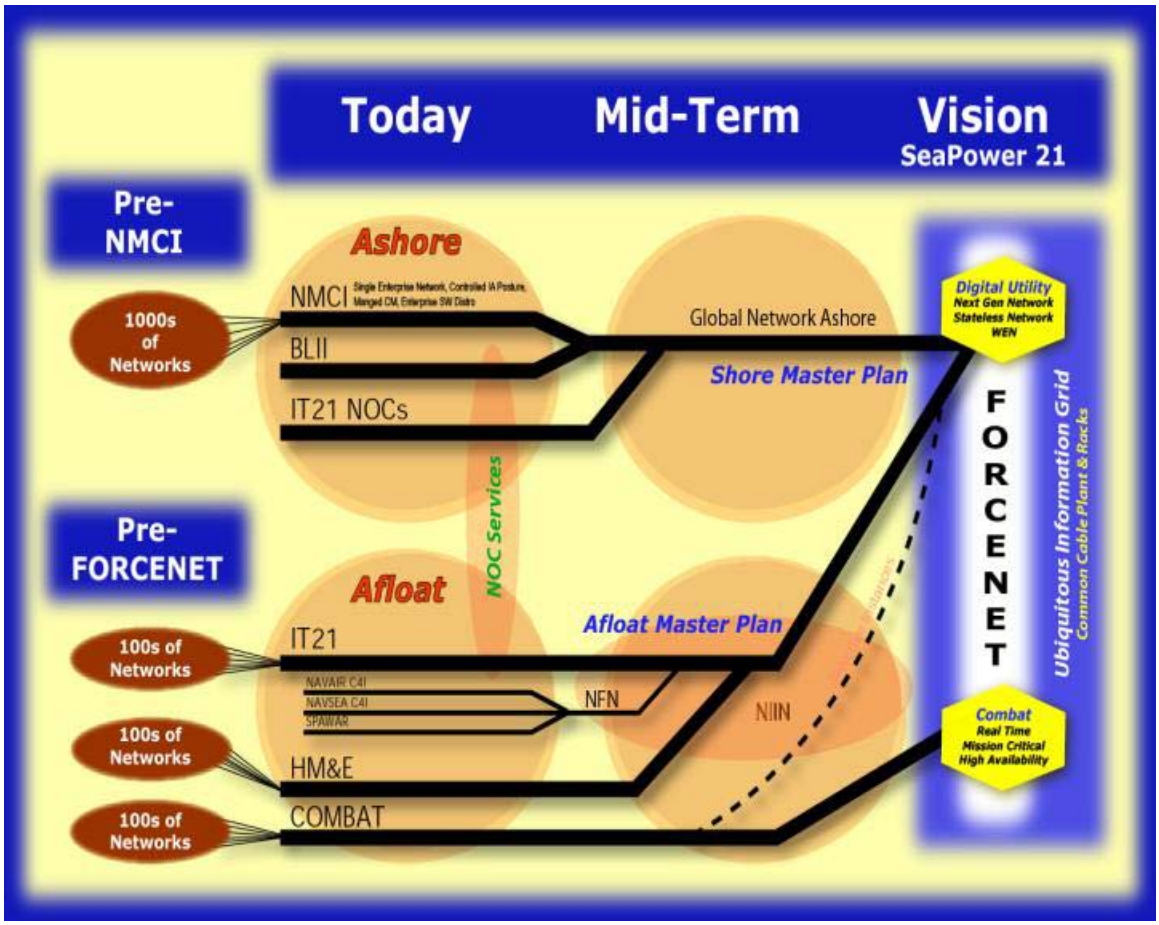


Figure 8: Elements of FORCEnet towards a Wide Enterprise Network (WEN), from RADM Mike Sharp, USN Vice Commander Space & Naval Warfare Systems Command Briefing, at the NMCI – Industry Symposium 19 June 2003

The Navy-Marine Corps Intranet is a corporate-style intranet that will link together Navy and Marine Corps shore installations in much the same way that the IT-21 effort will link together Navy ships. When completed, the NMCI will include a total of about 360,000 computer workstations, or "seats," at numerous Naval and Marine Corps installations. The NMCI service area includes the Continental United States (CONUS), as

well as Alaska, Hawaii, Guantanamo (Cuba), Puerto Rico, and Iceland for an estimated 360,000 Navy and Marine Corps Uniform and civilian workforce members (which includes 6,000 USMC reserve seats) in addition to 80,000 Navy Selected Reserve force members. Additionally, DoN has reserved the right to expand the NMCI service area outside the continental US (OCONUS) sites, beyond those listed above. (NMCI Contract N00024-00-D-6000**,** Conformed Contract P00080 10/6/2003, p. 1)

6. The Necessity of NMCI

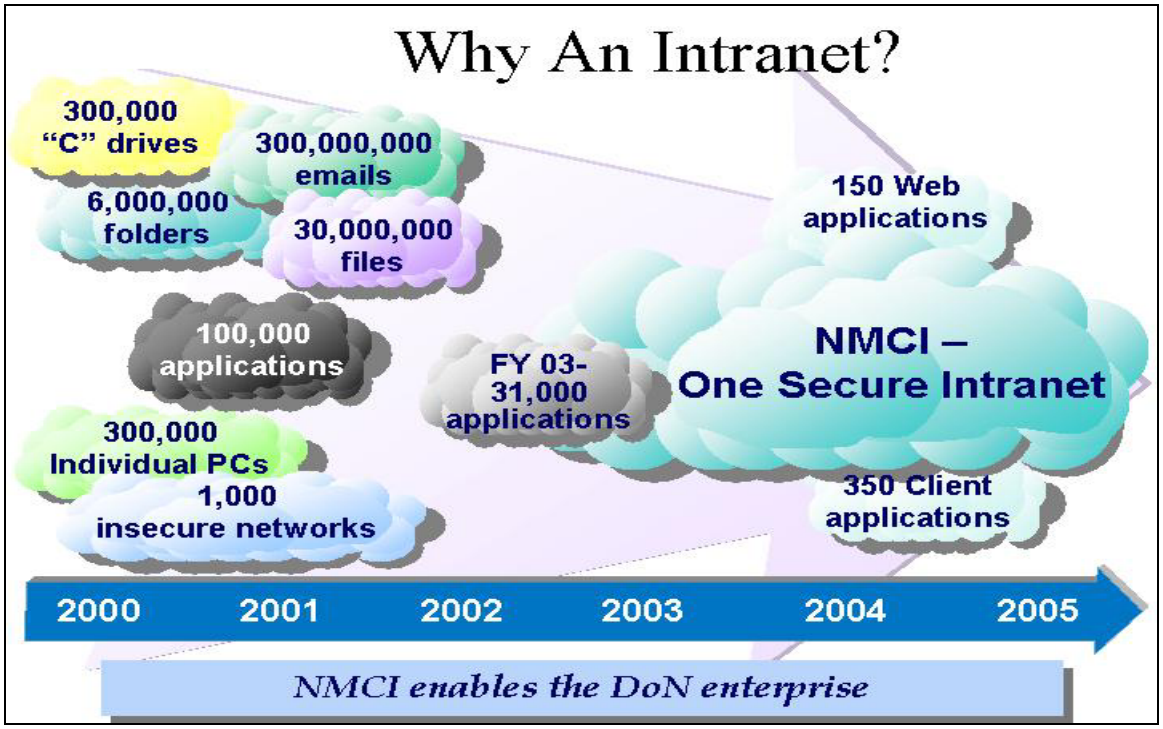


Figure 9: Why an Intranet, from Rear Admiral Chuck Munns, Director of NMCI, NMCI Progress Briefing, at the NMCI – Industry Symposium 17 June 2003

NMCI is a very important part of the tremendous integration effort currently underway and will contribute to the final creation of FORCEnet and the Global Information Grid (GIG) that are the capstone ideas under NCW. The purpose of NMCI is to provide the Navy and Marine Corps with secure universal access to integrated voice, video and data communications; eliminate interoperability problems; and remove network impediments to improve productivity and speed of command. The task of the NMCI contract seems simple enough: Bring the Navy and Marine Corps' disparate information technology ashore systems together under a single vendor to provide greater security and interoperability.

NMCI is the largest information technology contract ever awarded by the United States (U.S.) Federal Government, replacing hundreds of Navy and Marines Corps networks across the continental U.S. that were used before the NMCI introduction. The initiative is not only dealing with agencies ashore but it will provide pier-side connectivity for naval vessels in port, practically involving the total number of the Navy's workforce (military and civilians) in the NMCI implementation. The magnitude of the numbers indicated that the outsourced option was the best way to go. In a huge outsourcing effort, **Electronic Data Systems Corp. (EDS)** will take over the ownership and operation of the Navy and Marine Corps Information Technology (IT) hardware, software and other related services and will build and run a Navy and Marine Corp Intranet at a lower cost than what the DoN and Marine Corps were paying by purchasing and managing IT themselves. The contract coordinator, Texas based EDS, is a global leader in desktop and network management, currently overseeing more than 3.3 million desktops for government and commercial customers around the world. (www.eds.com (Facts about EDS) accessed February 2004)

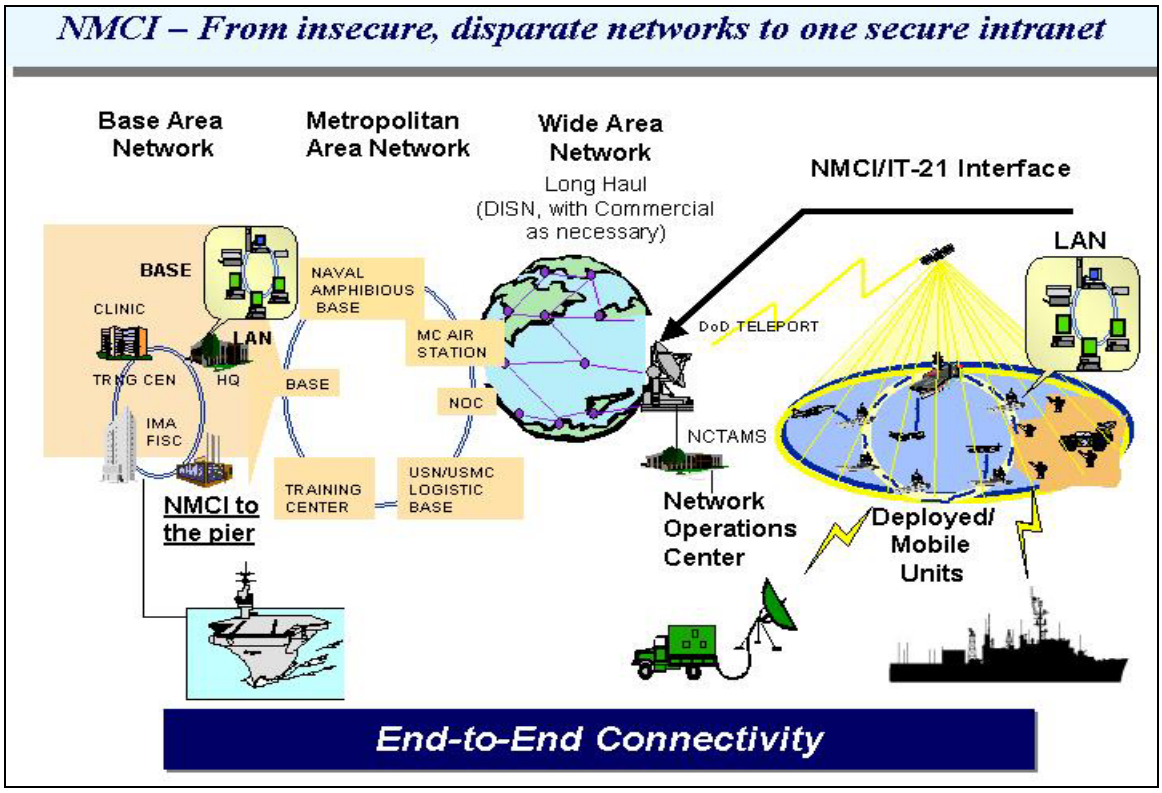


Figure 10: NMCI and Tactical Networks Interface, from the NMCI - Industry Symposium, 19 June 2003, *FORCEnet–Engineering& Architecting the Navy's IT Future*

The concept behind the NMCI transformation effort is to apply the speed and opportunities of Internet technology not only in the already under strong emphasis war-fighting tasks, but also in the very daily activities of naval personnel and especially those dealing with administrative and support tasks. Supporting the war-fighter are logistics, administration and other related operations or even training functions. These activities also rely heavily on IT to produce the right type of support. The goal of the NMCI contract is to eliminate stovepipe systems and modernize the way Navy does business. DoN will have network services as an enterprise level asset, with bandwidth on demand, making life better for every Marine, Sailor and DoN Civilian. The ultimate aim is to allow DoN operators to focus on their mission rather than be concerned with IT services and all the technical problems related with infrastructures and administration activities.

Moving NMCI from theory towards reality has proved a challenge, because the Navy's information technology (IT) infrastructure must be transformed from one in which products are purchased piecemeal (emphasis into buying commercial off the Shelves (COTS) products by various vendors, without a coordinated plan) into a utility similar to a telephone service (one single vendor, responsible for hardware, software and IT services at the same time). As a result of the importance of the NMCI initiative, there has been a plethora of information (positive and negative) published. Almost every government information technology industry trade magazine has published the good but also the bad and the ugly side of the DoN's attempts to initiate this change. The NMCI initiative differs from a traditional DoD acquisition program, where typically a system is purchased and the government assumes configuration control and life cycle maintenance responsibility. The NMCI contract is for the procurement of IT services (not systems) based on a commercial model of **Service Level Agreements (SLA)**. Under this model, the emphasis is placed on the verification, validation, and monitoring of the end-user services and not on the underlying infrastructure or systems.

B. PURPOSE AND BENNEFIT OF THE STUDY

1. Performance Measures Used

The Government Performance and Results Act of 1993 (GPRA) and the Information Technology Management Reform Act (ITMRA also known as Clinger-Cohen act) mandate the use of specific performance metrics for IT acquisitions. The

Clinger - Cohen Act requires the establishment of performance measures to assess how well NMCI supports mission accomplishment and for accountability and evaluation of investment post-deployment. Section 5123 of the ITMRA, Performance and Results-Based Management, requires that the head of an executive agency shall:

> Ensure that performance measurements are prescribed for information technology used by, or to be acquired for, the executive agency and that the performance measurements measure how well the information technology supports programs of the executive agency.
>
> (www.cit.nih.gov (Clinger-Cohen Act (CCA)) accessed February 2004)

The EDS-NMCI team provides services to a range of Navy and Marine Corps end points or as described in the contract, Service Delivery Points (SDP). These SDP include voice, video and data connection points for end users, the general NMCI enterprise, and interfaces to other DoN and DoD communications environments. The specific services to be provided to the end points vary but include the IT services listed in Table A, at Appendix A. When the NMCI contract was initially written, it laid out more than a hundred and thirty five (135) specific performance requirements in twenty (20) different categories. The Navy and EDS are continuously reviewing and adjust the SLAs that are the basis of measuring the performance of the NMCI.

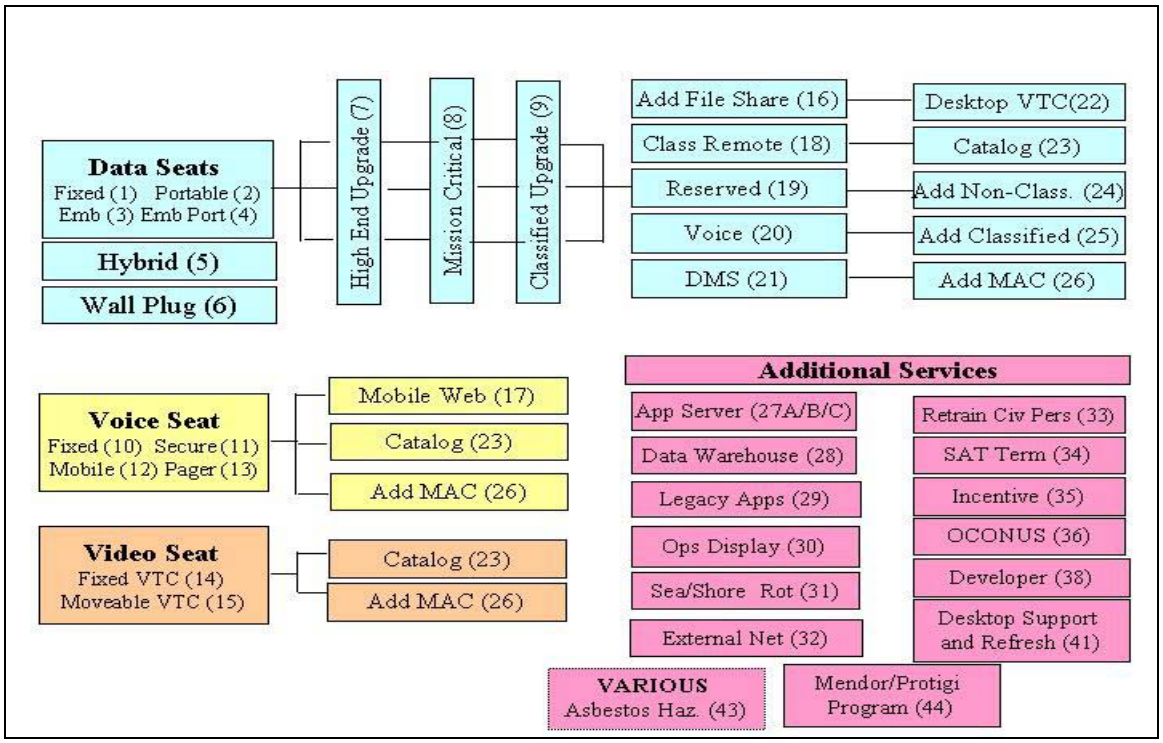


Figure 11: Summary of CLINs and the Related Domains, updated in February 2004

The purpose of the analysis that follows will be to briefly examine the mechanisms involved with monitoring the implementation effort of NMCI, as well as testing its performance, in relation to the end user. The research shall examine the current roughly 200 different criteria and measurements as described by the **Contract Line Item Number (CLINs) and SLAs** used by DoN to monitor the success of the common network capability for the whole Department and make recommendations regarding the tools and methods currently used to test and monitor the common network capability.

2. Concept of SLAs

The NMCI contract works by setting out performance levels that EDS must either meet or beat. The Navy will pay EDS bonuses if they exceed performance levels and penalize them for poor performance. DoN will receive all the connectivity, customer help services, repair services and so on as part of the basic seat price, while the NMCI vendor maintains configuration management and asset management and is expected to keep the customer well informed of changing service and technology refreshments. The NMCI contract is relying on the concept of SLA to ensure mutual government and provider understanding of the services to be provided and to ensure that stakeholder and user expectations are satisfactorily defined and executed.

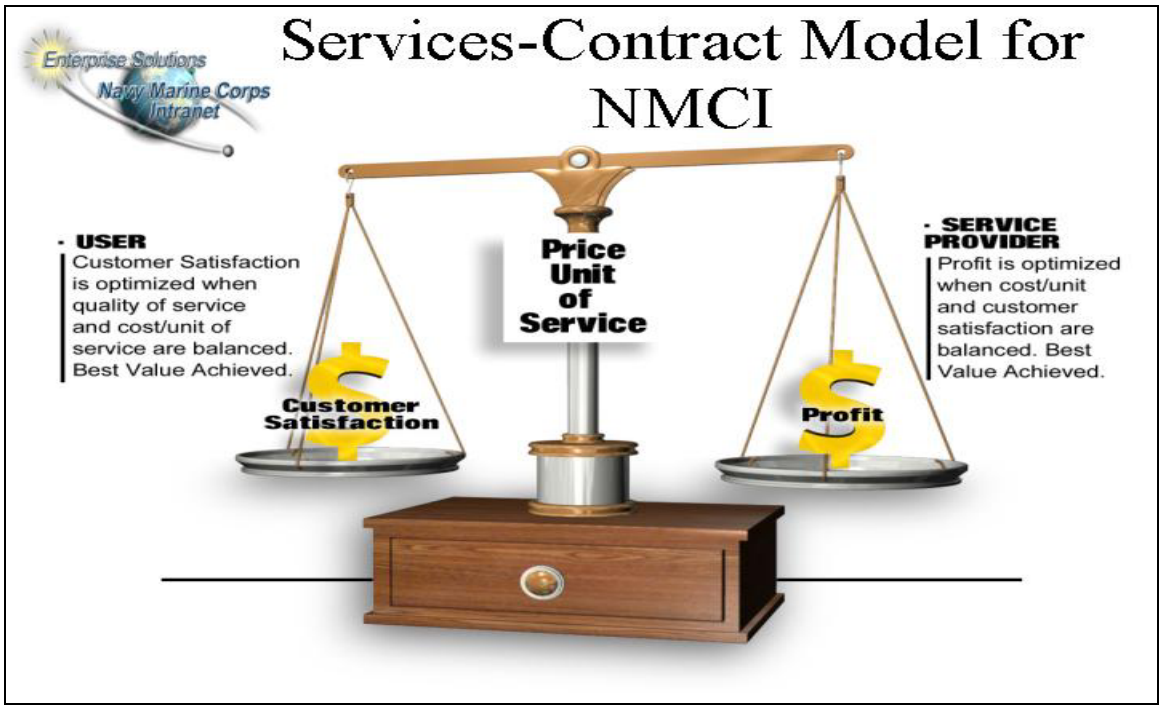


Figure 12: Contract Model of NMCI, from Captain Chris Christopher, U.S. Navy, NMCI Briefing for the Joint Logistics Council, USA, 29 March 2001

Traditionally, organizations list their IT requirements for procurement, in a statement of work that is included in the **request for proposals (RFP)**. SLAs expand this approach further by detailing the level of service and performance quality that the organization expects. For this process to work correctly, both the customer and vendor must agree up front about their expectations as well as the metrics by which quality will be measured. The idea is to ensure that the service levels are measuring things that actually matter and that the project is in line with the organization's mission. Legislation such as the Clinger-Cohen Act of 1996, which links funding with agency performance, has been one of the main drivers behind adopting this different approach.

SLA performance monitoring should be a continuous activity to evaluate and maintain the desired level of Help Desk support, customer satisfaction, system performance, and resources stability. While many of the services emphasize end-to-end performance, from a user perspective, a number of enterprise level services are viewed as mission critical and equally important to measure. Services covered by SLA fall into the following categories:

- User upgrades
- End user services
- Maintenance and Help Desk services
- Communications services
- Systems services
- Information assurance services
- Seashore rotation support
- Specific requirements

(Navy Marine Corps Intranet Site Deployment Guide Version 1.2, 07 March 2003, p. 41)

The thesis shall examine what is really important to this monitoring methodology and analyze whether a much smaller version of critical factors can be used more effectively or not. Potential impacts due to the magnitude of this "DoN wide level"

network will also be identified, especially in terms of Department of Defense (DoD) Information Assurance (IA) policies and procedures. The aim will be to identify any weak points related with interoperability and security across the DoN and make appropriate recommendations to be included in future changes of the SLA's.

C. RESEARCH QUESTIONS

This thesis shall explore the current effort of implementing the NMCI within DoN and analyze the way this common network capability is tested and monitored. A snapshot to the implementation numbers of NMCI will be given to conclude if the effort remains within track or not. Additionally, the thesis will examine briefly the security policies related with the NMCI project and offer recommendations for improvement if possible. The research will provide a single source of information for managers seeking to quickly understand the factors influencing the end user in embracing NMCI in terms of Information Assurance (IA).

1. Primary Research Question

Examining the way the NMCI implementation effort is progressing. What are the key factors and their impact on the effort and determine the current DoN capability to successfully monitor the performance measurements related with the NMCI.

2. Secondary Research Questions

A. Is DoN facing a problem by using 200 different criteria and why is it using this methodology?

B. What tools are currently available to aid in the monitoring process?

C. Brief examination of the NMCI's IA and security policies

a) Suggestion of possible solutions in order to improve security from INTERNAL threats.

D. SCOPE AND RESEARCH METHOD

The basic documents supporting this case study of the NMCI implementation effort will be the officially updated NMCI Contract N00024-00-D-6000, (Conformed Contract P00080), 10/6/2003, along with the Navy Marine Corps Intranet Site Deployment Guide Version 1.2, 3/07/2003. The Business Case Analysis (BCA) for

NMCI by Booz, Allen and Hamilton Inc. (Contract GS-23F-0755H) will be used extensively to justify the reasons necessary to migrate towards NMCI and describe the impact of the common network capability in DoN's mission. The Navy's official website related with NMCI (www.nmci.navy.mil) will also be use to provide details as necessary. Data collected through literary research of published articles and reports in information technology related journals and magazines will be used to deliver the weak or strong points of NMCI's implementation.

The research will be principally qualitative in nature as it seeks to answer the primary and subsidiary research questions. The purpose is to determine the current status of NMCI's implementation effort and deliver a list of critical factors to enable DoN in the determination of the **Quality of Services Level (QoS)** provided by the contractor. The thesis shall look at the general criteria currently in use and their applicability and will establish the general framework in order to deliver recommendations based on data collected through examination of Business Case Analysis (BCA) for the Navy Marine Corps Intranet, as well as the NMCI reports to the Congressional Committees.

E. ORGANIZATION OF THESIS

The methodology used in this thesis research will consist of the following:

1. Examine the NMCI contracting environment to include the methodology and techniques for testing and the monitoring criteria used by the contractor.

2. Conduct a literature search of applicable reports, journal and newspaper articles as well as other information sources to determine various issues associated with the NMCI implementation efforts and their impact.

   a. The time associated with the conduct of the research indicated that the early years of the contract up to the year 2003 should be examined in the background section of the thesis. Developments in the year 2003 and later are covered in the data collection section.

3. Determine the impact of NMCI on end users, in terms of IA.

4. Analyze the criteria used to evaluate NMCI's performance.

5. Make recommendations based upon research and analysis.

F. ENDNOTES

1. Joint Vision 2020, released May 30 2000 and signed by the chairman of the Joint Chiefs of Staff, Army Gen. Henry Shelton, extends the concepts laid out in Joint Vision 2010. "Full-spectrum dominance" is the key term in "Joint Vision 2020," the blueprint DoD will follow in the future. While full-spectrum dominance is the goal, the way to get there is to "invest in and develop new military capabilities." The four capabilities at the heart of full-spectrum dominance are: dominate maneuver, precision engagement, focused logistics and full-dimensional protection. (Jim Garamone (American Forces Press Service), article *"Joint Vision 2020 Emphasizes Full-spectrum Dominance"*, (**www.defenselink.mil (Joint Vision 2020),** accessed January 2004)

2. The DoD's building blocks of this information grid consist of more than 3 million individual computers on 12,000 local area networks (LANs). These interconnected classified and unclassified computers and LANs form the Global Information Grid (GIG), which supports combatant commanders, fixed installations and deployed forces around the world. The GIG supports every component of the DoD, including war-fighters, policymakers and business processes. (Major General J. David Bryan (Vice Director of Defense Information Systems Agency), article *"IA: Holistic View, Targeted Response"*, Military Information Technology, September 2003) The GIG relies on commercial technology to tackle information security challenges.

3. The Unclassified But Sensitive Internet Protocol Router Network, or "NIPRNet" and the Secret Internet Protocol Router Network, or "SIPRNet" comprises the Defense Information System Agency's Defense Information Systems Network (DISN). The essentiality of these networks has developed over time, and has been accelerated by the increasing dependence of the Department of Defense on the Internet as a common business process infrastructure. Taken together, these two data networks provide the essential information necessary to conduct and support the full range of military operations. Both the NIPRNet and the SIPRNet are Wide Area Networks (WAN), consisting of routers, modems, encryption devices and other ancillary equipment interconnected by high capacity data links and distributed throughout the world. In addition, these networks will continue to grow in importance to the Department of Defense as "Community of Interest" networks are developed and fielded. These Service-

specific networks will be using the NIPRNet and SIPRNet as the common data transport infrastructure. **The largest of these networks at the moment is the Navy and Marine Corps Intranet (NMCI).** (Major General David Bryan, Vice Director of the Defense Information Systems Agency and the Commander of the Joint Task Force Computer Network Operations, *Testimony to the Congressional subcommittee on the Department of Defense responsibility for the protection of its computer networks from cyber attack*, 17 May 2001)

4. The Cooperative Engagement Capability (CEC) system is intended to provide the capability for a warship to cooperatively engage targets by using data from other CEC-equipped ships, aircrafts and land target sensors, even in a jamming environment. The CEC system links U.S. Navy ships and aircraft operating in a particular area into a single, integrated air-defense network in which radar data collected by each platform is transmitted on a real-time basis to the other units in the network. The system works in conjunction with individual ship, aircraft and shore systems and it also provides a common, consistent highly accurate air picture, allowing for battle group defense as one integrated system, by networking assets together. (COTS Journal, Interview of [U.S.] Captain Dan Busch, *Cooperative Engagement Capability*, August 2001)

5. IT-21, which stands for IT for the 21st Century, is the Navy's investment strategy for procuring the desktop computers, data links, and networking software needed to establish an intranet for transmitting tactical and administrative data within and between Navy ships. The IT-21 network will be built around commercial, off-the-shelf (COTS) desktop computers and networking software. (Ronald O'Rourke, Congressional Research Service Report: *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress, Order Code RS20557*, 6 June 2001, p. 4)

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. OVERVIEW OF THE NMCI CONTRACT

1. Historical Data and Modifications of the Contract Until the Year 2003

NMCI is an IT initiative and procurement strategy to provide secure, seamless, global end-to-end connectivity for Naval war-fighting tasks and enhance business functionality. Ensuring that this intranet is interoperable within the **Global Information Grid** (GIG), it will interface with other joint forces' systems. Through the NMCI program, the United States Navy (USN) and United States Marine Corps (USMC) aim to procure IT services through a commercial seat management contract, with the intend to deliver comprehensive, end-to-end information services via a common computing and communications environment. The DoN conducted an informal analysis of alternatives in the spring of 1999 and determined that commercially contracted seat management represented the best option to efficiently satisfy current and future DoN IT support requirements. (Booz, Allen and Hamilton, *Business Case Analysis (BCA) for NMCI*, (Contract GS-23F-0755H), 6/30/2000, p. 1)

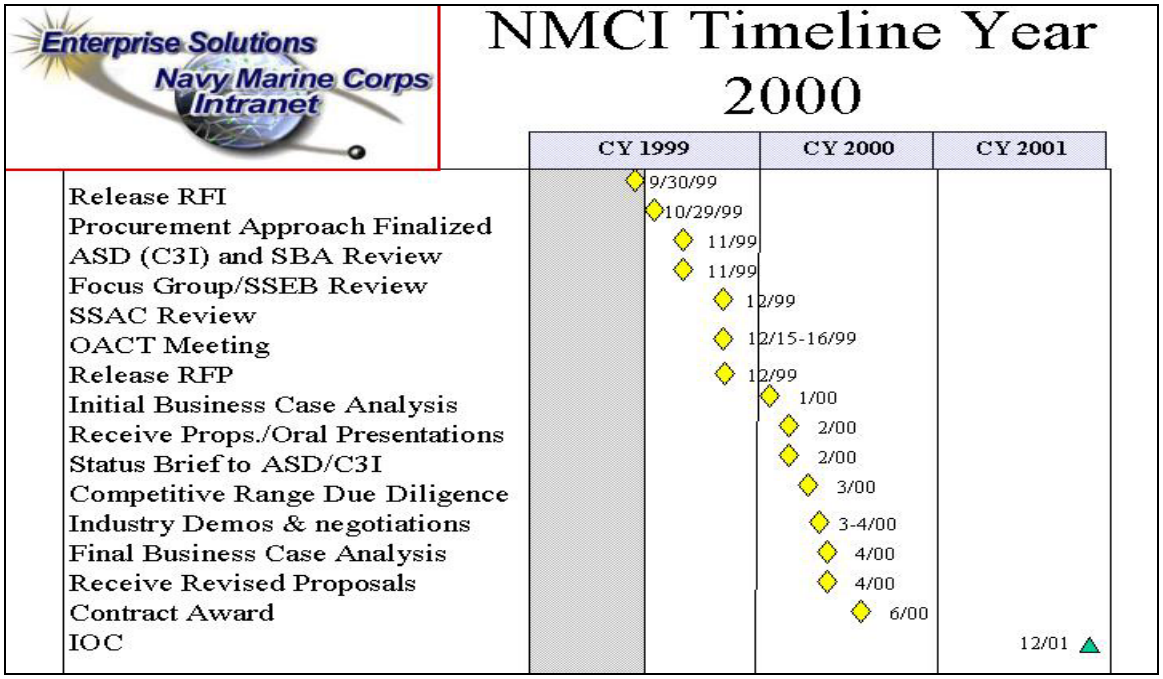


Figure 13: The Evolution of NMCI towards Reality, by Joseph Cipriano, PEO for IT, from his NMCI briefing at the Armed Forces Communications and Electronics Association, San Diego-USA, 16 February 2000

However, it is necessary to note that the initial estimates for implementation from the Navy and the views expressed by the potential contractors were quite optimistic. Taking into account the technical complexity, the magnitude of the effort and the fact that both parties were moving into "uncharted waters" with standards and specifications in a continuous flux, there were delays occurring during the negotiations even as early as the establishment of business proposals phase. The incremental realization of the technical obstacles necessary to overcome by every participant in the NMCI effort indicated that more time was needed. However, the significant importance of the need to create uniform standards and applications for the DoN enterprise pointed towards moving ahead no matter the adjustments necessary. Finally, the contract was awarded to Electronic Data Systems Corp. (EDS) on the 6th of October 2000, for a total of $6.9 billion and duration of five years plus three optional years at the Department of the Navy (DoN) discretion. The final bid was about $3 billion less than the three other bidders—Computer Sciences Corp., IBM Corp. and General Dynamics Corp. NMCI's transformation effort aims to bring together the vast majority of DoN personnel; military, government civilians and contractors into a single integrated IT environment.

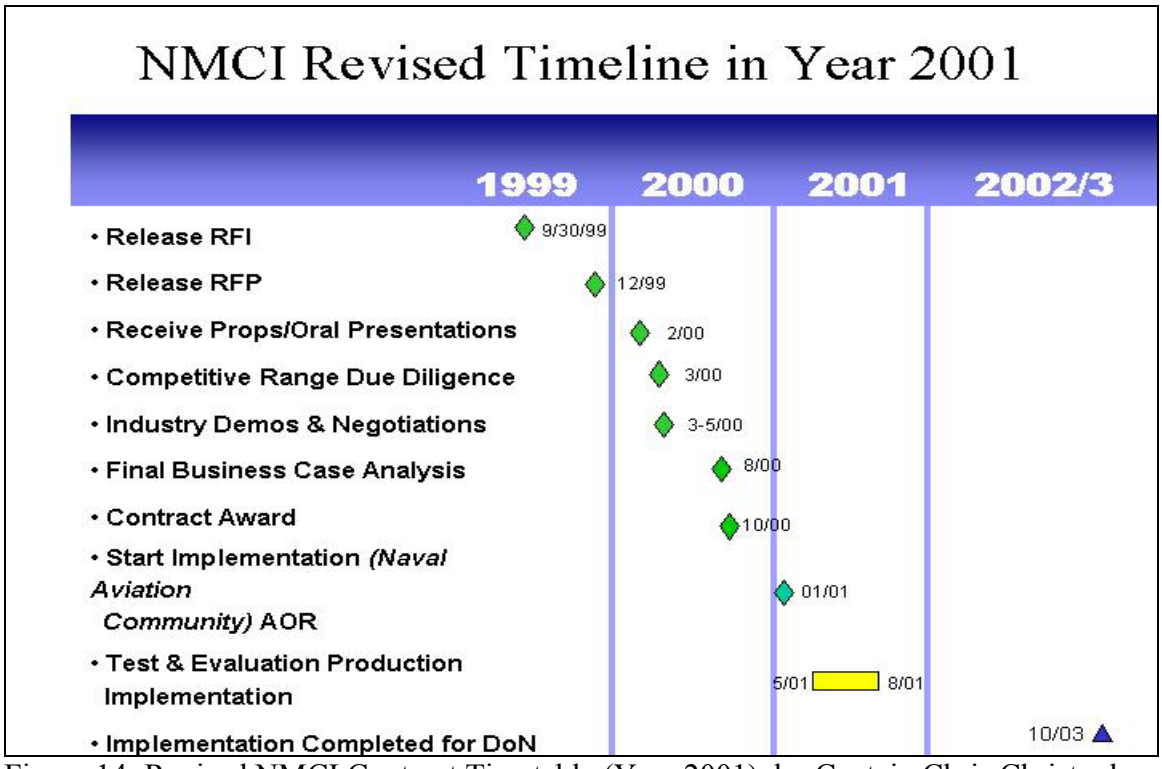


Figure 14: Revised NMCI Contract Timetable (Year 2001), by Captain Chris Christopher from his NMCI Briefing for the Joint Logistics Council, USA, 29 March 2001

This adjustment in the time-schedule involved with the NMCI implementation was only the first of the many to come. Much was at stake for EDS and the Navy in the NMCI program. For the Navy, NMCI offered the opportunity to fundamentally redesign and modernize its day-to-day operations by replacing an unplanned hodgepodge of standalone PCs and multiple local area networks that grew up over decades and do not communicate with each other. Additionally, as the largest federal information technology project ever attempted, the pressure on the project was intense: Many within the military and intelligence establishments were closely watching the effort because of President Bush's mandate to improve internal communications for homeland security. For EDS, the project represented a large chunk of business and also provides the company with a high-profile platform to demonstrate its capabilities to other military and civilian agencies contemplating similar seat management projects. Needless to say, the NMCI contract represented (and still is) the "Crown Jewel" in the extremely competitive IT services market.

Implementing NMCI globally across an organization as large as the Navy and Marine Corps requires cultural change, this, does not come without some degree of anxiety and after overcoming a variety of obstacles. Additionally, Congress has been skeptical about the cost benefit of the project ever since it was proposed. The Navy was originally set to announce the contract award in May 2000, but it was delayed for more than four months after Congress raised objections. The main concerns were the amount of money involved and institutional resistance towards change within the services. From the early steps of the NMCI implementation, the multi billion dollars project had turned into a major technology headache for the USN/USMC and EDS.

The project already was a year behind schedule, and many in Congress were concerned it would not stay within its authorized budget. Members of the Armed Services committees in the House of Representatives and the Senate began asking tough questions related with NMCI. They wanted to know in every detail how much money the Navy was already spending on desktop IT products and services, how it would pay for NMCI, what the project exact schedule would be, and how it would impact the Navy's civilian employees and small business partners. Disagreement between the Navy and the Pentagon about the level of testing required for NMCI delayed the project and raised

even more concerns within Congress. The Navy advocated commercial testing procedures; the Pentagon wanted more stringent testing measures such as those applied to weapons systems. Among the problems, the Navy discovered that instead of a few thousand software applications, its systems actually housed a staggering 100,000. Hundreds of old applications could not be moved to the new system, meaning that hundreds of workers were forced to have two computers on their desks. The large number of old applications uncovered another set of problems: Some programs could not be merged into the new system. They were either too antiquated to be compatible with the standard NMCI operating system (Microsoft Windows 2000), or it was not even possible to determine their level of compliance with the new security requirements of NMCI.

A compromise was reached and incorporated into the Defense authorization bill, S. 1438, which passed the Senate on the 13th of December 2001 and allowed the Navy to order additional seats under NMCI after specific testing and performance milestones were reached. This event-driven implementation of NMCI was introduced to ensure that the program would be fully tested and proven through its introduction into Navy and Marine field units. (Gail Repsher Emery, article: *"After slow start, Congress learning to like NMCI"*, Washington Technology magazine, February 2002) The incompatible applications had been "quarantined" in separate terminals, meaning that for a specific timeframe some employees have two computers; one handling the new system's traffic and another with the old programs, but they were able to continue with their normal business. As for the legacy applications, the Navy adopted an approach called "ruthless rationalization," the objective of which was to eliminate all unnecessary applications and reduce the number in place to fewer than 10,000; the goal was 1,000. With most of the initial misgivings resolved and better communication between Congress and the Navy, lawmakers approved $582 million for NMCI in the 2002 Defense Authorization Act.

But the legislation also established milestones and conditions including rigorous testing, that the high-profile program should satisfy in order to win funding during the next budget cycle. The bill also required the Navy Secretary to report to Congress on the testing and implementation of NMCI, when the Navy would order more seats, and also when EDS would assume responsibility for more seats, according to the proposed

schedule laid out. Additionally, it required the Navy to appoint a manager for NMCI whose sole responsibility was to oversee and direct the program.

In the period between March to May 2002, an independent third party, Management Systems Designers, Inc. (MSD) announced the NMCI Contractor's Test and Evaluation (CTE) phases 2 & 3 were completed successfully, at the first NMCI operational sites at Naval Air Station Patuxent River, Maryland; Naval Air Facility, Washington, DC; Naval Air Station Lemoore, California; and network operating centers at Norfolk, Virginia and San Diego, California, therefore removing the legislative barriers and making way for additional "seats" to be ordered .[Note 1] The NMCI system also passed a test according to the DoD established framework and guidance, in May 2002, verifying that it was working properly. Under an agreement between Pentagon and Navy officials, the Navy was permitted to roll out about 60,000 seats as a test of the feasibility of the project. John Stenbit, CIO at the U.S. Department of Defense, approved on May 3 the continued rollout of the NMCI after EDS successfully passed initial tests conducted on the pilot seats that were already in place. Achievement of "Milestone One" allowed DoN to order an additional 100,000 seats. However, Navy officials and outside experts acknowledged that the program still faced significant challenges, particularly in the areas of change management and legacy system integration.

DoN officially turned up the heat on EDS on August 2002, when it began monitoring the service users were receiving through NMCI. Those service-level agreements kicked in on the 9th of August, when NMCI passed the 20,000-user mark. Under a September 2001 agreement with Pentagon officials, EDS and the Navy had to review the service levels for a month and conduct an "operational assessment" that shows that the data monitored by the enterprise management system is accurate. In the same month, the NMCI team reached another critical milestone, with the Pentagon giving the Navy the go-ahead to connect about 40,000 users working on the Defense Department's classified network, SIPRNET. More specifically, SIPRNET is DoD's classified network that military personnel use for accessing classified applications and databases and for secure messaging. Although it uses common Internet Protocol (IP) standards, it is physically and logically separated from all other computer systems, because it is using dedicated encrypted lines for transmission.

With the pace of the program accelerating, DoN and EDS decided to "tighten" the service-level agreements that are the basis of measuring the performance of NMCI. (Christopher J. Dorobek, article*: "Navy, EDS to refine performance metrics"*-Federal Computer Week, September 2002) Such tinkering should be a normal part of a performance-based IT contract and the operation of the enterprise management system, monitoring the SLAs was one of the questions at the heart of NMCI's next milestone. The Pentagon had already asked DoN to demonstrate the capability of accurately monitoring service levels across the whole available network. Additionally, the Defense Operational Test and Evaluation division completed its independent assessment and testing of NMCI on the 4th of October, which would provide the data for the project's next significant milestone, demonstration of the contractor's with the established SLAs. Those tests showed mixed results, but the overall consensus of those involved with the management of the NMCI initiative was that the newly built system had all the potentials to achieve its specified goals. On the positive side, the same evaluation concluded that NMCI's external security met SLA goals. Internal security needed improvement in password and configuration management, but the Common Access Card Public Key Infrastructure cryptographic login should provide additional security when implemented.

Some of those problems discovered in the testing included:

- Reach-back to legacy e-mail was slow.
- Help-desk performance was below service level goals
- Performance at the workstation level was inconsistent.
- Configuration management, incident and problem management processes were immature. (Matthew French, article: *"NMCI Testing shows mixed results"*- Federal Computer Week, December 2002)

> We are now in Part Two of the process, and that is to brief those who need to be briefed [to receive approval] to go beyond that 60,000-seat cutover and ensure the service level agreements to go to an order beyond 160,000 seats
>
> Rear Admiral Charles Munns, U.S. Navy, NMCI director, from the Mathew French article

The contract model has always called for the firm to invest money upfront and make a profit later. Deploying the equipment and manpower has been costly for EDS. After already investing $650 million to $800 million in the Navy intranet, it discovered that it would take longer than expected to turn a profit. Given its weak financial position, reaching profitability was increasingly important. Nevertheless, the Navy asked Congress to extend the contract for two more years, which would make up for delays and allow EDS to recoup its costs. The contract received a significant modification in the 30th of October 2002. EDS Corp. was awarded a $1,916,000,000 modification to the previously contract (N00024-00-D-6000) for an extension to add two years to the basic contract period. (www.defenselink.mil (DOD News: Contracts for October 30, 2002) accessed February 2004) The final modification of the contract has resulted into a base period of seven (7) program years and maintains the option for an additional three (3) program years.

2. Establishment of SLAs

NMCI represents more than just the harmonizing of hundreds of separate systems within ashore installations. DoN is adopting an approach that has already been extremely successful for industry, by purchasing IT services that include hardware, software, maintenance and training. While many commercial organizations in the past have employed service level agreements (SLAs) for information technology acquisition and maintenance, the NMCI represents one of the few instances where a government agency has adopted this approach, therefore pioneering the way. The heart of every performance-based contract is the SLA that defines satisfactory performance, computes payment, and measures success. The first and most important step in a performance-based contract is selecting and specifying achievable performance levels.

To ensure that the Navy and Marine Corps had adequate opportunity to outline their requirements and expectations, representatives from the various stakeholder groups contributed input from the early inception of the project, to include feedback from the end user team. They met on a regular basis to determine necessary features, the value of each feature to a specific group and DoN in general, affordable and acceptable costs, appropriate incentives for vendors that were all included in the SLAs and the RFP for the

NMCI contract. Service Level Agreement (SLA) is a specifically defined level of performance required by the NMCI contract.

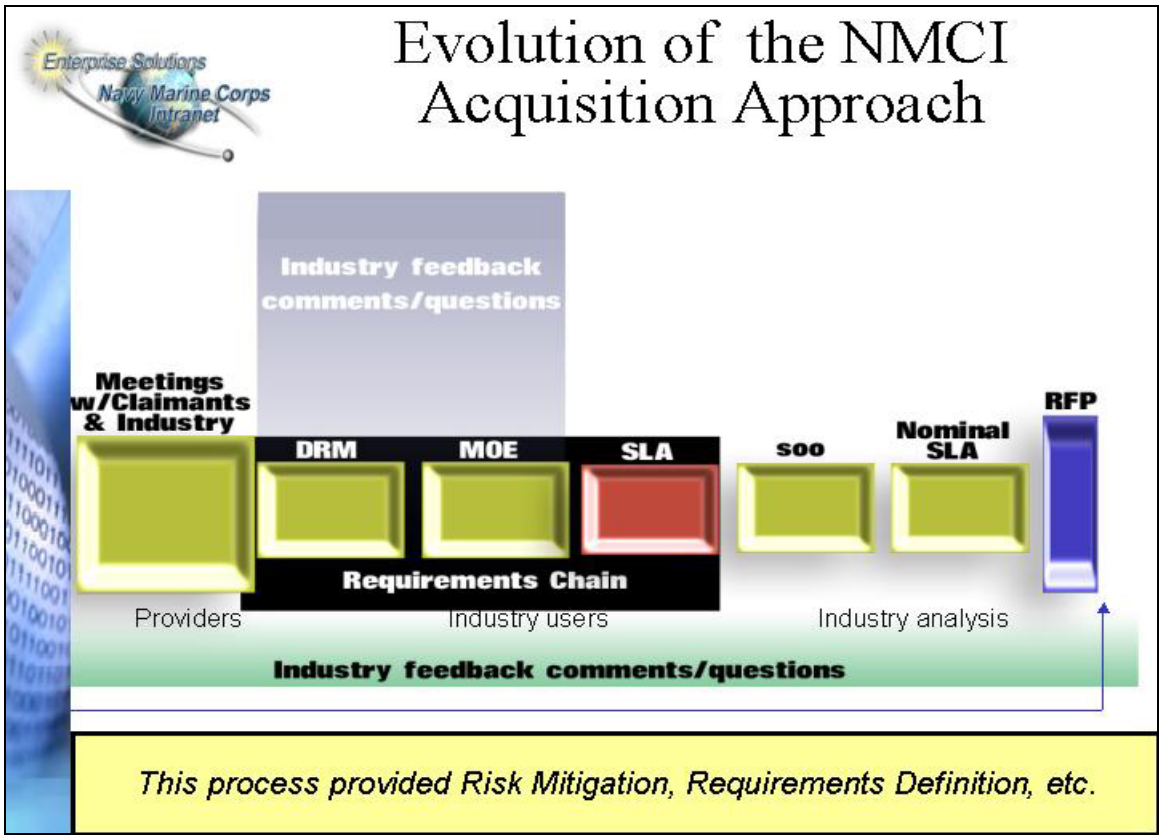


Figure 15: The DoN's Approach to Determine the SLA's Related with NMCI (via interaction with the potential providers and end-users), by Captain Chris Christopher from his NMCI Briefing for the Joint Logistics Council, USA, 29 March 2001

The NMCI contract includes a total of thirty-seven (37) SLA's and establishes financial penalties if the contractor fails to meet them. This utility-like costing and billing style associated with NMCI is expected to result in numerous benefits like lower overall costs, faster IT acquisition cycles and easier integration of new personnel into a command. It is a common standard within industry that service level performance should be based, in part, on end-user satisfaction and that the specific level of satisfaction should be measured by a third party that is independent of both the Navy and EDS. As a result, there are incentives included within the contract to motivate superior contractor's support. EDS could earn hundreds of millions of dollars if it meets certain specific standards. (Matthew French, article: *Survey says... NMCI users satisfied*, Federal Computer Week, 24 March 2003). These incentives are:

- A one-time $10 million payment when all 360,000 seats have been transitioned to NMCI.
- Up to $1.25 million per year for using small and disadvantaged businesses as subcontractors.
- Up to $144 million per year for meeting customer satisfaction goals — based on earning $25 per seat per quarter if customer satisfaction levels are at 85 percent, $50 per seat per quarter for 90 percent customer satisfaction or $100 per seat per quarter for 95 percent customer satisfaction.
- Up to $10 million per year for information assurance if NMCI performs well in unannounced "information warfare" tests of the network's security and survivability.

Each SLA is quite extensive in details and includes:

- Service Name
- Service Description
- Service Delivery Points
- Performance Categories
- Performance Measurement Requirements
- Performance Requirements
- Equivalent Level of Service
    - Level of Service 1 - Basic
    - Level of Service 2 - High End
    - Level of Service 3 - Mission Critical

In the following Table (Table 1) the analytical description of the randomly selected SLA 2 is presented, in order to provide an example of the final level of details included within the contract, while Table B at Appendix B provides the analytical description of the monitoring performance criteria involved with the NMCI, along with the methodology used to determine variations from the optimal level of service.

Service Name: Standard Office Automation Software			**SLA: 2**
Service Description: Vendor provided standard desktop integrated software suite. It includes word processing, spreadsheet, presentation graphics, and database. These packages must interoperate across DON and within the Department of Defense.			
Applicable Service Delivery Points: Fixed and Portable (Basic, High End, Mission Critical) Workstation, Embarkable Workstation, Embarkable Portable (Government and Contractor provided), Hybrid Seat			
Levels of Services: 3: (Basic, High End, Mission Critical)			
Performance Category 1: Installation Accuracy			
Performance Measure Description: Percentage of office automation software installations/upgrades successful on first use. Formula is: (# of office automation software installation/upgrades in month - # of 'failed/improper' installation/upgrades) / # of installation/upgrades in month. The failed number includes incorrect software version, improper configuration, failure to install/upgrade in designed time-window, etc, that are reported within 72 hours of completion of the seat installation checklist by the ISF technician and acceptance by a Government user. It excludes any network related failures if software loading performed from a central source. The measurement is an aggregate and average by site of the installation accuracy by similar seats as determined by trouble tickets at the Help Desk. The software is assumed to be installed properly unless the NMCI end user notifies the Help Desk informing of a failure.. If no installations/upgrades occur during a reporting period, the value will be reported as "N/A".			
Who: Contractor		Frequency: Monthly	
Where: NMCI-wide		How measured: Vendor includes all events of failed installation/upgrades in monthly reports to the Government. It includes date, software package and user/PC ID for which it failed. The 'failed installation/upgrade' data will be audited by the Government or a designated third party.	
	B Value	Pre-Negotiation	Contract SLA
Level of Service (1)	0.995	0.995	0.995
Level of Service (2)	0.995	0.995	0.995
Level of Service (3)	0.995	0.995	0.995
Performance Category 2: Software Currency			
Performance Measure Description: Office automation software currency relative to industry standards. OA software standard across the enterprise. The metric values listed are qualified as follows: where a current NMCI software version falls 2 versions behind the latest commercially available release, then the contractor must upgrade the enterprise to the newest release within three months of the release of the new version, unless the Government determines otherwise. In the case where current NMCI software version has been implemented for greater than one year, and a more current version is available, the contractor will upgrade to the latest version within 3 months following the one year anniversary, unless the Government determines otherwise.			
Who: Government team		Frequency: Quarterly	
Where: Enterprise level		How measured: Analysis of NMCINMCI standard office automation software compared to state-of-the shelf office automation software, as determined by contractor/Government configuration control board.	
	B Value	Pre-Negotiation	Contract SLA
Level of Service (1)	<= 1yr or 2 versions	<= 1yr and/or 2 versions	<= 1yr and/or 2 versions
Level of Service (2)	<= 1yr or 2 versions	<= 1yr and/or 2 versions	<= 1yr and/or 2 versions
Level of Service (3)	<= 1yr or 2 versions	<= 1yr and/or 2 versions	<= 1yr and/or 2 versions

Performance Category 3: Interoperability			
Performance Measure Description: For Standard Office Automation Software, the interoperability requirement is to provide users with the ability to exchange information using standard Gold Disk applications with other DON users not served by NMCI (IT-21, MCTN, and OCONUS), with DoD/Joint partners, and with major acquisition partners. The products and data produced on NMCI desktops must be managed to ensure that all current and future versions of the Gold Disk support the information exchange requirements of the Navy and Marine Corps mission, to include backward compatibility. Standard Office Automation Software interoperability will be measured in two ways: (1) proof of interoperability and (2) Help Desk Interoperability Trouble Tickets. -The proof of interoperability is to establish and maintain connection for the purpose of transferring standard office products between the test client and a set of representative test sites. This set is described in the Interoperability Test Plan. Gold Disk applications will be exercised by scripts operated from user agents installed at network devices located within NMCI and at external locations including IT-21/MCTN, DoD/Joint and commercial partner (major acquisition partners). The proof of interoperability is successful end-to-end testing between the test client and remote test site and is defined by the receipt of an anticipated script response. Failure equates to (2) two consecutive unsuccessful executions of a single application script from/to the same sites. Measurement will be performed by schedule and by event (to include introduction of a new application version); additional measurements will be performed as appropriate to ensure interoperability. - Interoperability will also be assessed by submission by users of Help Desk Interoperability Trouble Tickets. The definition of interoperability failure is exceeding the Government and ISF agreed upon Help desk reporting threshold value. The interoperability measurement must capture two-way functionality. Notification of the Government is required for Office Automation Software failure established by the DON; the timeliness of reporting is stipulated in the Level of Service metric.			
Who: Contractor		Frequency: Measured a minimum of once monthly for user agents; continuously for Help Desk. Reported monthly.	
Where: Measured from an NMCI user agent (located at an NMCI workstation) or an equivalent client configuration operated from a NOC test installation to test points identified in the NMCI Interoperability Test Plan, to include NMCI, DoD/Joint, and at least one Commercial (Major Acquisition Partner). Help Desk data will be captured from interoperability trouble reports.		How measured: 1) End User Incident Reports to Help Desk, and Remote Locked Down Workstation test results by running scripts. Collection and analysis granularity will be by test site for script-based tests; by organization, site, claimant/command for trouble ticket based reports.	
	B Value	Pre-Negotiation	Contract SLA
Level of Service (1)			Notification within six (6) hours
Level of Service (2)			N/A
Level of Service (3)			Notification within three (3) hours
Performance Category 4: Customer Satisfaction			
Performance Measure Description: Level of customer satisfaction.			
Who: Contractor		Frequency: Initially measured at six month intervals for first year of contract and then yearly thereafter.	
Where: NMCI Customers using service		How measured: Customer survey, random sampling of NMCI customers using this service.	

	B Value	Pre-Negotiation	Contract SLA
Level of Service (1)	0.85 satisfactory rating	0.85 satisfactory rating	0.85 satisfactory rating
Level of Service (2)	0.85 satisfactory rating	0.85 satisfactory rating	0.85 satisfactory rating
Level of Service (3)	0.90 satisfactory rating	0.85 satisfactory rating	0.85 satisfactory rating

Table 1: NMCI SLA 2 Analytical Description, from the original NMCI Contract N00024-00-D-6000, 30 Oct 2002

The following Table (Table 2) provides the cumulative list of SLA, still in effect within the NMCI contract.

NMCI Services (per Attachment 1)	Service Level Agreement (SLA) Provided
User Upgrades	
Desktop Hardware and Operating System	1
End User Services	
Standard Office Automation Software	2
E-mail Services	3
Directory Services	4
File Shared Services	5
Web Access Services	6
Newsgroup Services	7
Multimedia Capabilities Services	Deleted
Print Services	9
NMCI Intranet Performance	10
NIPRNET Access	11
Internet Access	12
Mainframe Access	13
Desktop Access to Government Apps	14
Moves, Adds, and Changes	15
Software Distribution and Upgrades	16
User Training	17
	Deleted
Unclassified Remote Access	18
Classified Remote Access	19
Portable Workstation Wireless Dial-in	20
Organizational Messaging Services	20A
Desktop VTC (hardware & software)	21
	Deleted
	Deleted
Voice Communications	22
Voice Mail	22A
Maintenance and Help Desk Services	
Basic Help Desk Services	23
Communications Services	
Wide Area Network Connectivity	24
BAN/LAN Communications Services	25
	Deleted
	Deleted
Moveable Video Teleconferencing Seat	26
	Deleted
Proxy and Caching Services	26A
External Networks	27
Systems Services	
Network Management System Services	28
Operational Support Services	29

Capacity Planning	30
Domain Name Server	31
Application Server Connectivity	32
Network Operations Display	32A
Information Assurance Services	
NMCI Security Operational Services General	33
NMCI Security Operational Services PKI	34
NMCI Security Operational Services SIPRNET	35
NMCI Security Planning Services	36
Advanced Application and IM Support	
	Delete
	Delete
Other Requirements	
Integrated Configuration Management	36A
Integration and Testing	36B
Technology Refreshment	36C
Technology Insertion	36D
Sea-Shore Rotation Support	
Sea-Shore Rotation Support Training	37

Table 2: Cumulative NMCI Standard Target Performance Measures, from the NMCI Contract N00024-00-D-6000, 30 October 2002

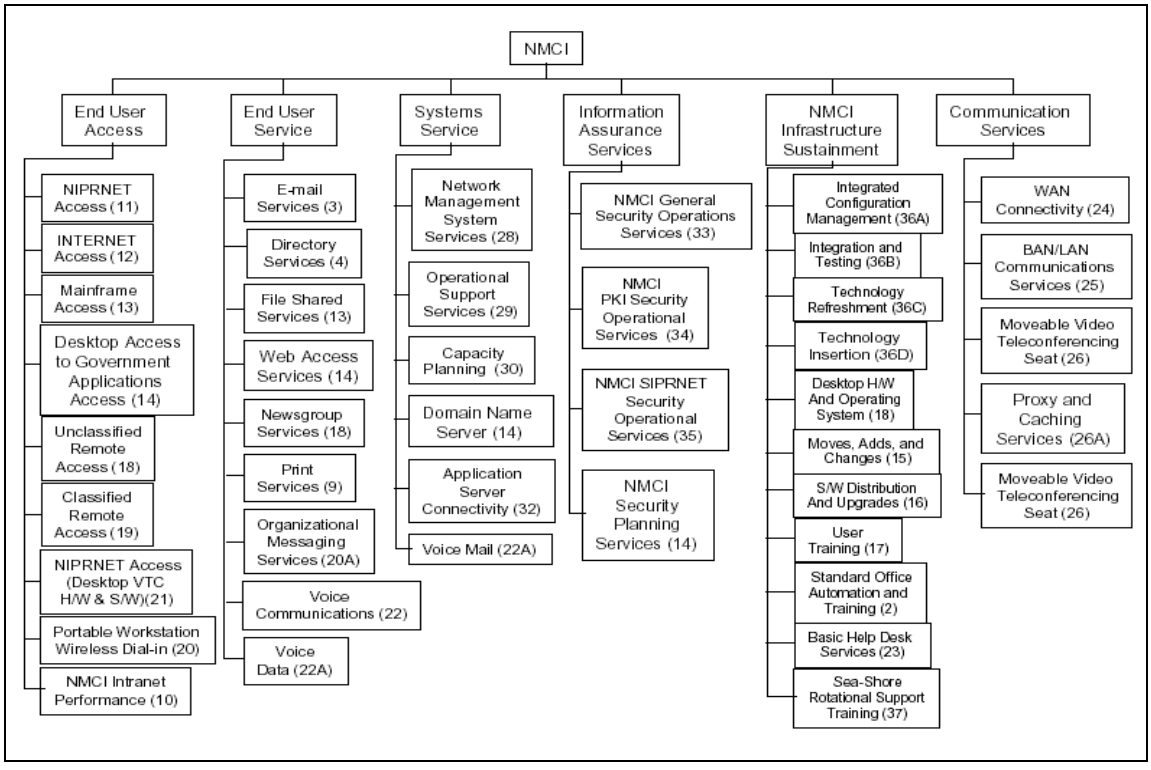


Figure 16: Breakdown of NMCI SLAs, by Captain Chris Christopher, from the NMCI Briefing for the Joint Logistics Council, 29 March 2001

3. The Transition towards NMCI

a. Companies Involved

EDS, as the coordinator of the NMCI contract has assumed the responsibility for providing all assets and services needed to ensure the transmission of voice, video and data across DoN. In order to fulfill the requirements of the contract, EDS has formed a partnership with leading businesses in the domain of IT, under the title **Information Strike Force (ISF)**. Their roles and responsibilities are as follows: (www.nmci-isf.com (EDS-NMCI Team), accessed February 2004)

- EDS for overall service delivery
- Raytheon for security and information assurance
- MCI for the Wide Area Network (WAN)
- WAM! NET for Base Area Network (BAN)/ Local Area Network (LAN)/Metropolitan Area Network (MAN)
- General Dynamics for the BAN/LAN/ MAN
- Robbins-Gioia for project scheduling
- Cisco for routers and switches
- Microsoft for software
- Dell for desktops, laptops, servers and enterprise storage systems
- Dolch for desktop and portable embarkables
- Dataline for voice services
- Hundreds of small businesses for help desk, network operations center and field services

b. The Plan Used

The **transition** to NMCI is divided into distinctive phases, resulting into an evolutionary process used to gradually transform USN and USMC sites from the previous IT environment towards NMCI. The idea is to:

- Adopt an incremental approach
- Leverage current contractors
- Use empowered, on-site teams

- Minimized disruptions to ongoing operations

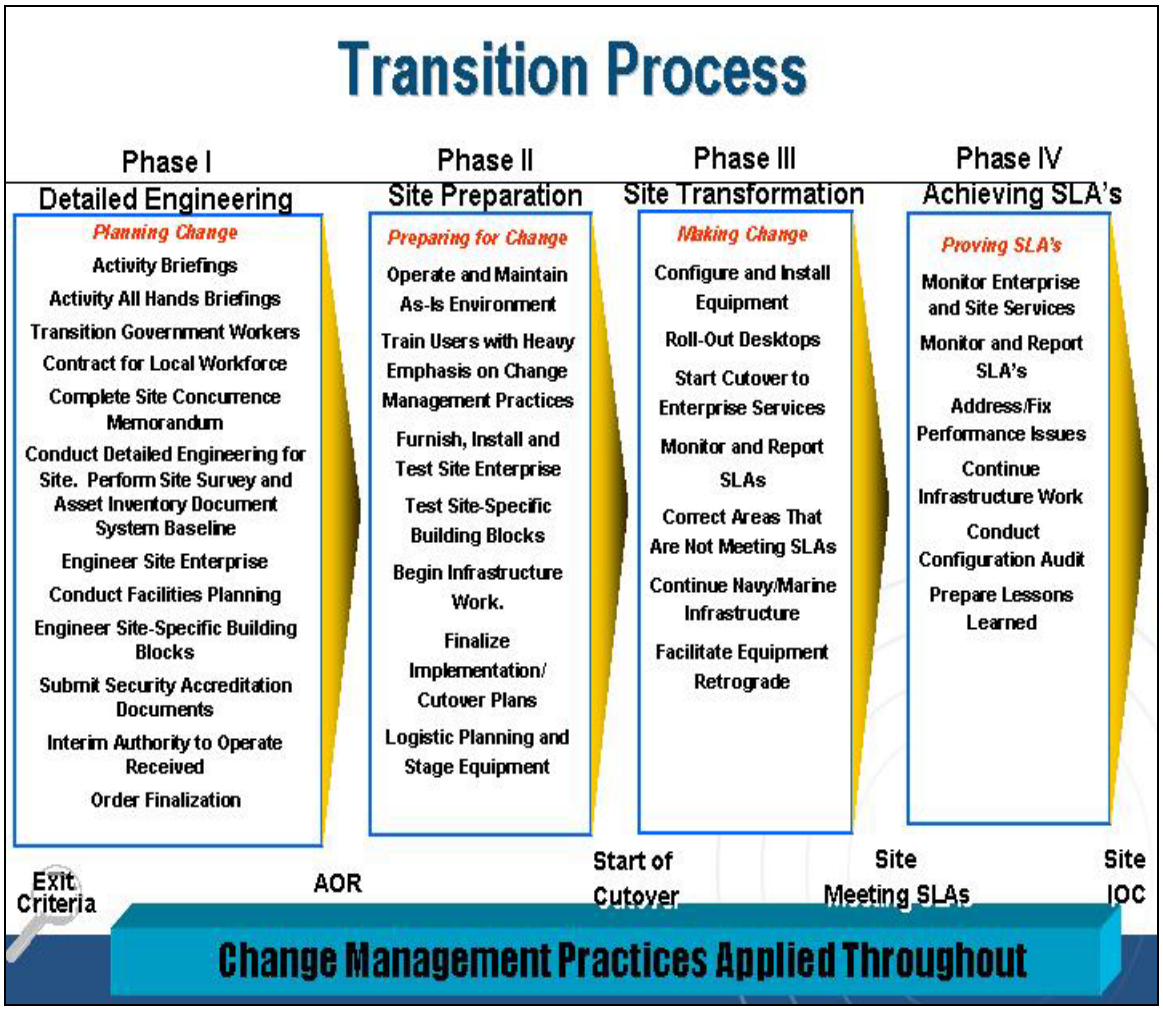


Figure 17: Transitioning Sites into NMCI.

In more details the procedure and its supporting activity can be broken down as follows (www.nmci.navy.mil (Transition to NMCI), accessed February 2004)

Phase 1: Pre-AOR [Planning Phase]

The planning phase begins when DoN awards a task order for NMCI services to the ISF. During this phase, the ISF collects the information it needs for initial work force development and planning activities based on the total site order. **Assumption of Responsibility (AOR) is defined as the date when responsibility for operating the "as-is" (current IT) environment, for work defined by the ordered NMCI CLINs, shifts from the government and its local contractors to the Information Strike Force (ISF).** During this phase, ISF validation teams arrive

on the implementation location to begin collecting data and to coordinate long lead-time activities. The validation teams assess information technology and warehouse facilities, security accreditation, legacy applications, and WAN provisioning. The teams also begin to make detailed assessments of the Base Area Network/Local Area Network (BAN/LAN) and the existing desktop and server environments, and collect additional information on security hardware in order to finalize the NMCI design. The following means are used to coordinate activities:

- Preliminary Site Questionnaire (PSQ): Collection tool that assists commands in collecting required data prior to their transition to the NMCI environment. Includes detail about:
  - Data Network Organization
  - Registered IP Addresses
  - Current Network Infrastructure Components
  - Current Servers
  - Wide Area Network (WAN)
  - Local Area Network (LAN)
  - Legacy Software Applications (non-COTS)
  - COTS Software Applications
  - Existing Hardware
  - Trouble Call / Help Desk Support
  - COMSEC
  - Information Assurance
  - Contracting / Procurement
- AOR Checklist: Defines the actions required by ISF, the customer and the government Program Office to achieve ISF Assumption of Responsibility at a site.

- Site Concurrence Memorandum (SCM): Define the roles and responsibilities of the ISF and Navy Marine Corps organizations at individual sites for the accomplishment of transition to NMCI

- Government Furnished Facility (GFF) Checklists: Assess the suitability of proposed government-furnished facilities for use as server farms and supporting facilities, by the ISF team

- List of Potentially Impacted Federal Civilian Employees: (Self-explanatory)

- Contractor Ordering Process: Amplifying information on ordering NMCI services for government contractors who support the DoN

Phase 2: AOR to Cutover [Site Preparation]

During the site preparation phase, the ISF team completes the build out necessary for the operation of NMCI. Activities include furnishing, installing, and testing the NMCI site enterprise, and beginning infrastructure work in order to finalize implementation and cutover plans. The following tools are used during this phase:

- Cutover Checklist: The Cutover Checklist defines the actions required of all those involved to achieve start of Cutover to NMCI.

- Legacy Applications Transition Guide: Governs required actions for collecting detailed information on legacy applications prior to transitioning to NMCI.

    - ISF Tools Web Site/IT Survey Tools & Related Files: Legacy application information and application certification status information.

    - Classified Legacy Applications Rationalized List Template: Guidance for submission of classified legacy applications.

- NMCI Legacy Applications Submissions Guide: Describes how to submit unclassified and classified application media for NMCI certification & validation testing.
- Engineering Review Questionnaires: Completed to facilitated accreditation process.
- NMCI Release Development & Deployment Guide: Information and guidance to developers interested in migrating content, introducing new applications, or changing existing applications within NMCI.

Phase 3: Cutover [Site Transformation]

Cutover is the final major milestone in the NMCI transition process. It is that date when the ISF and government site personnel initiate the deployment of NMCI seats and services on site. Tools used to support the procedure are:

- Cutover Checklist: The Cutover Checklist defines the actions required to achieve start of Cutover to NMCI
- Workstation Migration:
  - Ready Guide: overview of processes and procedures leading to the installation of NMCI seats and the software training programs available after installation
  - Workstation Set Guides: Step-by-step instructions for the user to prepare the existing workstation for the rollout process
  - Desktop User Share Guides: Assist in transferring the user file access available between Legacy workstations, called desktop user shares, to the networked environment of NMCI.
  - Workstation Migration User Guide
- Legacy Microsoft Server Migration Guide: Establishment of strategy for integrating legacy application servers with NMCI.
- Remote Access Service Guides

- Outlook Web Access Users Guide
- NMCI Asset Disposal

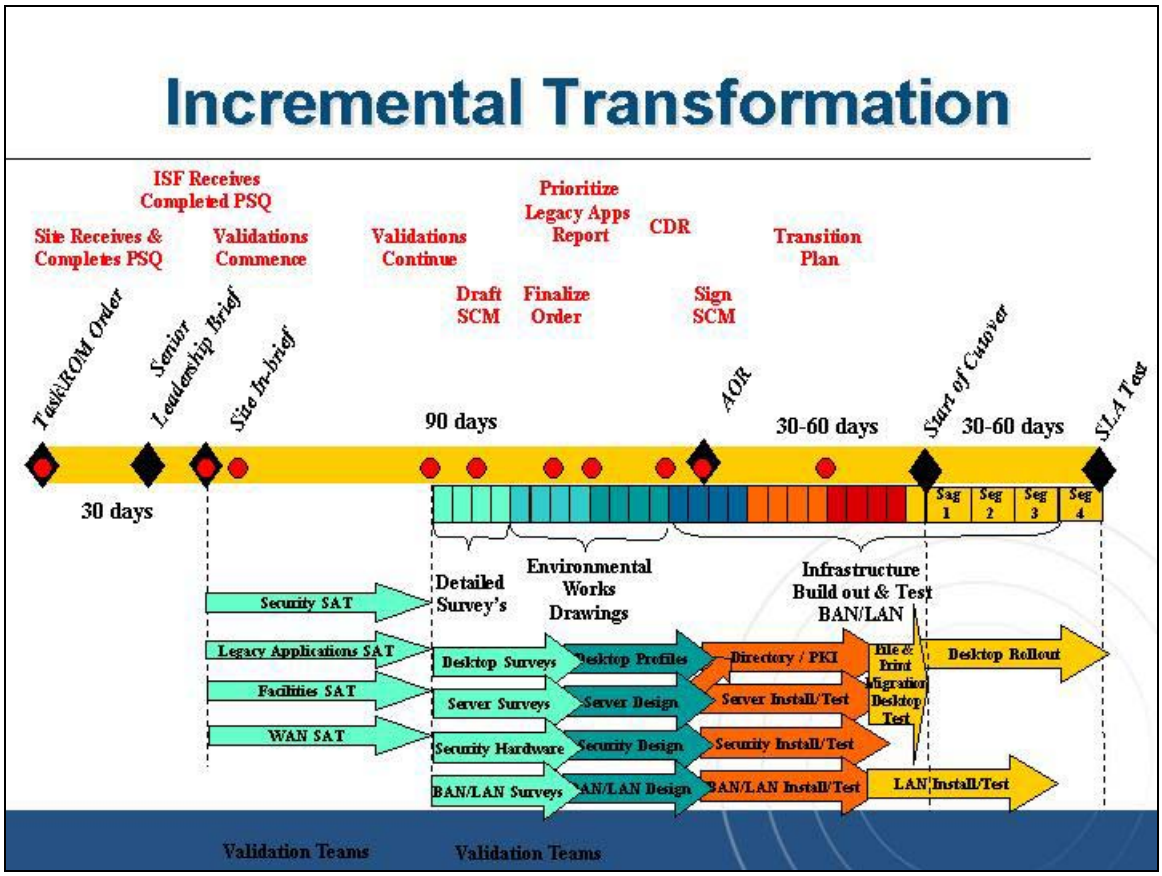


Figure 18: Summary of the Activity to Transition towards an Operational Site with NMCI

Phase 4: Meeting SLAs-[Site Operational]

The building activity of the site, to include testing of the facility, has finished and the site is now under the EDS-ISF technical responsibility and support. The driver behind the operational concept is to conform to the SLAs that describe the desired level of services.

4. Key Policies and Regulations

a. NMCI Interoperability and C4I Support

DoN was committed to ensure that interoperability within Naval establishments and with the joint community within DoD would not be degraded in the new IT environment and used NMCI to lay the groundwork for significant improvements

in the domain of communications. The NMCI project would ensure continued interoperability within the GIG and along with other Department of Defense Enterprise level applications, while through the NMCI contract requirements DoN would maintain access to all legacy applications. Two major aspects of interoperability had been identified for special emphasis:

- Operational Architectures
- Compatibility of NMCI IT services with existing external applications

Interoperability and C4I Support were documented as firm NMCI requirements throughout the NMCI Request for Proposal and in the Test Planning related documentation. Additionally, DoN imposed the requirement for the NMCI vendor to generate and use a separate Interoperability Test Plan. The NMCI RFP incorporated a draft Interface Control Document (ICD) that cited specific standards, interfaces and partners for which interoperability had to be maintained. This document provided detailed descriptions and specifications of the interfaces between the NMCI and other Defense related networks. The ICD was used to enforce the NMCI vendor to comply with the Joint Technical Architecture (JTA) [Note 2]. The NMCI RFP established SLAs that include interoperability metrics requiring both real time threshold reporting and periodic reporting. The NMCI vendor was required to propose specific mechanisms to measure interoperability of 23 separate services. (NMCI Report to Congress, 30th of June 2000, p. D-4-1)

b. Test and Evaluation Strategy

The NMCI contract provides for Inspection and Acceptance as the method for verifying that the services provided by the Contractor are in compliance with the requirements of the contract. Inspection and acceptance should be performed using a combination of the following two methodologies and demonstration of successful service delivery is defined as successfully completing both aspects:

- Contractor executed testing and verification against contract requirements with contractor-developed and Government-approved test processes and procedures.

- Government execution, with contractor support, of government developed test processes and procedures. (NMCI Report to Congress, 30th of June 2000, p. D-5-1)

NMCI services Inspection and acceptance were divided into two distinct periods:

- Proof of concept testing and evaluation. (NMCI First Installation Increment) Successful completion of proof of concept testing and evaluation constituted achievement of Initial Operational Capability (IOC) for the NMCI implementation

- Transition testing and evaluation

c. NMCI Governance

Federal statutes, DoD and DoN directives provide the overarching policy that governs every aspect of NMCI and the related computing environment. The Director NMCI is manages the acquisition of NMCI and provides additional acquisition guidance to the Navy and Marine Corps NMCI Program Managers, while operating within the policy constraints of DoD's acquisition regulations framework.

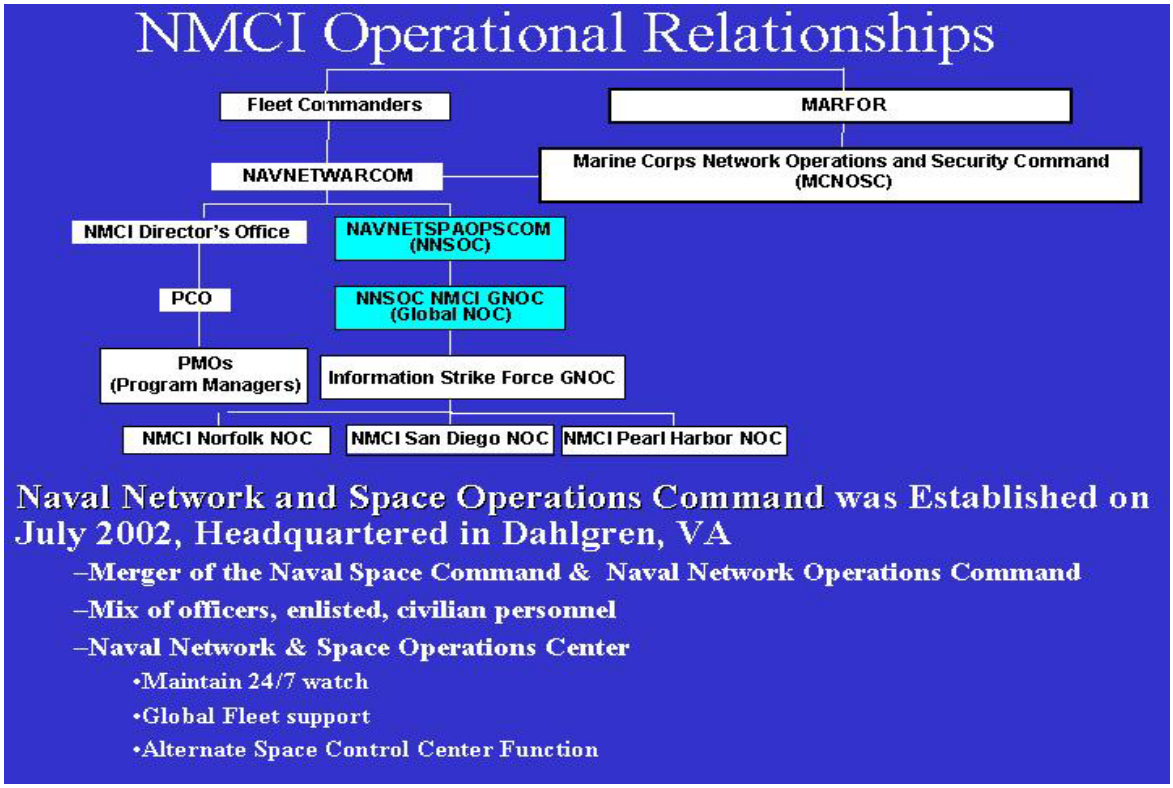


Figure 19: The NMCI Operational Relationships-Historic Evolution and Purpose

The Navy and Marine Corps organizations responsible for network operations and security oversee the operation of NMCI. Within the Navy this is Naval Network and Space Operations Command (NNSOC). Within the Marine Corps this is the Director Headquarters Marine Corps C4. These organizations work closely to develop operating and security policies that govern the day-to-day operations of the NMCI. These policies reflect higher-level guidance from the DoD, the Joint Chiefs of Staff, and the Department of the Navy CIO, along with the Navy Information Officer and the Marine Corps Chief Information Officer. (www.nmci.navy.mil (Policy Statement), accessed February 2004)

Figure 20: NMCI Governance, from Rear Admiral J. P. Cryer, U.S. Navy, Commander of Naval Network and Space Operations Command, NMCI Operations Brief at the NMCI – Industry Symposium, 18 June 2003

NNSOC is the operational arm of NETWARCOM for network and space operations. NNSOC's role in NMCI Network Operations is as follows:

- Global Network Operations Center (GNOC)-Detachment Norfolk supporting 310,000 planned users by end of year 2003
- NNSOC teams with:

- Director NMCI for NMCI cutovers & installs
- SPAWAR PMW-161 for contract issues
- Operational Direction in support of Fleet Commanders
- Supports NETWARCOM NMCI Governance process
- Maintains NMCI Security oversight
- Manages Sea Shore Rotation (SSR) for associated personnel

NMCI Security roles can be summarized as follows:

- Administration (NAVNETWARCOM)
  - Designated Approval Authority (DAA)
  - Establishes policies and procedures for all Navy networks
  - Approves Certification and Accreditation of the network
- Operations (NNSOC)
  - Directs the contractor (EDS) at the operational level
  - Implement Information Assurance Vulnerabilities-Alerts / Bulletins / Technical Advisories
  - Change Information Conditions (INFOCON)
  - Ensures adherence to DoD/DoN security policy
  - –Manages contractor's responses to security incidents

5. Impact on the DoN Mission

NMCI has the potential to enhance and improve enterprise-wide working procedures and training, by providing common IT services across the Navy & Marine Corps enterprise. Additionally, by having as a requirement the support of new initiatives such as knowledge management, distance learning, and telemedicine, it has the potential to significantly improve the quality of life for Department of the Navy employees and support personnel. By bringing together the Navy and Marine Corps ashore workforce

into a common IT infrastructure, NMCI will foster greater levels of communication, collaboration and sharing of ideas than would ever have been possible before.

The BCA for the NMCI strongly emphasized that the previous IT environment was providing adequate operational and strategic support for the DoN mission. NMCI is introduced with the aim to be the tool enabling and the driver supporting innovations in business processes and practices that are necessary to create a totally new, improved Naval-operating environment, with significant financial savings through superior management of resources and personnel. The idea of widely available data that is consistent throughout the enterprise will promote fundamental changes in the way the Navy is conducting its business or transactions, training sailors and even supporting critical war-fighting tasks.

Current Environment	Requirement (NMCI)
Large disparity in quality of service across the DoN	Consistent (high) level of service for ALL DoN end users
Redundant procurement, sourcing and support infrastructures	Consolidated sourcing, support and procurement
Unmanaged cost environment – allocated from a variety of budget sources (IT budgets, end of year money, etc.). Lack of visibility into true cost of IT.	Cost is discrete, competitive with current IT spending. Full visibility into cost of IT services.
Fragmented, inconsistent and informal Help Desk.	"One-stop" help desk support.
Non-IT systems adversely impacted by inconsistent performance of IT systems and current support model.	Improved productivity for all IT users.
Insufficient asset management.	Comprehensive asset management, tracking, and configuration control standard in commercial best practices. Asset management role switched from DoN to vendor.
Navy personnel managing many networks.	Allow DoN personnel to refocus on core mission. Key network attributes managed through a central DoN IT organization.

Table 3: Comparisons Made Between the Previous and the Expected NMCI IT environment, from the BCA for the NMCI

Last but not least, NMCI will provide significantly improved level of security, with protection from outside attack as well as internal safeguards. From a technology standpoint, NMCI is not only intended to address the problems that various commands experienced in the past when attempting to share information through collaborative tools

and e-mail. With the continuous focus on security that has become a critical concern for military and industry organizations alike, a cohesive system will reduce the number of potential entryways that increase organizations' vulnerabilities to information operations and “malicious cyber-activity”.

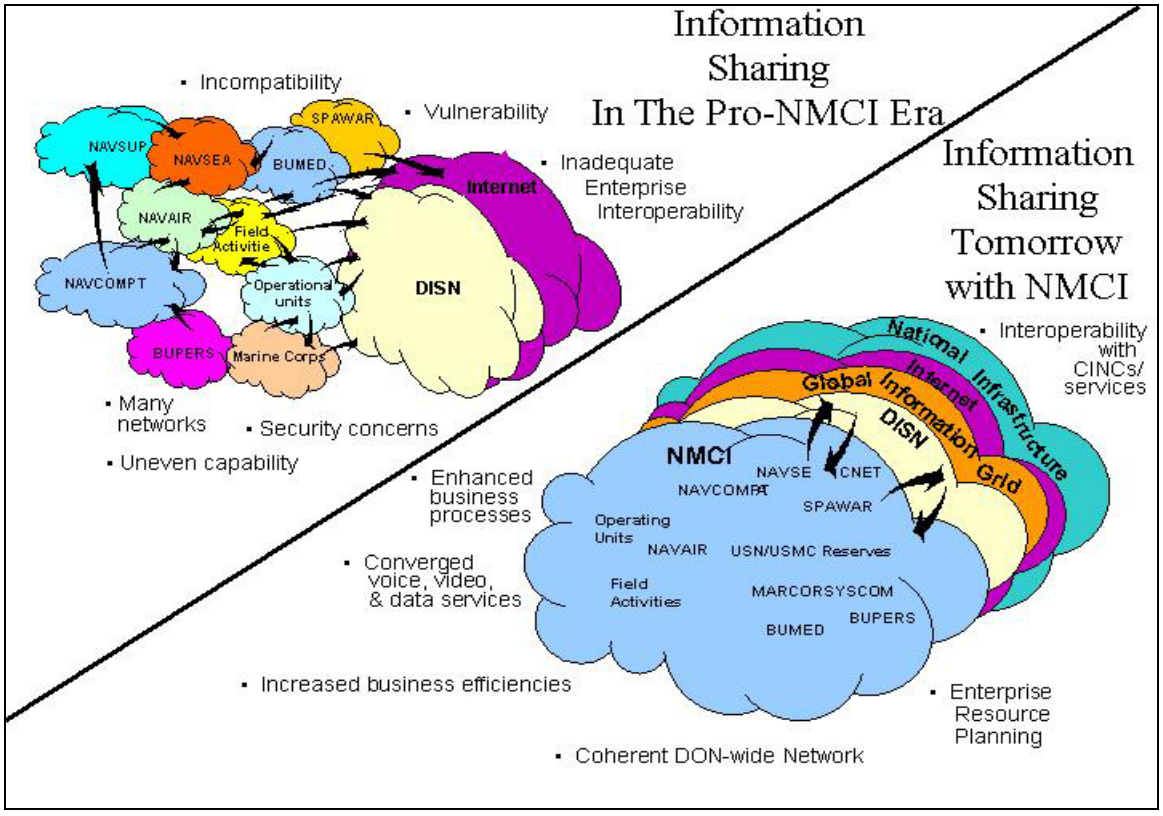


Figure 21: NMCI Impact for DoN, at the Enterprise Level

The idea behind NMCI is to create a system that will enable the Navy to carry out all kinds of service-wide initiatives, from providing a portal for common information to streamlining training opportunities. Over the long term this contract should permit more frequent refresh of hardware, infrastructure upgrades, enterprise distribution of advanced applications, and continuous improvement in operations. The economic benefits of NMCI include fixed per-seat pricing; the economy of scale - buying from a single provider; shared cost savings; and regular technology refreshes to upgrade hardware every three years and software every two years at no additional cost.

The benefits of the NMCI environment include a significant reduction in the Total Cost of Ownership for the DoN IT infrastructure that will accompany improved and

consistent levels of service and performance for all Navy and Marine Corps CONUS IT customers. The contractor will handle systems administration, purchasing, training and maintenance, allowing more sailors and marines to concentrate on their core mission or even re-assigned to different tasks. At the same time, users will have quicker access to the most up-to-date equipment without costly procurements or large up-front capital expenditures.

NMCI has a favorable impact on the Navy in the following three areas:

1. Mission

- NMCI's integrated approach allows operations staff to coordinate their efforts quickly and efficiently to make decisions and provide ready access to the real-time information needed to make decisions. This yields improved access, interoperability, and security.
- Operational readiness improvement as a consequence of the dependable connectivity that NMCI will provide and the more efficient telecommunications operations that are not achievable with DoN's current IT infrastructure.
- Increased productivity achieved through better access to information services, better connectivity with peers and other organizations, improved communications/interoperability, and ease of use across platforms (i.e., same look and feel of the access point) regardless of location.
- Improved productivity at the command level through streamlined budgeting and planning, on-line training and enterprise software deployment.

2. Technical Architecture

- Improved business processes through enhanced standardization and harmonization of IT services, ability to keep pace with technological change, increased reliability and availability.
- Enabling ERP, which is a principal Navy Revolution in Business Affairs (RBA) Initiative.

- Establishment of desktop and server standards and configurations, many of which could be rolled out remotely via the Internet and administered from a centralized point within the new support model.
- More consistent Help desk learning as the number of different types of hardware, software, and configurations will decrease allowing help desk technicians to better focus on the environment they are maintaining.
- Extended sharing of knowledge and expertise worldwide.
- Improved VTC capability.

3. Personnel / Service

- Creation of collaborative information databases and resources.
- Empowered innovative work and training solutions.
- Enhanced quality of life and/or work for every Marine, Sailor, and civilian in the DoN workforce. By-products of NMCI such as on-line training, a standard look and feel across the Naval IT spectrum, a consolidated Help Desk and MOS/NEC stability and retention will each contribute to the enhanced quality of life (Booz, Allen and Hamilton Inc., Business Case Analysis (BCA) for NMCI, (Contract GS-23F-0755H), 6/30/200, pp. 75-77)

To summarize, this new approach towards IT will help USN and USMC meet the following objectives: (www.nmci-isf.com (About NMCI), accessed January 2004)

- Enhanced network security
- Interoperability among them as well as other Services
- Instant Web access
- Knowledge sharing across the globe
- Consistent office environment
- Increased productivity
- Improved systems reliability and quality of service
- Reduced cost of voice, video and data services
- Better, faster decision-making
- Greater productivity reduced costs
- Increased combat readiness

B. SUMMARY AND CONCLUSION FOR THE EARLY STAGES OF NMCI

The previous DoN computing environments were so varied and complex that it was exceedingly difficult to communicate electronically across the Department. Virtually every major command and installation has its own process for acquisition, management, maintenance, and disposal of IT systems. Without a single DoN source for configuration control and minimal hardware standards, the local and/or regional IS management staff often set standards without integration of the tactical, operational, and strategic requirements of communications across DoN organizations. The Navy Marine Corps Intranet (NMCI) is an information technology (IT) services contract to provide reliable, secure, and seamless information services to the shore-based components of the Navy and Marine Corps.

The approach offered by the Information Strike Force (ISF), a partnership of companies with world wide recognition under the coordination of EDS, a leading company in providing E-business and information technology services to government and commercial clients around the world, uses an incremental delivery plan to create a single, integrated network IT environment, with standardized software suites and one security architecture in order to maximize security and enhance performance and interoperability across the entire spectrum of the Department of the Navy (DoN) agencies

1. Analytical Breakdown of NMCI Implementation Events up to the Year 2003.

1999

July 7: Navy briefs industry on NMCI

Oct. 6: Request for information released

Dec. 23: RFP released

2000

Apr. 28: Revised solicitation released

May 11: Congress decides to withhold money for at least two months after the Navy justifies the project to the Hill

June 19: Proposals submitted by EDS, CSC, IBM and General Dynamics

June 30: NMCI report to Congress

July 21: Questions from Congress postpones award until Sept. 1

Sep. 01: Award delayed again for more questions

Oct. 02: Award postponed again

Oct. 06: EDS wins contract

2001

Feb.: EDS takes responsibility for 28,250 seats

Mar.: An additional 13,985 seats added to the contract, giving EDS responsibility for 42,235 at 26 Navy facilities

July 9: First network center in Norfolk opens; Sen. John Warner, R-Va., questions commercial testing of NMCI

Aug. 2: House Armed Services Committee proposes Marines not be part of NMCI. Proposal later dropped

Aug. 6: Second network center in San Diego opens

Aug. 28: Navy and Department of Defense settle dispute over how to test NMCI

Sept. 7: First sailor logs on

Sept. 25: Contract modification lowers fiscal 2002 payment to EDS to $600 million from $728 million; Congress requests more monitoring

Sept.: 310 of 3,100 NMCI contract employees laid off by EDS because of slow rollout of the system

Oct. 18: Naval Reserve Air Facility-Washington with 400 seats becomes first facility to exclusively use NMCI

Nov.: Rollout begins for 3,500 seats at the Naval Air Station in Lemoore, Calif., and for 1,000 seats at the Patuxent River Naval Air Station in Maryland

December: Phase 3 testing and evaluation begins

(www.washingtontechnology.com (Timeline of NMCI in the startup of the program) accessed January 2004)

2002

January: Navy begins search for NMCI leader. Rear Admiral Charles Munns, U.S. Navy, is appointed NMCI director

March-May: Testing Phase completed, triggering order but not transitioning for 100,000 additional seats.

June: NNSOC is created.

August: Start of monitoring the level of SLAs. Congress imposes a cap of 60,000 seats until EDS reached more of its service level agreements

August: Testing of the operation of the enterprise management system for the SLA level.

October: Testing completed, announcement of mixed results.

October: Expansion of the baseline timeframe is agreed between DoN and EDS.

December: Analysis of the measurements indicates EDS is close to reaching the SLAs

2. Conclusions for the NMCI Start-Up

The NMCI project has been plagued by off-track progress from the very beginning. During the first year of the contract, NMCI leaders faced issues ranging from how to handle thousands of old legacy applications to questions about how the Pentagon will oversee the program. Nothing similar in nature and magnitude had ever before been attempted: the reduction of hundreds of disparate networks across the globe and tens of thousands of legacy applications into one single, integrated and secure intranet architecture. Such change on a massive scale has fueled infighting and charges of mismanagement. The potential long term results, in terms of cost avoidance, increased security, interoperability and advanced capability, were considered to outweight the near term discomfort. Therefore, based on the idea “better late than never”, the decision for a revised timetable based on “event-driven” facts was mutually agreed to provide a more feasible solution for the NMCI implementation.

The introduction of a rigorous testing process and the move from a time-based to an event-based schedule reassured many on Capitol Hill, and when a program manager was named, communication with Congress and oversight of NMCI within the Navy improved further, therefore turning Congress into an open supporter of the NMCI effort. The Navy's decision to bring a two-star admiral in to run the program indicated its commitment to ensuring that the required change would take place. The Navy plans during the year 2002 were to complete testing of the Navy-Marine Corps Intranet by the

end of April and receive permission from the DoD to add 100,000 more seats to the program. (www.washingtontechnology.com (NMCI testing Moves Forward), accessed February 2004) Again, the target date was lost but after successful completion of testing that involved checking to see if NMCI was secure, reliable and compatible with other defense systems and whether service-level agreements were met the future started to look more prosperous.

A managed services contract requires that the customer focus on the results provided by the contractor and give up some or all of the decision making involved with implementing those services. Because of this, it is imperative that the customer has the following in place, preferably well in advance of awarding the managed services contract: (www.belarc.com (IT as a Utility), accessed February 2004)

- **An accurate and complete inventory** of existing computer hardware, software and users. That element was totally neglected by DoN and left until the contract had been awarded and resulted in unpleasant surprises, i.e. the estimated number of legacy and quarantined applications that had negative impact on the implementation progress. EDS also attributed the technical delays to the extremely large number of legacy applications discovered, many of which should be installed on kiosks outside of the intranet because they failed the security testing or do not run on Windows 2000.

- **Realistic goals and objectives**. The setting of goals and objectives is what most customers focus on, however without an accurate, complete and up-to-date baseline, these goals can be unrealistic from the start. The timeline involved with NMCI was over-optimistic again, with a negative impact in the Congress' confidence in the program and the Navy's workforce morale without a concrete change management plan in place. On the other hand, the interaction between DoN representatives, industry experts and end – user groups made possible a realistic determination of SLAs that are the foundation of the NMCI contract.

- **An independent performance measurement and review process**. The issue is that the service provider supplies IT infrastructure and services and then sends the customer a bill. However, the customer has no independent method of auditing the level of services, systems, software, and networks actually provided. The solution of hiring independent parties to do the NMCI testing along with auditing activity by the appropriate DoD agencies was the optimal solution to ensure the NMCI would remain on high standards and the outside pressure would cause the contractor "to cut corners".

IT-21 implementation was the initial step towards shipboard open communications. Once fully in place, it is expected to enable war-fighters to share classified and unclassified tactical and non-tactical information through a single network interface. This would shorten time lines and increase combat power. However, this capability will probably increase the demands on the shore information technology infrastructure and create a "bandwidth" burden. We are never going to be able to provide enough bandwidth to cover the demands of the GIG, so the alternative solution might be to manage more efficiently the quality of service (QoS) and prioritize the flow of information. Providing an integrated computing infrastructure that allows the authorized end user to communicate seamlessly across the DoN enterprise is a priority. Therefore, it is critical that computing devices utilize the same communication protocols and have access to the bandwidth needed to facilitate prompt communication and collaboration.

One goal of the NMCI is to meet this demand by making available bandwidth "on demand". In conjunction with IT-21, deployed forces will have readily available access to maintenance, logistics, medical and personnel data that resides within the supporting ashore establishments. NMCI could facilitate tele-maintenance by allowing deployed personnel to address a problem on a ship via on-line communication with technical experts ashore, therefore allowing less-experience personnel onboard-deployed units to deal with far more complex issues than they are qualified to. In the medical arena, personnel who come across complex situations will have the support of more experienced medical personnel within installations ashore. Web-based collaborative tools could be used to ensure ease of communications and interactions with the various

echelons of command. This collaborative environment would facilitate a worldwide interactive dialogue and by offering commanders the ability to share knowledge, not just data, it could significantly improve decision-making.

C. ENDNOTES

1. The Virginia based MSD Company had a supporting role on the EDS Product Assurance team and the testing included network WAN/LAN/server performance, information assurance testing and customer support process verification. Using hardware and software test tools the company technicians measured voice, video, data, and imagery networks' fidelity and performance. The focus was to deliver a complete understanding of traffic's effect on system latency, response time, throughput, and jitter.

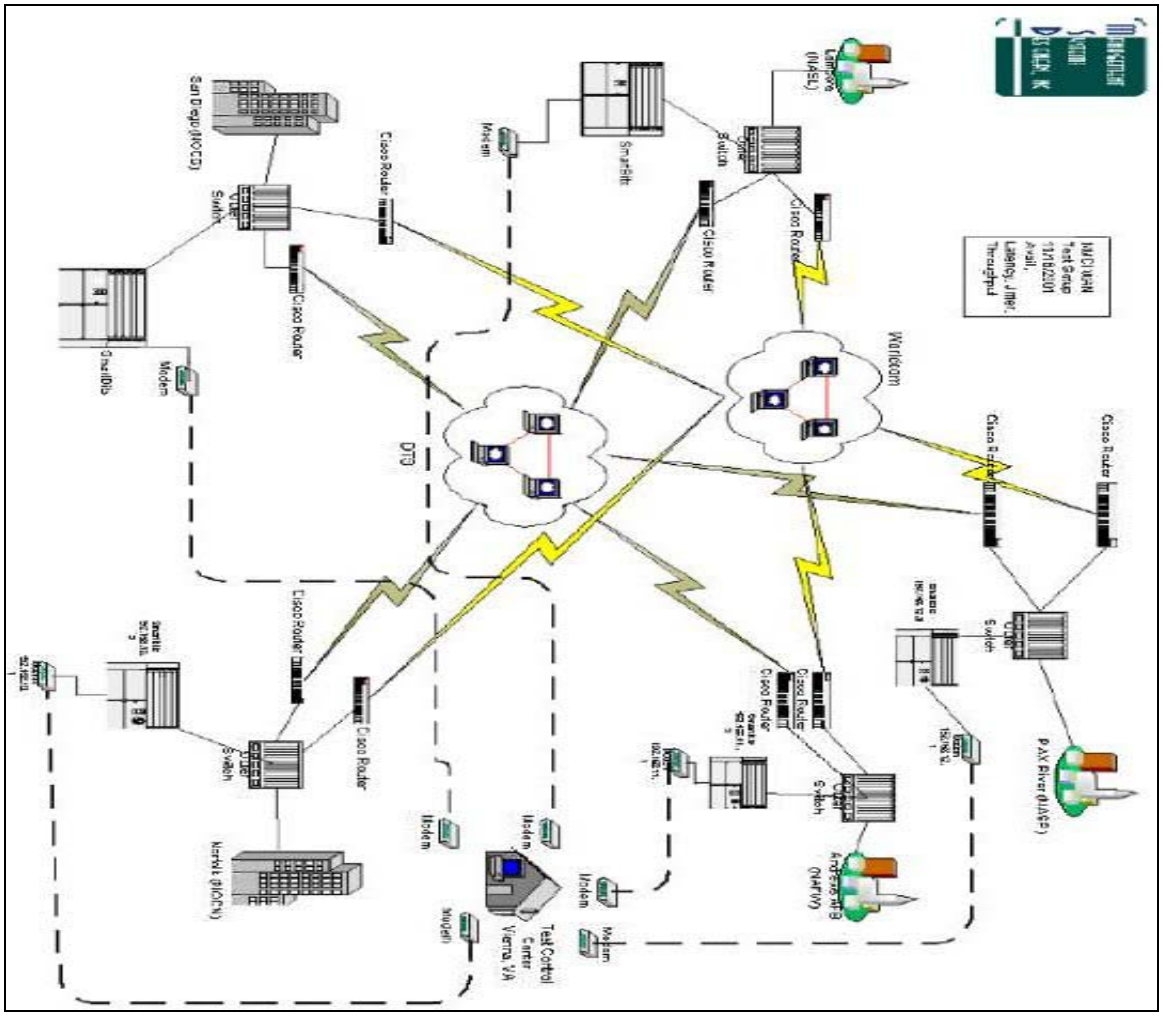


Figure 22: The Initial Testing of NMCI, from www.msdinc.com (NMCI Initial Testing), accessed February 2004

2. DoD has defined three types of architectures: operational, technical, and system. A technical architecture is a set of rules or "building codes" that are used when a system engineer begins to design/specify a system. These rules consist primarily of a common set of standards/protocols to be used for sending and receiving information (information transfer standards such as Internet Protocol suite), for understanding the information (information content and format standards such as data elements, or image interpretation standards) and for processing that information. It also includes a common human-computer interface and "rules" for protecting the information (i.e., information system security standards). The JTA is a document that mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The applicable mandated standards in the JTA are the starting set of standards for a system and additional standards may be used to meet requirements if they are not in conflict with standards mandated in the JTA. The JTA is mandatory to be used by anyone involved in the management, development, or acquisition of new or improved systems within DoD. (www.jta.disa.mil (Frequently Asked Questions Section), accessed February 2004)

III. DATA COLLECTION

A. PROGRESS OF THE NMCI CONTRACT

A draft report of the fiscal year 2003 Defense Appropriations bill cited inadequate testing methods and a failure to identify thousands of legacy systems as lingering concerns for the NMCI project. As the DoN moves closer to its new integrated network, there is a need to clean out thousands of old applications that either fail to meet the NMCI standard software configuration or do not meet the security requirements already established by the DoD. Concerns were also related to the overall budget of the program.

1. Historical Context in the year 2003

The most appropriate authority to provide the recent numbers related with the implementation progress of NMCI is the NMCI Director himself:

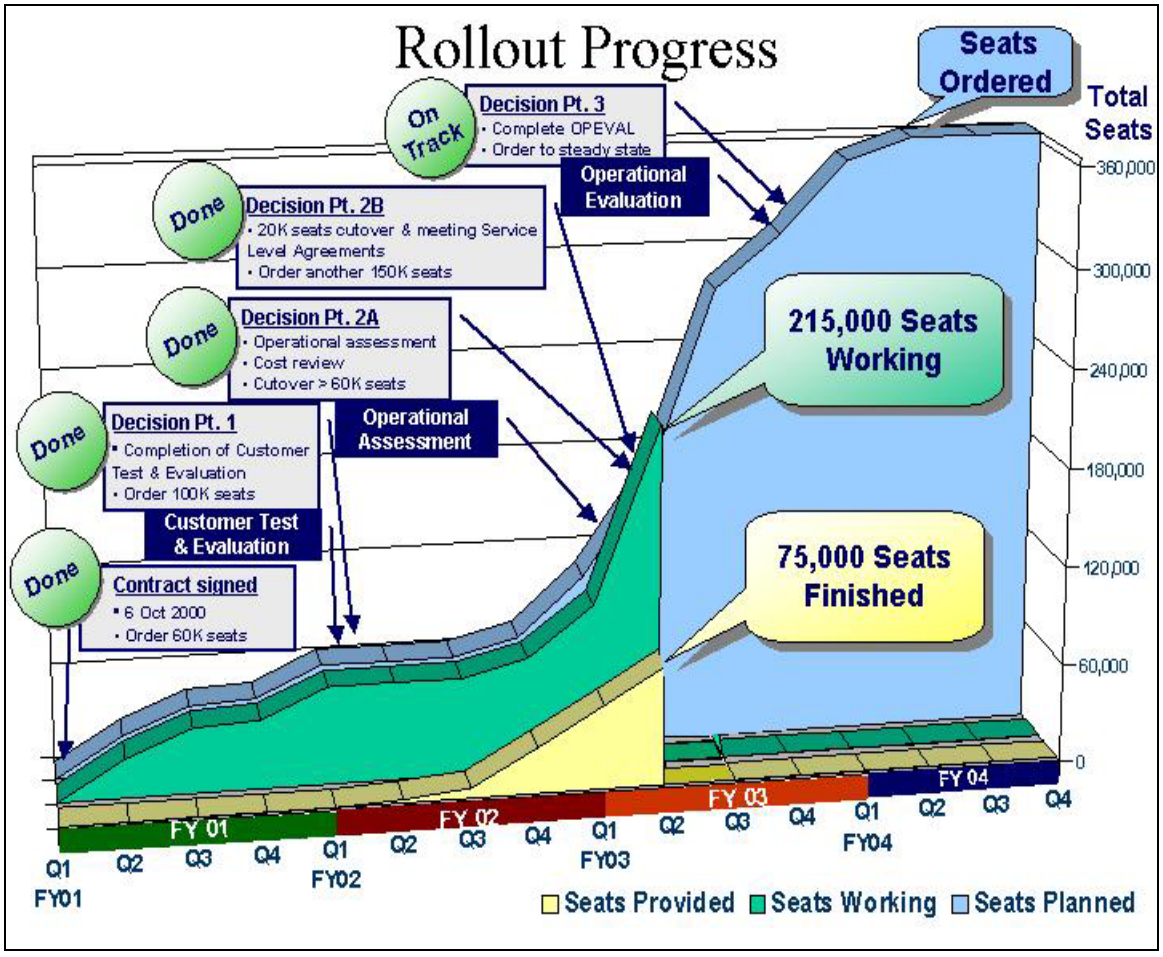


Figure 23: Progress of NMCI, from Rear Admiral Chuck Munns, Director of NMCI, NMCI Progress Briefing, at the NMCI – Industry Symposium 17 June 2003

The implementation process consists of 360,000 seats being moved into the NMCI in three stages. The first step is the official order by the Navy for a specific number of seats. The next milestone is when the Information Strike Force (ISF) assumes responsibility for the site (AOR). The final step is the seat cutover. The term "cutover" describes the point at which NMCI network users each receive a new desktop computer, operating system and software, and are connected to the full network services of the new intranet, including access to the legacy applications that resided on their previous workstations. The ISF, the industry team working on NMCI under the lead of EDS, in late 2002 had assumed responsibility for only 60,000 seats, out of the total goal of seats. Congress and the DoD had capped the size of the network while testing and evaluations were done, but in the end analysis of the results from four months of testing and EDS' demonstrated ability to meet Service Level Agreements on the 20,000 pilot seats clearly removed all the barriers and NMCI was ready to move to the next level.

The Pentagon gave to DoN the "go-ahead" to move as many as 310,000 Navy and Marine Corps IT users to the newly built network in the beginning of the year 2003. The decision came after months of operational testing that was required by Congress before it would allow DoN to proceed beyond the 60,000 user cap that it imposed after concerns surfaced about the program's technical feasibility and cost. With the successful completion of the testing phase, the Navy received approval to proceed with all of the 160,000 seats that had already been approved and to order an additional 150,000 seats. The official report at the end of the testing phase by the director of NMCI concluded:

> The results from four months of testing clearly demonstrated that the NMCI is ready to move to the next level
>
> Rear Admiral Charles L. Munns, U.S.N., Director of Navy Marine Corps Intranet.

However, the "go-ahead" decision, at the beginning of 2003, did not mean that the program had finally achieved a satisfactory seat delivery pace. During the 2nd quarter of 2003, progress was made but the cutover numbers were not adequate enough and there was still a long way towards the end state. The situation could be summarized as:

- Number Sites Active – 300
- Seats in AOR – 210,000

- Seats Cutover – Less than 80,000
- Significant number of dual desktops in place (24% of total- Too High)
- Facilities in place and Capacity:
    - 3 Network Operations Centers (Only two fully operational)
    - 2 Help Desks (With minimal "hands on" experience)
    - 24 Server Farms (Unclassified)- 263 Terabyte
    - 7 Server Farms (Classified)- 41 Terabyte

With a simple comparison with the pre-planned end state, the implementation pace appeared again sluggish.

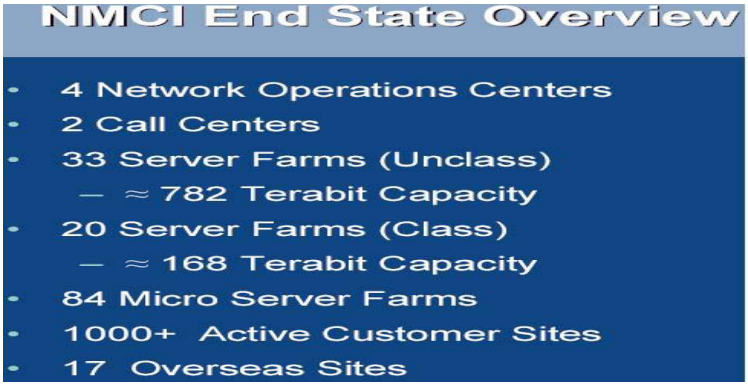


Figure 24: NMCI End-State

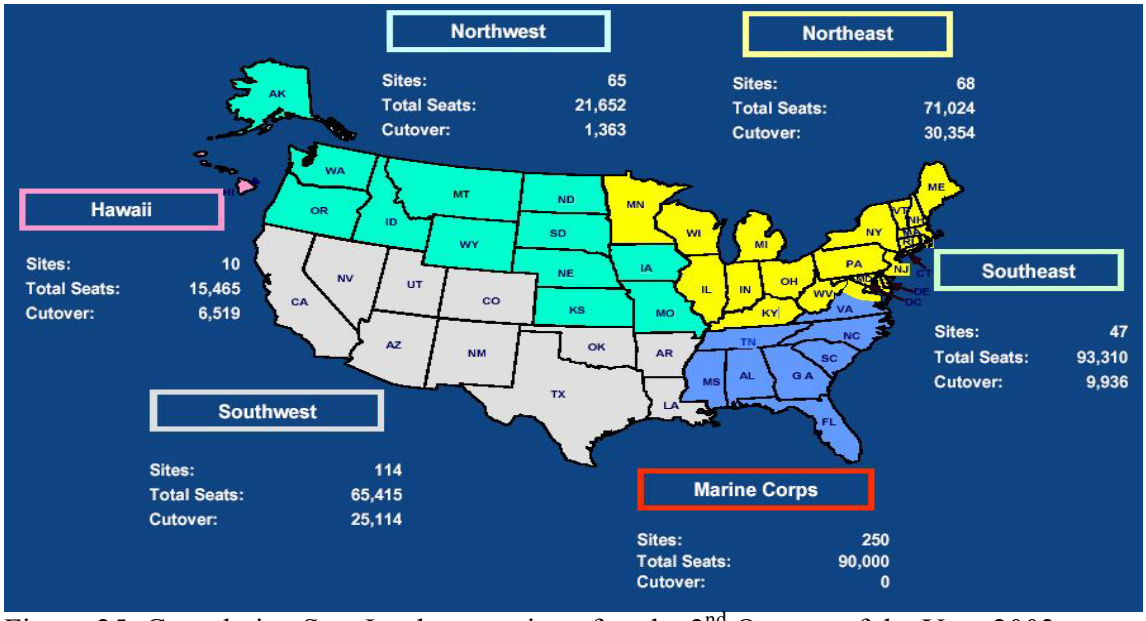


Figure 25: Cumulative Seat Implementation after the 2nd Quarter of the Year 2003

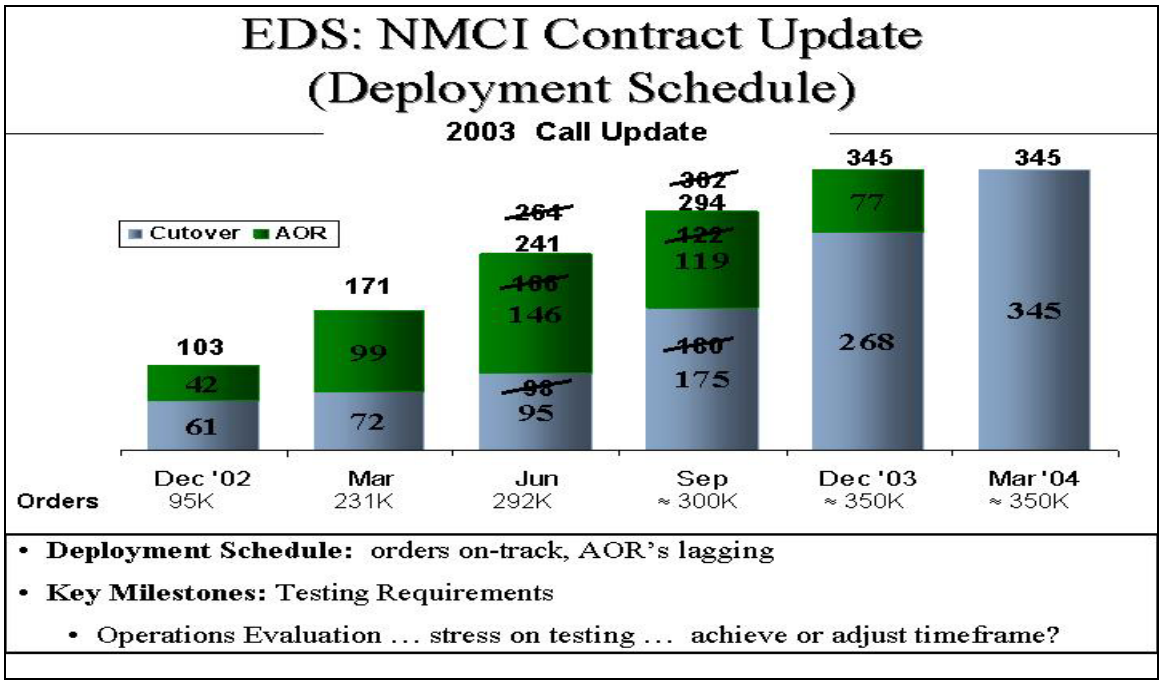


Figure 26: NMCI Progress and Main Concerns, from EDS Profits Review for the Year 2003

But EDS revised the Enterprise Deployment Rollout Plan (EDPP) at the time in place and accelerated the deployment. As of the 2003 fall, the ISF had responsibility for approximately 300,000 seats, with more than 107,000 seats moved to the cutover stage. Three network operation centers are currently fully operational in San Diego; Oahu, Hawaii; and Norfolk, Virginia. An additional network operations center also is in the process of being set up at the U.S. Marine Corps base in Quantico, Virginia, therefore completing the required numbers of NOCs and indicating progress within the USMC's portion of NMCI that had been put on hold by Congress until the completion of the first increment of the Intranet's tests. Help desks are in place in Norfolk and San Diego, with complete functionality and automated tools are deployed to increase performance. The current number of Navy and Marine Corps seats that are now under ISF control has improved significantly.

Snapshot	**27 FEB 04**
Seats in AOR	**303,369**
Seats Cut Over	**160,175**

Table 4: Current NMCI Implementation Numbers, from www.nmci.navy.mil (NMCI Now), accessed February 2004

B. IT SUPPORT AVAILABLE THOUGHT NMCI

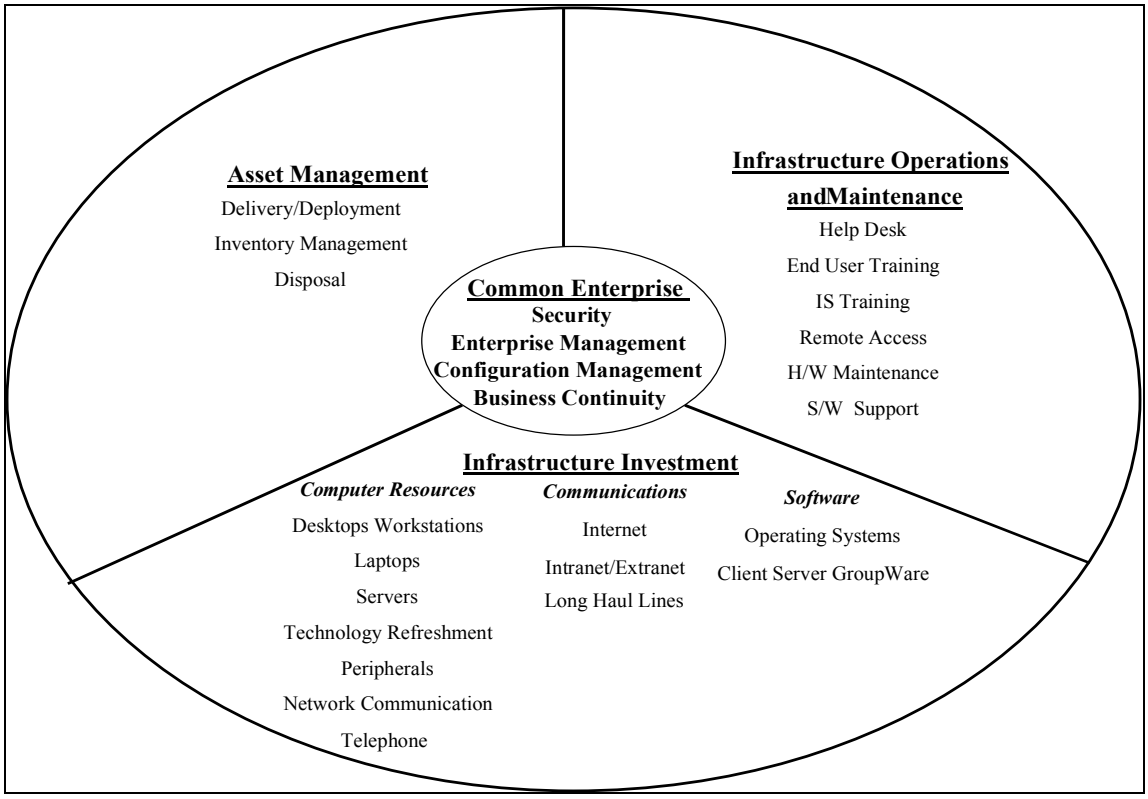


Figure 27: Total Cost of Ownership (TCO) within the Seat Management Framework, from the BCA for the NMCI, p.23

> The **NMCI approach** of a single private sector entity providing IT services under a long-term commercial seat management contract **is a good business decision** compared to the way Naval IT requirements are currently provided. In summary, considering all the dimensions of providing the Navy and Marine Corps war-fighters an optimal IT infrastructure and supporting network, there are more risks, uncertainties and hazards inherent in continuing to do business as usual, versus supporting basic IT services via NMCI.
>
> Conclusion, included in the Bussiness Case Analysis for the NMCI.

DoN has decided that the requirements of NMCI could be provided most efficiently and effectively by a single private-sector vendor providing such IT capabilities as a service under a “seat management" contract. These type of contracts, used widely in the commercial sector, are long-term service contracts under which all required enterprise-wide IT capabilities, including all required infrastructure, are provided and managed by a single contractor. The customer is charged a fixed price per user (“seat”)

for each applicable period (e.g. monthly) throughout the life of the contract, provided that the contractor satisfies certain established service levels in specified performance areas.

The NMCI contract is in keeping with the current federal government business trend of assigning accountability for various IT services to one vendor. The service-level agreements (SLAs) enables DoN to transition from a government-owned and -operated environment to a purchased-service environment in which the contractor provides for the daily operational task of maintaining a robust IT infrastructure. The SLA is a contracting tool keyed to a client's service performance expectations. This means that the client can evaluate the performance of the contractor and the services the contractor is providing. Meeting or beating the customer's expectations will earn the contractor a financial reward; failing to meet expectations results in the contractor earning less money for that phase of implementation.

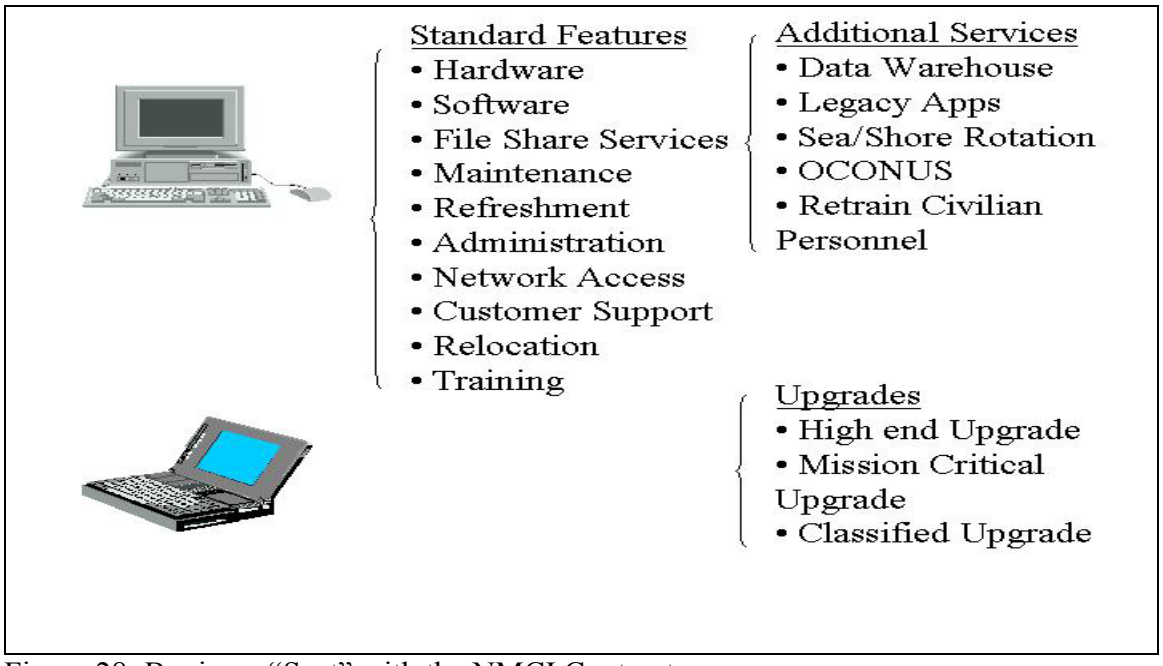


Figure 28: Buying a "Seat" with the NMCI Contract

The NMCI is acquired as a performance-based, enterprise-wide services contract that incorporates future strategic computing and communications capability that is managed like a utility. Service will be paid for, as it is delivered, similar to the concept of telephone utility service that is currently used in the commercial U.S. market. The customer (DoN) chooses from a list of basic and additional or "premium" services and pays for that level of service required or desired. Rather than treating information systems

as products that must be developed, maintained and upgraded in house, the Navy is "utilizing" commercial experts to provide the equipment, training, expertise and support as a service package for a set cost per user.

The NMCI contractor must support a mix of large, medium, and small sized activities with dissimilar business functions. To make this task feasible, the contractor is expected to leverage economies of scale by developing standardized hardware and software platforms, as well as consolidating services within the same geographical location. Each computer that is connected in the NMCI is described under the term "seat", while users have the ability to access the network from any type of seat available to them and not just from their "private" desktop.

CLIN	TITLE
0001AA	**Fixed Workstation - Red Seat - $2958.12 per year**. Pentium III 800MHz Provides performance for use with 2-D and light 3-D graphics or engineering-related applications, applications that require additional processing capability.
0001AB	**Fixed Workstation - White Seat - $2863.68 per year**. Pentium III 733MHz Ideal for the typical user of Microsoft Office Professional software.
0001AC	**Fixed Workstation - Blue Seat - $2788.08 per year**. Celeron 566MHZ. Provides adequate performance for daily office productivity applications. Ideal for administrative functions.
0001AD	**Fixed Workstation - Thin Client - $2335.92 per year**.
0002	**Portable Seat - $3699.00 per year**. Dell Lattitude C600. Provides excellent performance for office productivity software. Supports users needing remote access to NMCI. Makes high-quality presentations while on travel.
Actual Hardware Changes with Commercial Market Pace, NMCI Price Remains Fixed	

Figure 29: CLINs establishing the description of "Seats", from the first version of the NMCI contract

NMCI is by far the largest seat-management contract, and it includes not only the introduction of seats but also the supporting infrastructure on the bases and all the connectivity between and among any type of Naval installation ashore. Consolidating network management functions under the network operations centers (NOCs), aims to allow better management and utilization of security resources, configuration management

and network performance monitoring capabilities. Service desk functions will also be centralized, to provide more efficient "one-stop" support to end-users. In other words, this is an end-to-end, total service being ordered by the DoN.

1. Hardware Performance and Upgrades

KEY SYSTEM FEATURES

	Processor	Memory	Storage	Monitor
HIGH-END	Highest speed shipped in Opti line in volume (cum. vol. > 10k units)	80th percentile shipped w/ Dell *performance* Opti systems		Same as RED seat
RED	80th percentile of ALL Opti systems	80th percentile shipped w/ Dell *mainstream* Opti systems		
WHITE	Next best performance level below RED seat			
	Processor speed	Memory quantity (typically one-half)	Disc quantity (same drive speed if avail.)	Same as RED seat
BLUE	80th percentile of ALL Opti INTEL value chipset systems	80th percentile shipped w/ Dell *value* Opti systems (not exceeding WHITE seat performance)		Same as RED seat

Figure 30: Seat Division within the NMCI Contract

Performance of the hardware used is correlated with the importance of the functionality required and mission supported by the end user. Dell Company is providing complete IT systems for NMCI according to the above technology insertion matrix in order to ensure adequate technology refresh. Dell is also partly responsible for installation accuracy. The ISF provides Dell with a load set to install on each machine equipped with Microsoft Windows 2000 and Office 2000. When the systems arrive at the Navy and Marine Corps sites, they are pre-configured and NMCI-certified. Upgrades, modernization, and technology refreshment will occur over the NMCI contract life cycle.

2. Software

Standardized operating system (OS) and application packages are supported by NMCI through the use of COTS products to every possible extend, although some modification to the standard application packages may be necessary depending upon

unique DoN requirements. Software platforms are required to be within one year of the current service pack or major release. Client applications include e-mail capability, NIPRNet/Internet connectivity, database functions, spreadsheets, graphics and word processing functions, anti-virus software, and calendar applications.

Additionally, the number and functions of servers should also be consolidated, eliminating redundant platforms in order to optimize maintenance and support processes and provide the high level of service as designated by the SLAs. The application servers must be fully integrated with the workstation environment and processes facilitating administrative activity, such as automated software distribution, virus inoculation, detection and repair, should be present. Network management capabilities should include configuration and change management, inventory management and acquisition tools, centralized user account management, security functions, life cycle management, backup and disaster recovery capabilities and the ability to remotely access end user machines from network management stations.

Features	Benefits	Aim
Customizable Help and Alerts	Desktop administrator customizes online help based on prior history of help desk support calls.	Reduces or eliminates help desk support calls.
Self-Repairing Applications	Automatically detects and repairs errors without a user even knowing about them.	Decreases end-user downtime and eliminates need to call help desk. Reduced peer-to-peer support.
Install-on-Demand	Improves desktop manageability	Fewer custom installations decrease deployment costs. Reduced help desk costs since components install automatically.
Intelligent User Interface	Customizable and intelligent user interface simplifies daily tasks.	Easier completion of routine daily tasks

Table 5: Administrator's Software and Capabilities, from the BCA for the NMCI, p. 75

In Table C, in Appendix C there is the revision history of the software associated with the NMCI implementation. The standardized software package that is currently in place with every NMCI seat is often described as "*Gold Disk*". The products full list follows:

Gold Disk Contents

GOLD DISK CONTENTS		
SERVICE	**SOFTWARE DESCRIPTION (MINIMUM VERSION)**	**VENDOR**
Basic		
Operating System	MS Windows 2000 SP3	Microsoft
Office Suite	Standard Office Automation Software Included on the Gold Disk: • MS Word • MS Excel • MS PowerPoint • MS Access	Microsoft
Desktop Management	Diskeeper 7.0413	Executive Software
E-mail Client	MS Outlook 2000	Microsoft
Internet Browser	Internet Explorer MS 5.5 SP-2 128bit	Microsoft
Virus Protection	Norton A/V Corp Edition v7.5	Symantec
PDF Viewer	Acrobat Reader v5.05	Adobe
Terminal Emulator - Host (TN3270, VT100, X-Terminal)	Reflection 8.0.5 – Web Launch Utility	WRQ
Compression Tool	WinZip v8.1	WinZip
Collaboration Tool	Net Meeting v3.01 (4.4.3385)	Microsoft
Multimedia	RealPlayer 8 (6.0.9.450)	RealNetworks
Multimedia	Windows Media Player v9	Microsoft
Internet Browser	Communicator 4.76	Netscape
Electronic Records Mgmt	Trim Context	Tower
Plug-ins		
Web Controls	Macromedia Shockwave v8.0	Macromedia
Web Controls	Flash Player 5.0	Macromedia
Web Controls	Apple QuickTime Movie and Audio Viewer v 5.0	Apple
Web Controls	iPIX v6,2,0,5	Internet Pictures

Security Apps

Security	Intruder Alert v3.6	Symantec
Security	ESM v5.1	Symantec

Agents

Software Management	Radia Client Connect v.2.1	Novadigm
Inventory, Remote control	Tivoli TMA v3.71	IBM/Tivoli

Remote Connectivity (Notebooks)

Dial-up connectivity	PAL v4.3	MCI/WorldCom
VPN	VPN Client v4.1	Alcatel

Table 6: Contents of the "*Gold Disk*", from www.nmci-isf.com (Gold Disk Contents), updated on the 15th of December 2003, accessed February 2004

Because this thesis will provide recommendations for the information security (INFOSEC) and information assurance (IA) policies [Note 1] related to NMCI in the chapters that follow, a detailed description of security related software will be provided in this section. Symantec Corp. has been awarded a contract from EDS to help secure NMCI in the early years of the contract, in March 2001. Under terms of the agreement, Symantec provides a significant portion of the security components including firewall, virus protection, content filtering, vulnerability assessment, and intrusion detection solutions to safeguard the IT services provided. Under a subcontract from EDS, Raytheon is responsible for the overall network security and information assurance of the network. In implementing NMCI, the full complement of Symantec security solutions is utilized. With Norton AntiVirus at each desktop, NMCI has automatic protection against viruses and other malicious code as well as centralized anti-virus policy management to facilitate administration and enhance security.

Symantec Intruder Alert version 3.6 is a host-based, real-time intrusion monitoring system built with the purpose to detect unauthorized activity and security breaches and respond automatically, if the case arises. It includes specialized software agents that support server platforms running Windows 2000 and Windows Server 2003 Enterprise Edition and can be configured to monitor Web or database applications

running on servers. If Intruder Alert detects a threat, it will sound an alarm and initiate countermeasures according to the pre-established security policies. From a central console, administrators can create, update, and deploy policies and securely collect and archive audit logs for incident analysis. As a complement to firewalls and other access controls, Intruder Alert enables the development of precautionary security policies that prevent expert hackers or authorized users with malicious intent from misusing systems, applications, and data. The focus is on: (www.symandec.com (Intruder Alert), accessed February 2004)

- Monitoring systems and networks in real time in order to detect and prevent unauthorized activity
- Enabling the creation of customizable intrusion detection policies and responses
- Enforcing policy with the automatic deployment of new policies and updated detection signatures
- Delivering network-wide responses to security breaches from a central management console
- Providing audit data for incident analyses and generating graphical reports for both host and network intrusion detection activity
- Complementing firewalls and other access control systems with no impact on network performance

Intruder Alert has the aim to enhance the control over systems with policy-based management that determines which systems and activities to monitor and what actions to take, as well as with real-time intrusion detection reports for both host and network components. Administrative wizards perform many routine tasks and silent installation and remote tune-up capabilities make it easy to deploy and maintain the system. Intrude Alert ingrates with the Symantec Enterprise Security Manager™ (ESM).

Symantec ESM is an automation tool for the discovery of security vulnerabilities and deviations of the security policy in mission critical e-business applications and servers across the whole enterprise from a single location. It provides enterprise-class

tools that allow administrators to create security baselines for every system on the network and measure performance against those baselines to ensure that devices are properly configured and being used in accordance with policies. With the appropriate tools, administrators can quickly and cost effectively create and manage online security policies and user-defined security domains, identify systems that are not in compliance, and correct faulty security settings on systems at any location to bring them back into compliance.

Because Symantec Enterprise Security Manager integrates with the Symantec Security Management System, it can also leverage advanced management capabilities that provide improved overall security posture. Within the framework of the Symantec Security Management System, policy compliance data collected and analyzed by ESM can be correlated with security event data from a multitude of sources, including firewalls, intrusion detection systems, and vulnerability assessment products. And, the central logging, alerting, and reporting functions of the Symantec Security Management System can be combined with the correlation, risk prioritization, and management capabilities of Symantec™ Incident Manager to build a holistic, proactive security system. This enables organizations to respond rapidly to incidents, contain and eradicate threats faster, and utilize the full potential of their security systems. Key features include: (www.symantec.com (Enterprise security Products), accessed February 2004)

- Large number of specific security checks to help ensure that mission-critical information systems comply with an organization's security policies.
- Easy retrieval and deployment of security updates with Live Update ™technology.
- Integration with other Symantec Security Management System products to ensure a more holistic understanding of security risks and priorities.
- Measurement and reporting on compliance with industry standards and government regulations.
- Wide platform and application coverage.

- Customizable security policy support.
- Focuses on proactive security to ensure the maintenance of business operations.

3. Services Provided

The NMCI offers the required IT services under the framework of a single network, which is easier to manage and more secure, and enables military personnel to focus on their defense mission rather than information technology acquisition and support. A breakdown of the current data seat services within NMCI is shown in Figure 31:

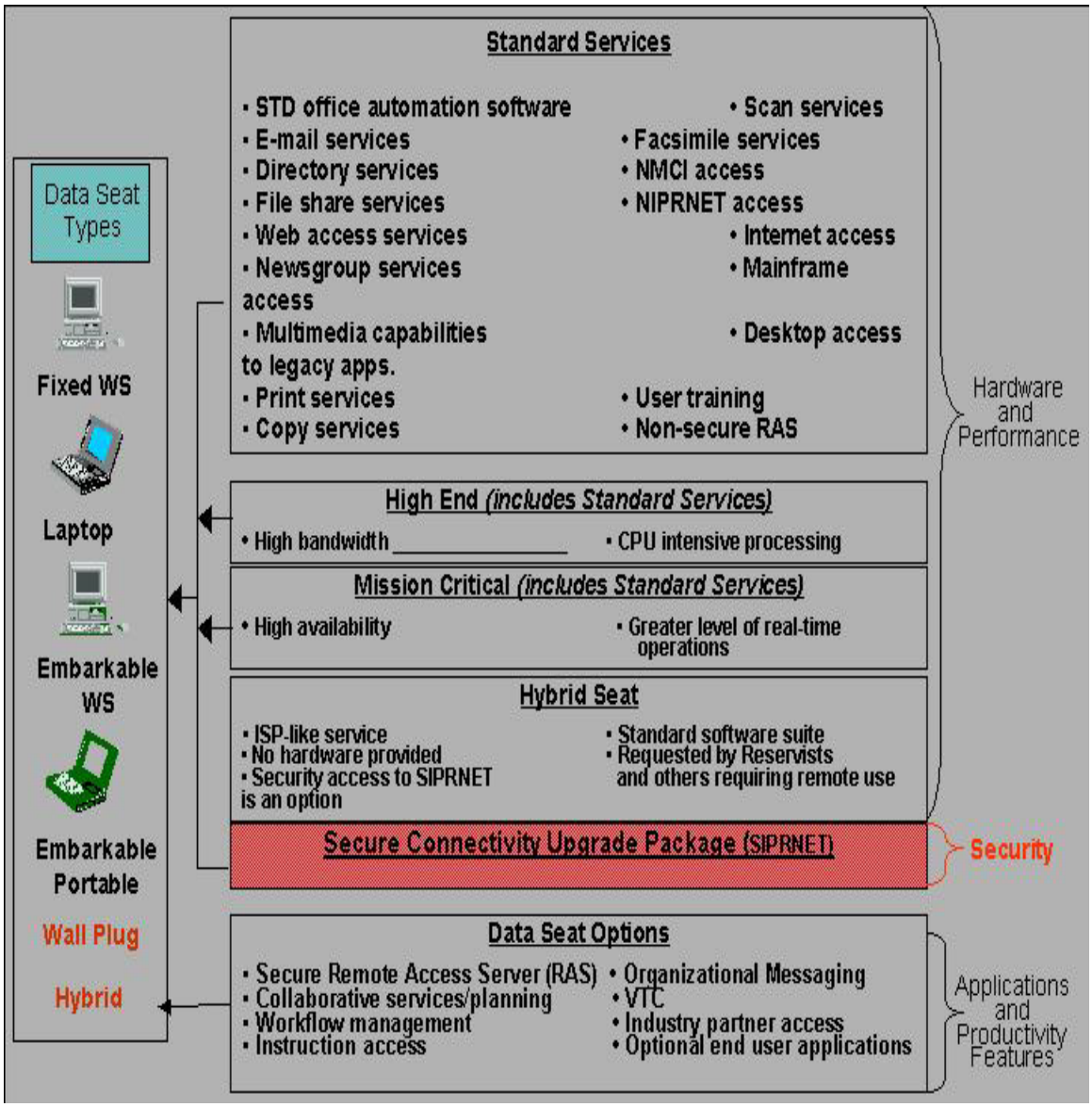


Figure 31: Breakdown of Data Seat Services

The domain of NMCI's "Basic Services" includes the following:

- Security services (firewalls, intrusion detection, encryption)
- WAN access (DISN, Commercial WAN, internet)
- Infrastructure (Voice video, & data transport)
- Joint and industry network interoperability
- Pier services (connectivity, NOC/JFTOC interface)
- Enterprise functions (Help Desk/Tech support)
- Network management services
- Desktop hardware (standard, high-end, and laptop)
- Desktop software (standard software suite)
- Organizational messaging (AUTODIN, Defense Message System (DMS))
- Training
- Directory services
- E-mail
- Remote telephone access
- Domain name service
- Help Desk/Tech support
- LAN (building LANs)
- System management services
- Telephony – Switched telephone networks
- Telephony to the desktop

(Navy Marine Corps Intranet Site Deployment Guide Version 1.2, 07 March 2003, p. 40)

C. NMCI SECURITY AND INFORMATION ASSURANCE POLICIES

The NMCI security policy supports the five fundamental information assurance elements (confidentiality, integrity, availability, authentication and non-repudiation) and establishes how the NMCI will manage, protect, and distribute sensitive information. The directive case (DC) security policy statements are derived from the appropriate DoD and DoN IT directives and instructions to which the NMCI must adhere by virtue of its existence as a DoN information system.

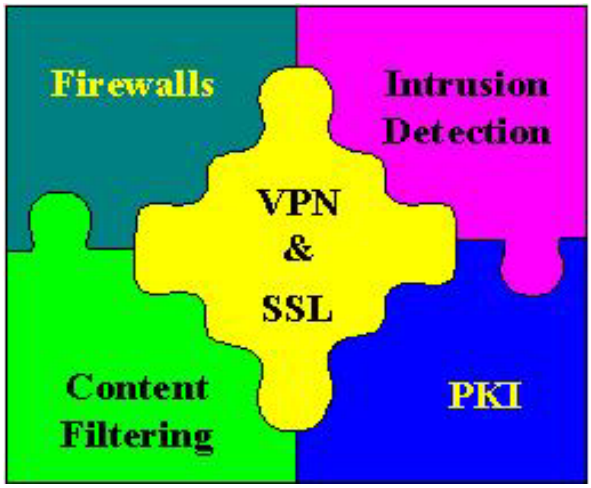


Figure 32: NMCI Security Components and Interactions

NMCI complies with DISN security policy and DISA requirements for connection to the SIPRNET. Security services provided for/within the NMCI implement Computer Network Defense (CND) initiatives such as Information Operations Condition (INFOCON) directives and Information Assurance Vulnerability Alert (IAVA) notices, and effort is made to integrate within the existing DoD and remaining of DoN CND infrastructure. Preference is given to COTS IA and IA-enabled IT products evaluated and validated, as appropriate, in accordance with one of the following:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement
- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program

- The NIST Federal Information Processing Standard (FIPS) validation program

(NMCI Contract N00024-00-D-6000, (Conformed Contract P00080), Attachment 5, p.7)

1. A Brief Introduction into Public Key Infrastructure (PKI)

PKI is a set of standards for applications that use encryption and is often called *trust hierarchy.* It is a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in a Web transaction. Public Key Infrastructure (PKI) is the term generally used to describe the laws, policies, standards, and software that regulate or manipulate digital certificates and public and private keys.

Figure 33: PKI Definition

Figure 34: Private and Public Keys

The DoD introduced PKI with the following capabilities in mind:

- Secure Unclassified E-mail (Sign, Encrypt and Decrypt) using digital certificates.
- Certificate-Based client-server “Mutual” Authentication
- Certificate-Based Authentication to Unclassified Web Applications
- Secure Encrypted Communications/Transactions Between Client and Web Servers Using SSL
- Certificate-Based Network Logon

The digital certificate is simply an attachment to an electronic message used for security purposes. The most common use of the certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or more commonly on the Internet.

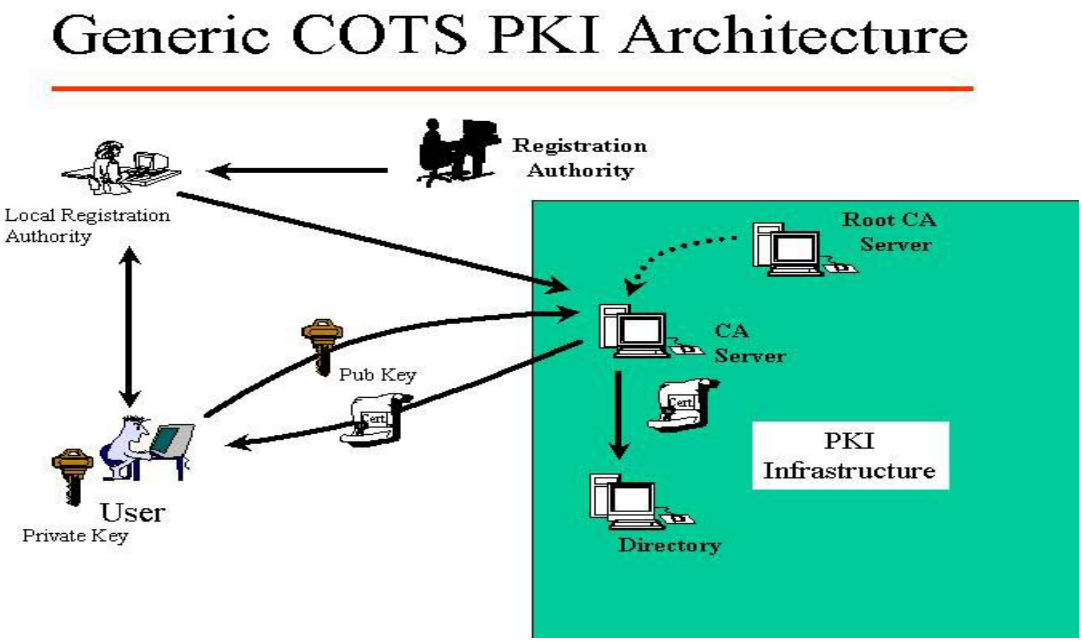


Figure 35: PKI Architecture

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. The most widely used standard for digital certificates is X.509.

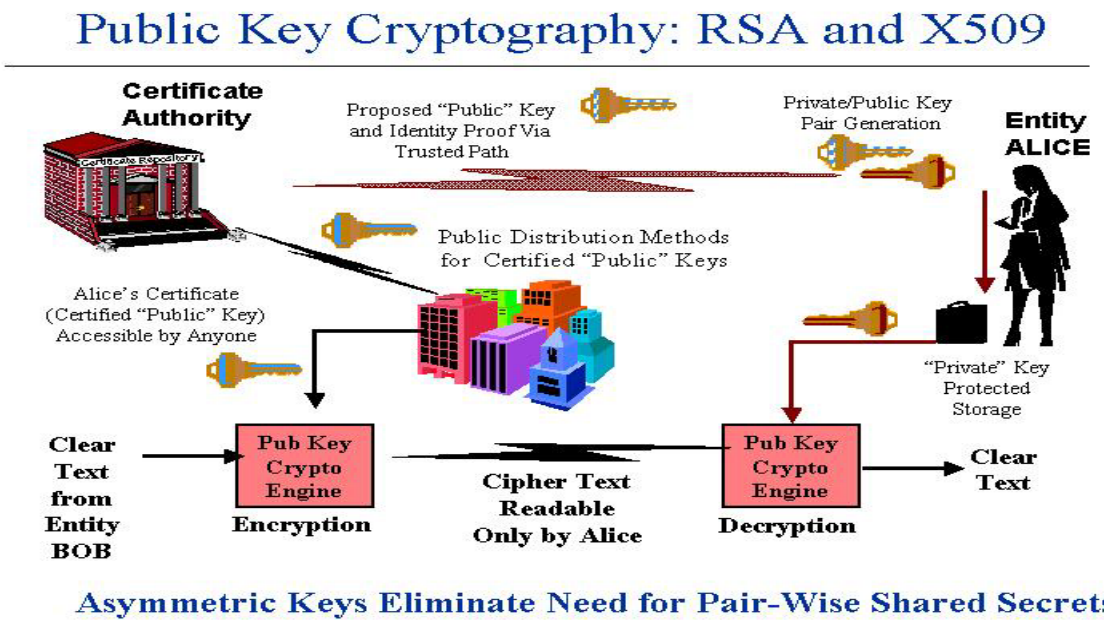


Figure 36: Public Key Cryptography

Within the NMCI, a PKI certificate is an electronic "document" officially linking a user's identity with his/her Public key. There are three types of PKI certificates:

- Identity: Digitally sign documents or electronic forms. Also used to authenticate the user to specific applications.
- E-mail Signature: Digitally sign e-mails
- E-mail Encryption: Digitally encrypt e-mail messages

(NMCI Public Key Infrastructure (PKI) User Guide, 2nd July 2003, p. 2)

The driver for the approach to implement DoN wide infrastructure to support PKI is to enhance the security posture of NMCI through the use of the already PKI posture established by DoD to:

- Enable end user cryptographic logon to NMCI

- Enable client authentication to private DoD websites
- Digitally sign all e-mail messages originated from Mission Assurance Category (MAC) I and MAC II systems, as well as all e-mail messages where the sender or recipient requires data integrity and/or non-repudiation.
- Encrypt Private and/or Sensitive But Unclassified e-mail.

2. Understanding Secure Socket Layer (SSL)

The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the Internet. [Note 2] SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. (www.Searchsecurity.com (SSL Definition), accessed February 2004)

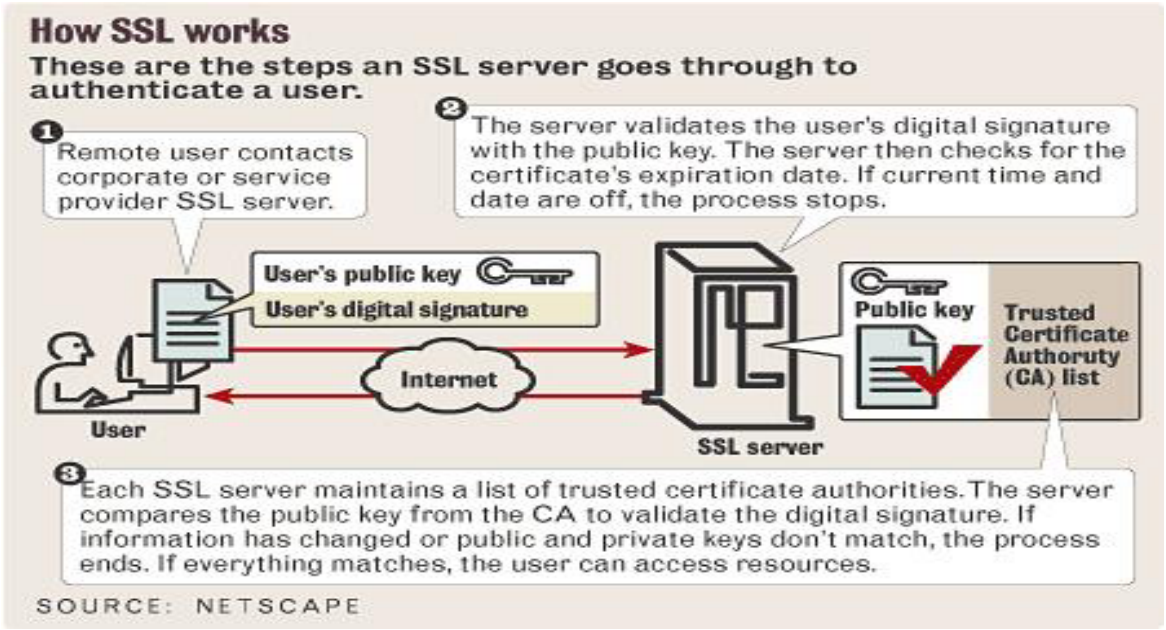


Figure 37: How SSL Works, from the Netscape Corp.

3. Defense in Depth Strategy

NMCI employs a defense-in-depth (DiD) strategy to mitigate the risk associated with a single point of failure. Available protection technologies are employed in a layered system of defenses. To this end, attacks directed against systems within NMCI's defined network boundaries are met by a series of protection mechanisms including, but not limited to, encryption, intrusion detection systems, access control, user identification and authentication, malicious content detection, audit, physical and environmental controls. Use of these mechanisms is intended to mitigate inherent system vulnerabilities and counter potential threats. The number and type of defense mechanisms used in each boundary layer is a consequence of the protective qualities of the device and the assigned value of the information within the protected enclave.

Content security-checking mechanisms to scan for malicious code are implemented via the NMCI approach for all connecting networks, systems and subsystems. All NMCI information systems are monitored to detect, isolate, and react to intrusions, disruptions or denials of services, or other incidents that threaten the security of the network. NMCI shall follows an enterprise-wide IA architecture that implements a DiD approach to incorporate multiple protection schemes at different levels to establish and maintain an overall acceptable IA posture across the NMCI.

These boundaries are:

- Boundary 1: Logical Boundary between NMCI and External Networks.
- Boundary 2: Logical Boundary between NMCI and Communities of Interest (COIs). These COIs could be at Metropolitan Area Network (MAN)/Base Area Network (BAN)/Local Area Network (LAN) level, or between different organizations or functional groups.
- Boundary 3: Logical Boundary between COIs and Host level I.
- Boundary 4: Final Layer of Defense: Application/Host Level.

Corresponding to the discussion of boundaries within the NMCI is a distinction of layers of defense implemented as part of DiD strategy.

- Layer 0: Demilitarized Zone (DMZ). Communication between the NMCI and public networks that is not afforded the same degree of protection provided by an integrated network security suite.
- Layer 1: External boundary level protection. Communication provided between the NMCI and external networks such as NIPRNet/INTERNET or SIPRNet.
- Layer 2: Communication internal to the NMCI.
- Layer 3: Communication within COIs in the NMCI without the use of a Virtual Private Network (VPN)
- Layer 4: Communication within COIs in the NMCI with the use of VPN
- Layer 5: Application/Host Level

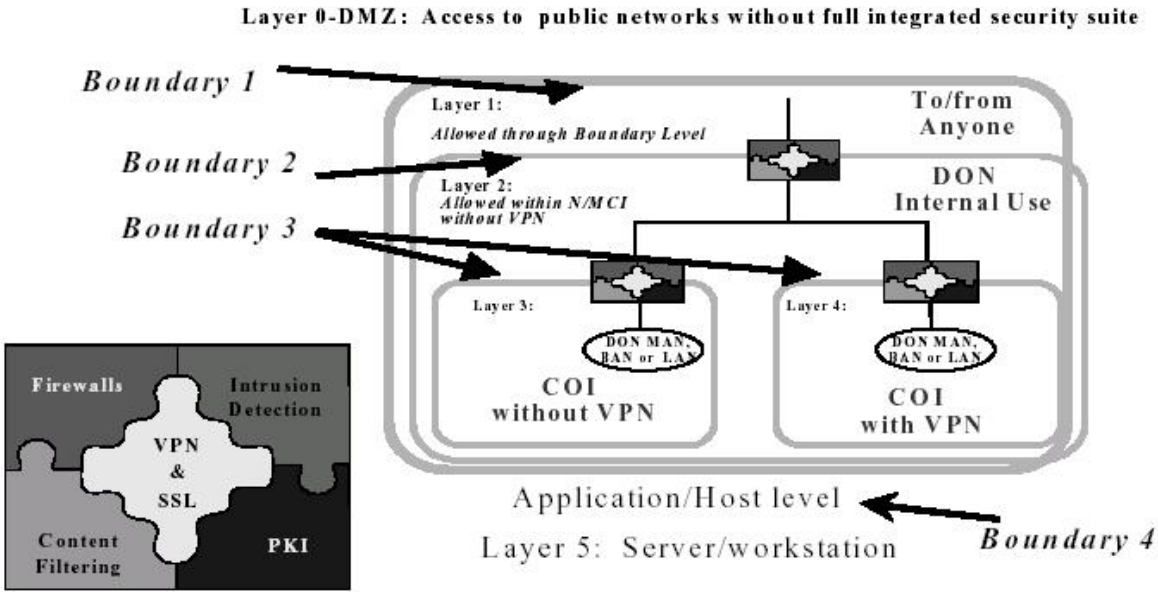


Figure 38: NMCI Layered Defense, from the NMCI Contract N00024-00-D-6000, (Conformed Contract P00080), Attachment 5, p.6)

Because government and especially military networks pose an attractive target and are attacked constantly, the NMCI must be fully prepared to respond. Under the NMCI and along with the increased security approach, DoN will have total visibility of the operational network for both setting strong procedures to detect, respond and guard against outside attack and ensuring information assurance for every user.

D. SUMMARY AND CONCLUSIONS FOR THE CURRENT STAGE OF THE NMCI IMPLEMENTATION

1. The Current Progress of Seats Delivered

Now entering its fourth year of implementation, the NMCI program has experienced a rather difficult start and unexpected squalls in its adaptation of commercial processes. The obvious conclusion from the figures related with the NMCI implementation is that the total numbers of seats that have achieve the "cut-over" under the NMCI environment up to now, is still not enough to deliver the full NMCI promise to the end-users.

The financial house of experts "Morgan Stanley" on October 2003 issued a report on the NMCI progress- EDS's profitability and the conclusions related to the NMCI effort could be described only as bad. According to the 23-page report, the analysts gave the company less than a 1 percent probability of meeting current [fourth-quarter fiscal 2003 and first-quarter fiscal 2004] accumulated cutover seat targets, given current cutover seat rates averaging 290 per day [during the past nine months], compared with 1,500 seats per day required to achieve its stated objectives and profitability. The EDS Corp. attributed the loss of profits to the decline in the average seat price based on the types of seats ordered and expected to be ordered by the DoN, as well as a reduced period of time in which to generate seat revenue due to deployment delays and associated incremental estimated operating costs. However, the report concluded that the year 2004 could be a pivotal year for the company and the project, as EDS will have ample opportunity to improve NMCI's free cash flow generation.

On the good news front, the program is now more mature with the entire requirements fully understood and crystallized by the client. The team supervising the implementation effort has now enough experience with the complex nature of the problems involved and the spiral approach for seats deployment that is now in place facilitates solving of technical issues in a more coordinated manner than the previous linear approach. Additionally, the EDS-ISF team has been flexible and always found ways to move around technical difficulties. More important is that within the year 2004 DoN is expecting to complete the operational evaluation of the network and enjoy the full technical capability and IT support by the ISF.

> The NMCI progress is obviously slower than we had anticipated. Going forward what we intend to do is separate the reporting on the Navy contract from the rest of our operations to give everybody a much cleaner picture of the base business, as well as a lot of transparency on the Navy contract itself.
>
> Michael Jordan, EDS president and chief executive, commenting the year 2003 economic results of EDS Corp

EDS officials announced on the 5th of February 2004 that they would separate the company's reporting on its earnings and its reporting on its DoN related business, because the company executives feel that losses caused by NMCI aren't reflective of the company's overall performance. EDS had to revise the NMCI rollout plan in midstream because the company was spending a lot of money, time and effort to roll out far fewer seats than it had anticipated. The revised deployment schedule, according to Jordan, requires that EDS will write down deferred construct costs of $559 million.

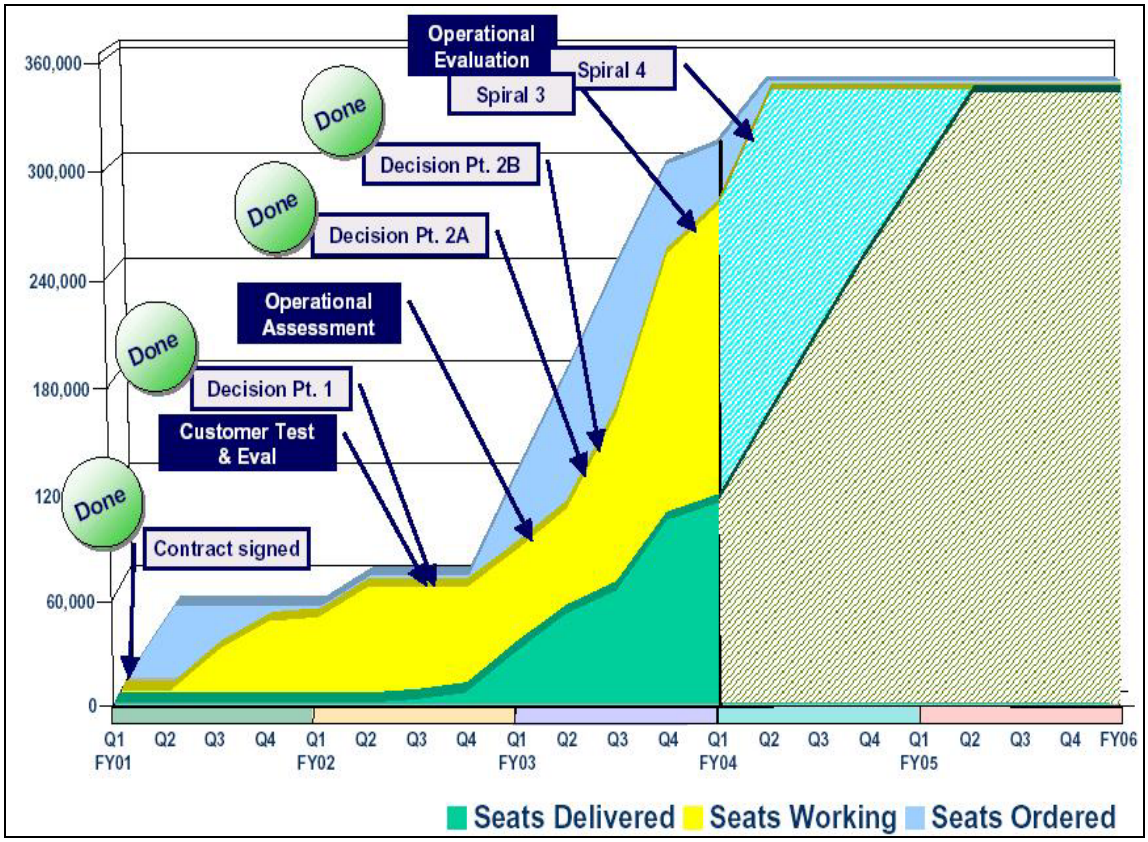


Figure 39: Current State of NMCI Seats, Rear Admiral Chuck Munns, U.S. Navy, NMCI Director, NMCI Briefing, at the SPAWAR Industry Day, San Diego-USA, 23rd October 2003

a. The NMCI Budget

In order to evaluate better the potential cost of NMCI against a comparable baseline, the Department has performed a Business Case Analysis (BCA). The "as-is" [Note 3] environment identified 335,000 current "seats" (as of FY 1999) throughout the DON and an average annual cost of $4,582 per seat. That implied a funded base of support for NMCI-like IT requirements of at least $1.5 billion annually. The fiscal 2003 budget called for $646 million, based on adjustment through the "reward-penalty" model of the SLAs.

NMCI Budget Summary
(in millions of dollars)

Account	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005
Operation & Maintenance, Navy	119.6	577.0	679.8	679.8	679.8
Operation & Maintenance, Marine Corps	0	70.1	280.5	280.5	280.5
Operation & Maintenance, Navy Reserve	19.8	131.3	183.2	183.2	183.2
Operation & Maintenance, Marine Corps Reserve	0	7.2	28.4	28.4	28.4
Environmental Restoration, Navy	0	.6	.7	.7	.7
Research, Development, Test & Evaluation, Navy	7.0	9.6	9.8	9.8	9.8
Military Construction, Navy	0	8.2	9.4	9.4	9.4
Family Housing, Navy & Marine Corps	0	.7	1.0	1.0	1.0
Base Realignment & Closure	0	1.0	1.1	1.1	1.1
Working Capital Fund	109.8	248.5	269.0	269.0	269.0
Defense Health Program	0	.1	.5	.5	.5
NMCI Total	256.1	1,054.3	1,463.4	1,463.4	1,463.4

Table 7: The NMCI Budget Summary, from the NMCI Report to the Congress, p. A-3

The Pentagon has given approval to the DoN to seek funding of $1.1 billion for the Navy Marine Corps Intranet in the fiscal 2004 budget, a markup of nearly $500 million from the fiscal 2003 budget. President Bush signed on the 24th of November 2003 the National Defense Authorization Act for fiscal 2004, authorizing the DoD budget for the current fiscal year. However, the federal government's General Accounting Office (GAO) said in late December 2003 that sloppy accounting practices

by the DoD led to a $1.6 billion discrepancy between two keys IT budget reports for fiscal 2004. (www.computerworld.com (GAO says inaccuracies in 2004 Pentagon IT budget), accessed February 2004) Topping the list of projects with inconsistent budget figures was the NMCI program. GAO determined that about 95% of the total dollar difference between IT budget requests from the DoN ($581M) could be attributed to the NMCI initiative. The GAO attributed the budget discrepancies to what it called "insufficient management attention" as well as ambiguities in the Defense Department's internal regulatory processes, including those for ensuring consistency between reports. For those who are not convinced about the NMCI initiative value, conclusions like that is the perfect ammunition to strike back, because the program appears over budget.

> Major initiatives do not consistently use the same type of appropriations to fund the same activities. To fund the same types of activities, some DoD organizations used the research, development, test and evaluation appropriations, and others used the operation and maintenance appropriations.
>
> Conclusion, included in GAO's Report *Improvements Needed in the Reliability of Defense Budget Submission* to the Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services, House of Representatives, December 2003.

However, it should be noted that it is crystal clear from the public announcements made by EDS relating to the reduced stream of NMCI expected profits that the SLA model works in favor of the DoN. Additionally, the fact that there are still discrepancies on budgeting and accounting procedures after all those years of improving visibility of the accounting systems is a proof that DoN needs NMCI to improve the accuracy of its budgetary data and reporting, because this IT initiative will allow network and IT infrastructure costs to be listed as separate expenses, rather than lumped into command operating budgets.

NMCI is a strategic approach that will enable the entire spectrum of DoN agencies to effectively communicate in the modern age. USN and USMC have recognized that intranets have become major communications tools for any type of activity in the 21st century and understood the value of a unified network organized and

managed at the Department/Enterprise level. NMCI has a proven Return On Investment (ROI) for the DoN and is expected to afford significant improvements in overall capability, connectivity, security and effectiveness of IT systems, benefits that are not possible to described through financial termilogy or easily captured in a spreadsheet matrix.

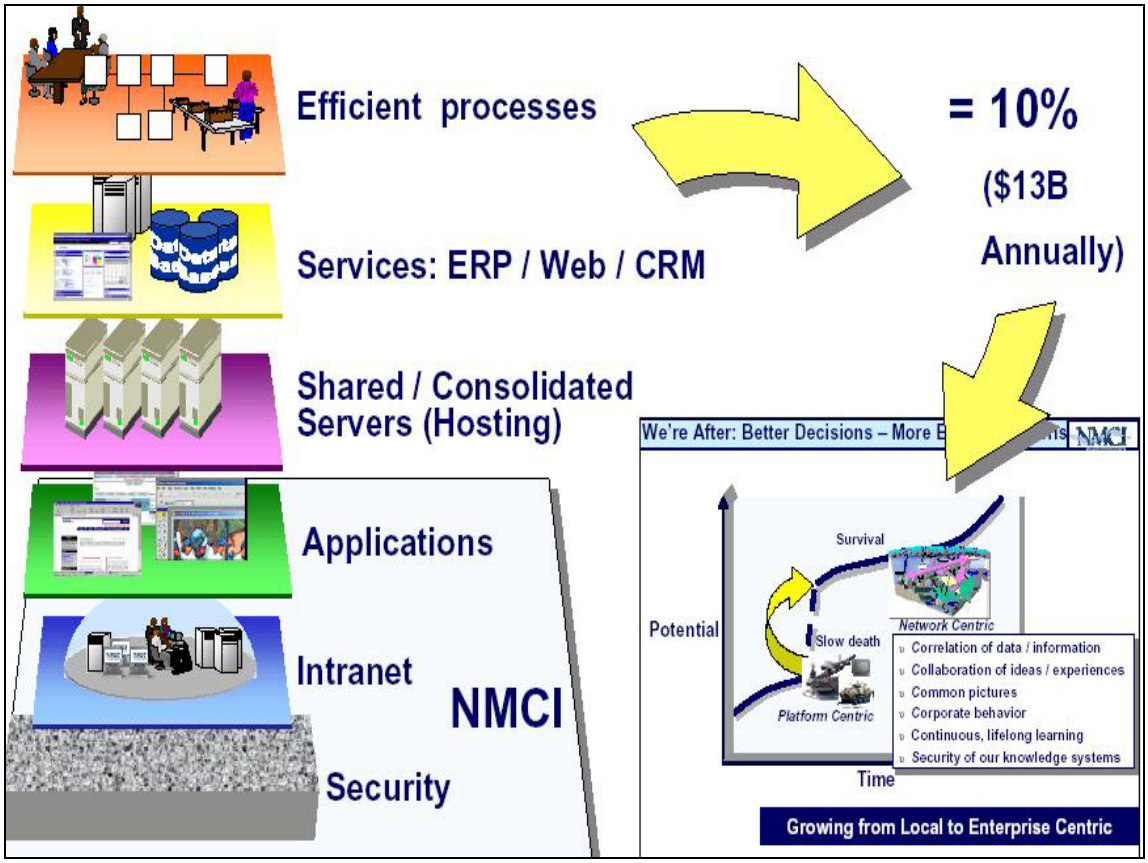


Figure 40: NMCI Savings and Other Bennefits, Rear Admiral Chuck Munns, U.S. Navy, NMCI Director, NMCI Briefing, at the SPAWAR Industry Day, San Diego-USA, 23rd October 2003

b. The Legacy Issue is still Present

In the year 2002 the main issue under concern was to cut back 100,000 legacy applications to 30,000. After the initial start up, those 30,000 remaining applications underwent evaluation to determine which are mission critical and meet NMCI guidelines. Over time, DoN and ISF hope to reduce the legacy number to approximately 7,000 applications. Ultimately, the goal is to reduce the number of applications to around 2,000, but getting participants in numerous departments to agree to change their software tools is a very complex task. Mission-critical legacy applications

that do not meet security requirements have been a major sticking point, but the Navy and ISF have dealt with them by placing the seats in quarantine. Old applications in nearly one-quarter of the seats could not be transferred to new Windows 2000 machines, forcing EDS to install “dual desktops”, leaving sailors and Marines with two PCs on their desks.

Legacy applications are not permitted onto the NMCI network either because of security risks or because they are incompatible with the standardized Windows 2000 environment. In 2003, the Navy issued stricter legacy application guidelines in order to trim down the number further. Under the directive, only applications identified as approved or allowed with restrictions by a functional area manager can be retained and allowed to run on NMCI. The tougher legacy application guidelines have caused some commands difficulty when their applications did not meet NMCI standards. (www.mit-kmi.com (NMCI: Now for the Networks), accessed February 2004)

Transitional firewalls in some places between the old Navy networks and NMCI have been installed in specific commands. The intent is to allow some applications, with appropriate security risk mitigation by NETWARCOM, to transmit in and out of NMCI that previously couldn't. But the long-term strategy is to reduce the number of applications and get those application servers inside the NMCI enclave. On the other hand, some 5,000 applications have already been certified on NMCI.

> By reducing the number of applications, it also reduces the time it takes to get applications NMCI certified, because there are fewer of them to certify. By the end of calendar year [2003], we anticipate EDS will operate everything in DoN. By mid-2004, we anticipate completely operating the NMCI.
>
> Captain Chris Christopher, U.S.N. staff director of the NMCI office

Last year, DoN turned the legacy challenge into an opportunity. Cataloging applications enabled the Navy to assess and understand which commands had which applications. A group of managers was designated to examine the applications in 23 functional areas such as logistics, personnel and administration. The managers scrutinized the list of applications and determined which to keep and which to delete. As

of the 1st of October 2003, only applications on the functional area managers' (FAM) list are allowed on NMCI seats.

c. Cultural Issue and Change Management

Resistance to change was another challenge for the NMCI implementation effort. Changing the paradigm from computers as individual property to a point of service is a major shift, and it has been an issue that the ISF has had to address at every site but without any coordinated planning. DoN and the ISF have not done a good job of managing the cultural change piece, but at least they are now trying to get better. After experiencing early glitches to move users to the NMCI environment, the DoN concluded that additional training will help future users make a smooth transition to the Navy's enterprise network.

The Navy formed a transition team last year to help commands switch from legacy systems to NMCI and to provide documents and resources to users to help them to get started and provide helpful hints on becoming a successful NMCI user. Training consists of briefings, introduction of related Web sites and information packets, but apparently not everyone is getting the training they need, according to the end users. Postings on the NMCI User Information Web page provide an on-line newsletter addressed to all users that keeps NMCI users up to date with upcoming changes to the NMCI environment and explains significant developments and events related with the NMCI implementation and operations. Additional recourses and tools include:

- A briefing given to command chief information officers, information technology leaders and command leaders six months before the transition. The briefing includes a list of contacts, a master glossary of acronyms and a lengthy presentation on the network's ins and outs.
- A subsequent briefing that takes place 60 to 90 days before the transition, again for the leaders and IT managers of a command.
- End users can download a series of "Ready," "Set" and "Go" guides and visit the EDS's special Web site about making the transition to NMCI, www.nmci-isf.com (User Information Main

Menu), accessed February 2004. These materials explain how users should prepare for NMCI prior to the installation of their NMCI workstation.

- A variety of information and electronic guidance/advice provided in the above mentioned website supported by the EDS-ISF team.

2. Information Assurance (IA) within NMCI

The overall strategy of defending the NMCI and the information it contains is articulated in the concept of information assurance (IA), which overlaps into the concept of computer network defense (CND), and also includes network availability and operational management. The NMCI network security policy is essentially a compilation of DoD and DoN information security policies. This ensures the new network's compliance and compatibility with existing and proposed DoD network architecture and operational procedures.

The NMCI network security architecture must be capable of providing protection of the Intranet's information systems and information content. This includes the execution of IA mechanisms to implement these security services and the conduct of vulnerability assessments to validate the necessary controls is in place to satisfy NMCI information assurance requirements. Because NMCI provides services critical to accomplishment of the DoN mission, network design associated with information assurance is subject to strict compliance with DoD/DoN security policy, government approval of IA products and CND operations.The NMCI security policy supports all the fundamental information assurance elements and establishes how the NMCI manages, protects and distributes sensitive information.

The NMCI system features five principal information assurance or security properties:

- Availability: Authorized users can properly access online information systems.
- Integrity: Safeguard information or communications from modification by unauthorized users.

- Authentication: A degree of certainty or assurance that information/communications are provided by authorized sources.
- Confidentiality: Only authorized individuals have access to sensitive information.
- Non-repudiation: There is some proof of sending and receiving information/communications for tracking/documentation purposes.

From the information security standpoint, the enforced uniform standards will probably reduce the number of available gateways that were vulnerable to cyber attacks in the previous IT environment. NMCI is intended to be one worldwide, configuration-managed enterprise network that meets or exceeds all DoD standards for security and information assurance. NETWARCOM is the central operational authority responsible for coordinating all information technology, information operations, and space requirements and operations within the Navy. Establishment of NETWARCOM has better aligned the various staffs needed to support the concept of one naval network and to support that network's end-to-end operational management.

The NMCI initiative, by rooting out vulnerabilities, is raising defenses. It is providing uniform security standards and training for naval personnel people before they use the network. The network operations centers control intranet traffic, and they can isolate the network if need be. NMCI delivers significant value as an asset for the DoN at the enterprise level with important improvements in IA, by providing:

- Public Key Infrastructure that is interoperable with the DoD's PKI.

  Navy and Marine Corps commands have been authorized an extension until the 1st of April 2004 to achieve full compliance with the following DoD's PKI milestones:

  - Client side authentication to DoD private web servers
  - Digitally signing all e-mail sent within DoD
  - PK-enable web applications in unclassified environments
  - PK-enable DoD unclassified networks for hardware token

- Certificate based access control
- DoN industry partners obtain DoD approved PKI digital certificates or external certificate authority (ECA) PKI digital certificates

- Strong Authentication: PKI Certificates are stored on a cryptographic smartcard (in almost every case, the DoD Common Access Card) that is required for network access, no matter of the point of entry.

- Central Security Management: Certification & Accreditation plus real-time network operation status provided.

- Incentives Performance on IA: DoN Teams will provide independent assessments of the security posture of the NMCI network. The NMCI vendor receives a monetary reward based on their performance on these assessments. Red teams, independent of the contractor, review network designs for vulnerabilities and periodically conduct simulated attacks. If they breach the network, the contractor could lose as much as $10 million a year.

- Defense-in-Depth: Multiple protection technologies installed in a layered system of defenses.

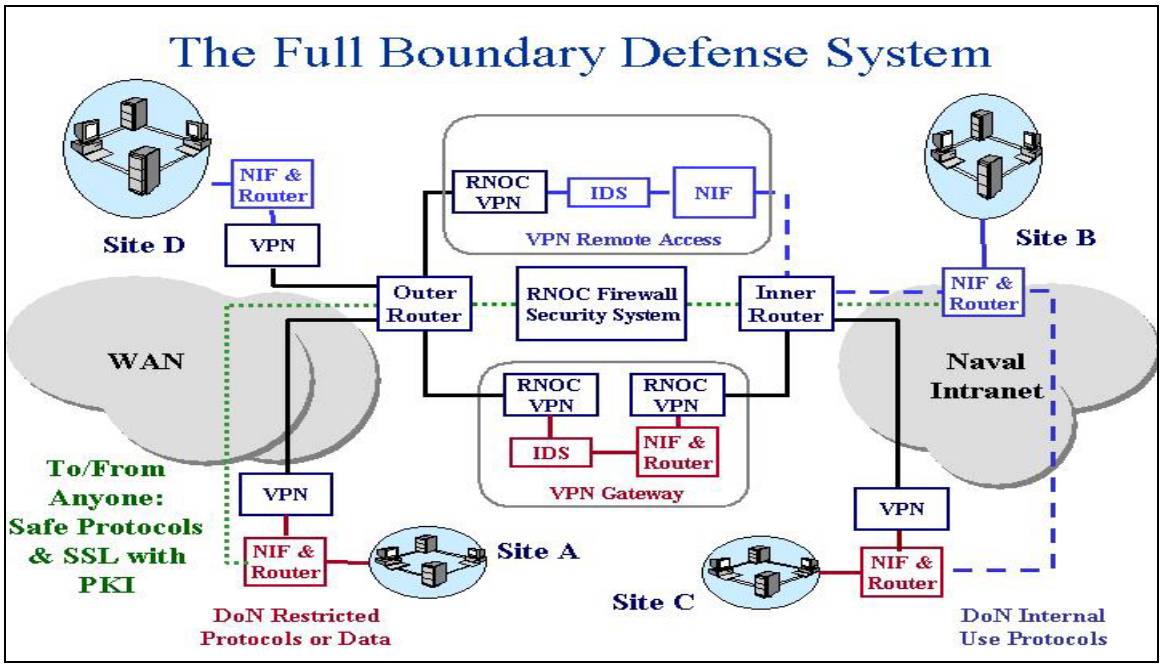


Figure 41: The NMCI Security Architecture.

E. ENDNOTES

1. Information Security (INFOSEC) can be defined as the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Information Assurance (IA) activities are defined as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities. (Dorothy E. Denning (1999). *Information Warfare and Security*. Massachusetts: Addison Wesley Longman, Inc., p. 40)

2. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. By convention, URLs that require an SSL connection start with *https* instead of *http*. (www.Searchsecurity.com (SSL Definition), accessed February 2004)

3. The purpose of the baseline (As-Is) study was to provide an assessment of assets and services in place within all installations at the time the BCA was conducted. Survey and extrapolation techniques were determined to be the best solution for estimating the DoN's "as-is" baseline. A sampling technique was implemented to gather a representative cross-section of data reflecting IT costs and service levels in effect.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

A. THE WAY NMCI IS TESTED

The DoN continues to try to identify the imperfections of NMCI and is currently in the process of conducting a complete operational evaluation of the intranet. The original plans from September of 2001 described a series of linear tests that resembled the “ship evaluation” approach. The network had at that time to pass specific tests before the next set of seats would be brought onboard. A critical task for the year 2004 is the successful completion of the evaluation of NMCI at the operational level. Unlike the original testing plans, the operational evaluation is not a "go, no-go" decision and the entire network will be rolled out. The focus of the new evaluation is to identify weak points and provide feedback to improve performance of the current environment.

It is necessary to briefly examine the previous testing concepts related to the NMCI’s implementation. Management Systems Designers, Inc. (MSD) successful support for the NMCI Contractor’s Test and Evaluation (CTE) phase was the reason to be awarded a two year task to perform turning-up testing at all NMCI (large and major) command sites prior to production turn over, on the 8th of March 2002. Turning-up testing is a critical activity at the end of “Site Preparation” phase during the transition towards the NMCI and is a binding activity according to the NMCI contract prior to declare the specific site operational, in order to validate the architecture of the infrastructure built to support the operation of the Intranet. Typical activities within the tests included fact-finding, data discovery, function activity and task analysis, tool selection, development and employment. Finally, the conclusions were derived after an extensively detailed architecture analysis. To facilitate the testing activity, MSD has built an enterprise architecture development practice by applying the Chief Information Officers’ Federal Enterprise Architecture Framework (CIO-FEAF) and DoD’s command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) frameworks, via selecting the specific components that best match DoN requirements. Feedback from end–users and modeling tools were used extensively to facilitate the design and development of the continuously adjusted testing procedures.

Testing was conducted at all seven layers of the open system interconnection (OSI) model and the network in question was stressed to its limits via a disciplined, pre-configured approach. The performance test methods were based on traffic generation, interoperability confirmation and on-going network surveillance techniques. The approach used was to assess interoperability and the effects of various network components, applications, and operating systems' changes on the network with a "holistic view", by identifying the various interdependencies.

This specific structured approach allows network engineers to measure network performance, predict failure, and analyze recovery accurately. The goal was to provide the data to understand systems or network limitations and to identify the corrective action in a repetitive process, thus achieving high levels of network availability. The performance measurements should go beyond simply measuring point statistics. Trend analysis should be used extensively to identify potential impending problems and highlights areas that need improvement.

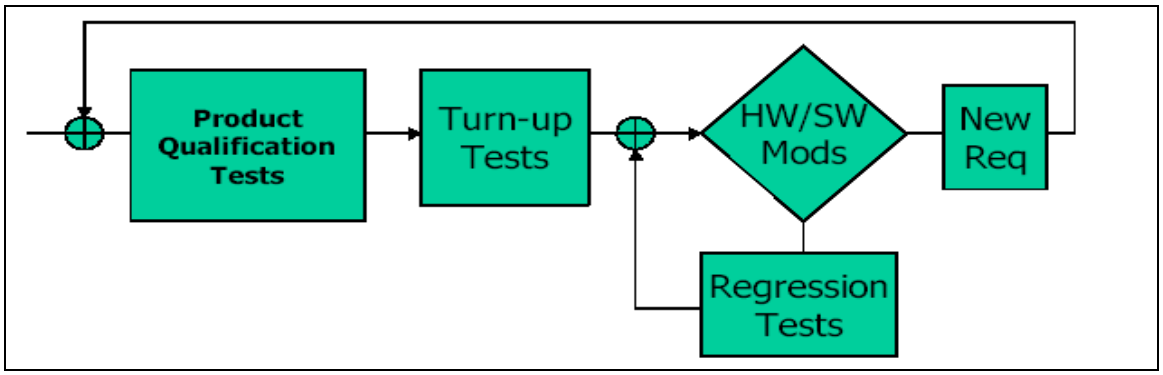


Figure 42: The MSD Framework for the NMCI Turning–Up Testing, from www.msdinc.com, accessed February 2004

MSD used the approach shown in figure 42 to support the first increment of NMCI evaluation activities, by developing a detailed test plan for the worldwide, base level and local area network testing, as well as key enterprise application tests such as directory services and e-mail latency. The plan involved identifying and developing an approach that is totally independent of the NMCI built-in network management system. It also required evaluating performance differences under varying conditions between different WAN carriers, identifying the necessary test tools and developing detailed testing procedures to conduct tests at the various NMCI operational sites.

A combined team, with the necessary DoN and EDS personnel was responsible to conduct the testing activities. An independent third party by specific DoD agencies ensured the validity of the results and the thorough analysis of the data collected, made possible the acceptance assessment that took place during the year 2002. At that time, the evaluation involved roughly 20,000 seats; this year there will be more than 100,000. The NMCI schedule for the operational evaluation activity established the beginning of the activities in early October 2003 and the delivery of conclusions around the 2nd quarter of 2004. The main idea is to closely examine the deployment and operation of the network. Based on a similar concept with the previous tests and in order to ensure the validity of the methodology, this new "operational evaluation" will be conducted by a combination of independent testing teams. MSD has recently announced the completion of the WAN/LAN and Servers (Email, Newsgroup, Active Directory, Web, etc.) performance testing in support of the NMCI evaluation.

B. EVALUATION OF NMCI PERFORMANCE

NMCI supports the fulfillment of both strategic and operational requirements for the DoN. Analysis made in the BCA for the NMCI concluded that the pre-NMCI DoN IT environment only partially exhibited the desired levels of service in Network Operations and Maintenance, Interoperability and Security/Information Assurance. Achieving the service levels specified in the NMCI contract aims to resolve these deficiencies. The NMCI's Performance Measurement Plan is the approach used to ensure that key outcome measures are identified and collected in order to facilitate the evaluation of the intranet's performance and determine whether NMCI is supporting the kinds of improvements it was designed to accomplish. In order to capture and analyze the full picture of the network and whether the capabilities this IT platform offers to the DoN enterprise are taken fully advantage by the users or not, the following strategic performance measurement categories are used:

- Interoperability
- Security and Information Assurance
- Service Efficiency
- Customer Satisfaction

- Work Force Capabilities
- Process Improvement
- Operational Performance

The first two measures, interoperability and security and information assurance, relate to the NMCI's supporting role of the DoD's Global Information Grid (GIG). The second pair of measures, service efficiency and customer satisfaction, measure the immediate impact of the intranet on the whole organization. By measuring the services provided, the total cost of providing services and making the customer (end-user) a key part of the process, the direct impact of NMCI can be readily assessed. The last three areas of measurement, assure that the intranet will be an integrated portion of the Navy and Marine Corps strategic vision, supporting the principles of using information technology (IT) to support people, focusing on the value of technology and using IT as a force multiplier. (NMCI Report to Congress, 30 June 2000, p. J-5-1)

To facilitate the establishment of performance criteria, the combination of different perspectives was necessary. It is necessary for government programs to assure that they address important strategic performance objectives in a measurable way. The Balanced Scorecard for NMCI is a DoN process that is designed to provide the Navy and Marine Corps leadership with tools to judge how well NMCI is supporting the missions and strategies of the Department. Furthermore, the main idea is not to simply collect and analyze data, but also use it to drive improvements in their organization and the associated programs. The five different domains shown in figure 43 are used to evaluate the NMCI performance and provide focus on how NMCI is supporting strategic goals:

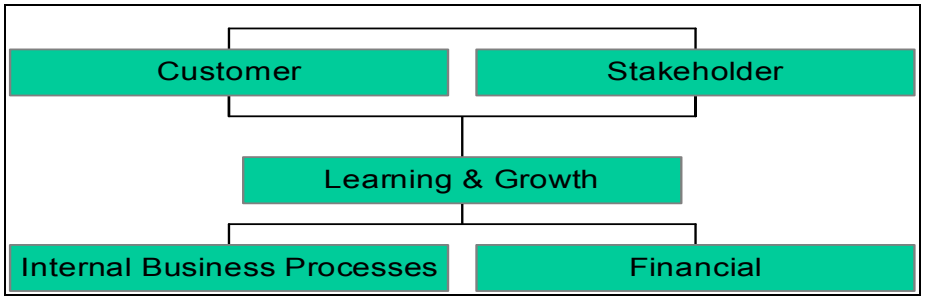


Figure 43: Balanced Scorecard Perspectives, from www.nmci.navy.mil (Performance Measures), accessed February 2004

Performance measurement and review may be the weakest link in today's managed services programs. The relationship between the customer and the services contract provider needs to consist of mutual understanding and cooperation. This relationship can only be strengthened when it is also based on independent, accurate and up-to-date performance measurements and reviews. Therefore, a multidimensional approach is necessary to provide the full picture of the NMCI performance.

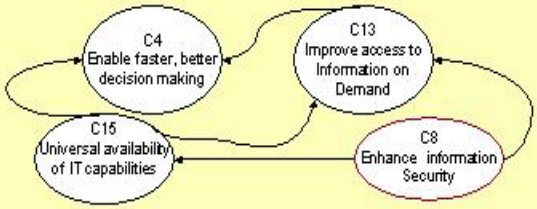
1. Customer Perspective

The first and most important component used in the NMCI evaluation is the customer perspective, expressed in terms of the NMCI's impact on the end user. Specific targets like the level of effort to access the offered IT capabilities, including seamless and faster handling of information and the overall security level have been defined and data is collected through surveys or automated software tools that capture statistical details.

Customer Objectives and Definitions

Customer Perspective

Champion :



Objectives	Definitions	Measures
C4. Enable faster, better decision making	C4. Provide access to a broader range of more meaningful information to facilitate decision making processes.	**C4.1 Survey 20% Echelon 3 (Lag)**
C15. Universal availability of IT capabilities	C15. All DON employees have access to full spectrum of IT capabilities.	**C15.1% of DON employees with NMCI account (Lag)**
C8. Enhance information security	C8. Eliminate network intrusion by unauthorized personnel while providing tightly controlled configuration of intranet hardware/software	**C8.3 Percentage of successful penetrations out of total detected and undetected attempted intrusion (Lag)**
C13. Improve access to information on demand	C13. Easier to find information requested and easier to gain authorized access.	**C13.3 % of workforce that can access users data 24/7 from any location (Lag)**

Figure 44: Customer Perspective used in the evaluation of the NMCI Performance, from www.nmci.navy.mil (Performance Measures), accessed February 2004

2. Stakeholder Perspective

NMCI is not only about delivering a better communication capability. The second component within the NMCI's performance matrix is the stakeholders' perspective, expressed via the impact at the various commands or even at the Department-wide level mission. Main areas of concern are the interoperability issue along with the adaptation of improved business practices and alignment if necessary with the commercial sector practices. The driver of the stakeholder perspective is to increase effectiveness of the personnel with the IT support allowing for reduced manning and to provide increase combat capability to the DoN, by "utilizing" commercial sector experts to further improve and solve problems of the associated infrastructure.

Stakeholder Objectives and Definitions

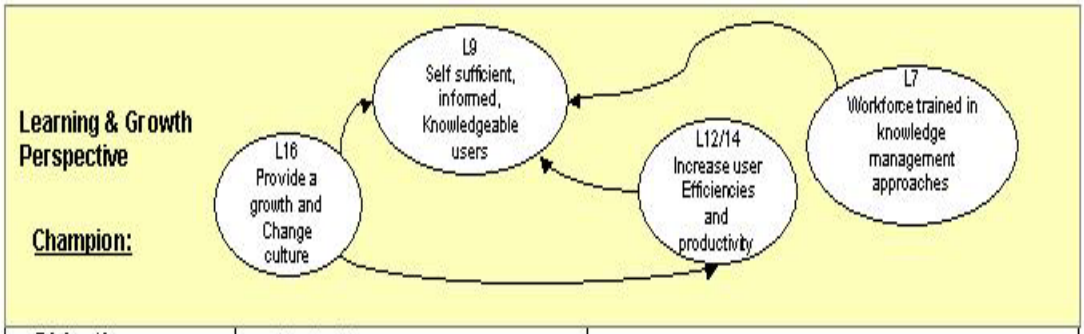
Objectives	Definitions	Measures
S1/2. Improved mission effectiveness and combat capability	S1/2. Perform missions and fight and deter wars better than we can presently.	**S1/2.1 20% survey MAGTF (Marine Commanders), Navy Battle Group Commanders, and Echelon 3 (Lag)**
S13. Supports adoption of best business practices	S13. Provides a networking infrastructure for easier and less costly adoption of new ways to do business.	S13.1 Increased number of successful re-engineered business processes leveraging IT (Lag)
S6. Increased Interoperability	S6 . Application and communication conformity from desktop to desktop within the enterprise and improved communications between DON network and external networks.	**S6.1 Increased access of internal and external users to network (Lag)**

Figure 45: Stakeholder Perspective used in the evaluation of the NMCI Performance, from www.nmci.navy.mil (Performance Measures), accessed February 2004

3. Learning and Growth

As already shown in Figure 43, this perspective overlaps with all the other domains used in the NMCI performance evaluation. The main idea is to promote innovation and introduce collaborative tools to achieve a better level of cooperation among the various elements of command. Again, it is necessary to use a combination of surveys along with statistical analysis to reach a measurable result.

Learning and Growth Objectives and Definitions



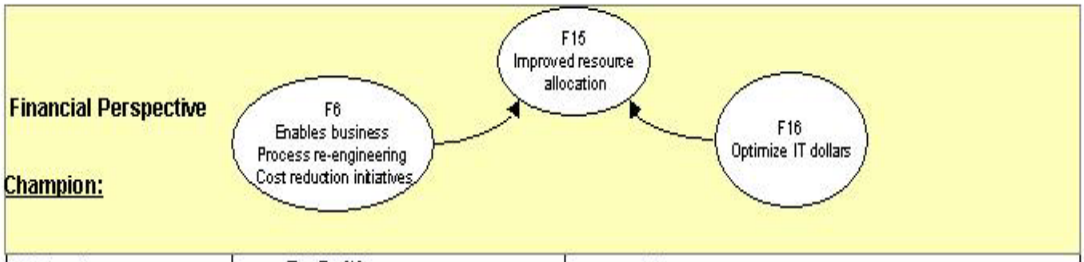
Objectives	Definitions	Measures
L9. Self sufficient, informed, knowledgeable users	L9. DON workforce trained and able to use NMCI capabilities to get their jobs done.	**L9 1, Workforce survey - % reporting NMCI helps to get job done (Lag)**
L16. Provide a growth and change culture	L16. A workforce that uses the new enterprise interconnectivity to prepare for the future and collaborate for improvement in processes and organizational re-engineering	**L16.1 Workforce survey - % reporting "yes" Navy supports a growth and change culture (Lag)**
L12/14. Increase user efficiencies and productivity through application of better IT interface and tools.	L12/14. More work in less time due to better IT interface and productivity tools. Fewer hours spent in waiting for network or system problems to be corrected combined with faster response time and enterprise access to data.	L12.1 Ratio of people serviced per IT support person (Lag)
L7. Workforce trained in knowledge management approaches	L7. A workforce trained to use the access, learning, collaboration and training tools in order to sustain and improve the core competencies of the DON.	L7.2 # of people using collaborative tools (Lag)

Figure 46: Learning and Growth Perspective in the evaluation of the NMCI Performance, from www.nmci.navy.mil (Performance Measures), accessed February 2004

4. Financial Perspective

The financial perspective includes a variety of estimates to determine the economic value related to this IT investment to include Return On Investment (ROI) and ratios used to describe improvements between the previous "As-Is" state and the current state under NMCI operation.

Financial Objectives and Definitions



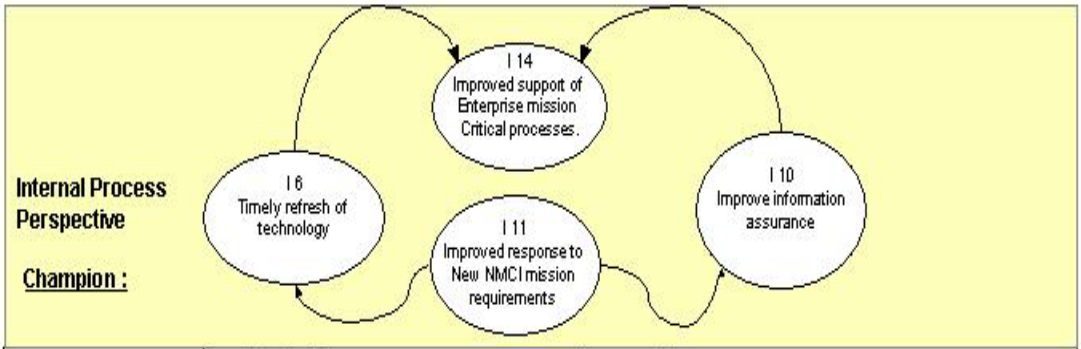
Objectives	Definitions	Measures
F15. Improved resource allocation	F15. More dollars correctly focused on core competencies instead of IT service and infrastructure	F15.1 Percent of applications that are enterprise vs. local
F6. Enables business process re-engineering cost reduction initiatives	F6. Provides an infrastructure supportive of re-engineering processes and legacy application reductions.	F6.2 Number of successful business process reengineering initiatives (Lag)
F16. Optimize IT dollars	F16. Dollars spent on NMCI translate into best value services for DON employees.	**F16.1 Improved ratio of service level per IT investment dollar (Lag)**

Figure 47: Financial Perspective in the evaluation of the NMCI Performance, from www.nmci.navy.mil (Performance Measures), accessed February 2004

5. Internal Process Perspective

Because NMCI is implemented under an "enterprise" paradigm it is also necessary to include performance estimates related to the overall support of the DoN mission and requirements. The pace of the introduction of technology is monitored along

with the necessary refreshment attempts. The specific domain also captures portions of the IA aspect and especially focuses at the level of protection of the network, to include reactions in case of intrusion.



	Definitions	Measures
I14. Improved support of enterprise mission critical processes	I14. Ensure that communications and computing resources necessary to meet the future combat and support needs of the DON are ready as needed.	**I14.1 Percentage of web enabled enterprise mission critical process. (of the whole number of enterprise mission critical processes) (Lag)**
I6. Provide timely refresh of technology.	I6. Keeps the user community up to date with the state of the art in computer desktop hardware, networks and other components.	**I6.4 Time between new commercial products announced and availability on NMCI service level (Lag)**
I11. Improved response to new NMCI mission requirements	I11. Anticipate the future demands for new communication and enterprise computing capabilities and be ready with hardware and services to meet the needs.	**I11.1 Reduction in the cycle time from user requirement identification to service delivery (Lag)**
I10. Improve information assurance	I10. Enterprise data is safe from compromise and the system is protected from security intrusions.	**I10.2 Reduced number of IA incidents reported. (Lag)**

Figure 48: Internal Process Perspective in the evaluation of the NMCI Performance, from www.nmci.navy.mil (Performance Measures), accessed February 2004

6. Tools to Create the NMCI Balanced Scorecard

The Predicate Logic, Inc., announced during the year 2003 that its tool TychoMetrics® has successfully gone through an extensive evaluation by the Gartner Group and Cranfield School of Management and was selected to deliver the NMCI automated Balanced Score Card (BSC). TychoMetrics can run on any TCP/IP network with the objective to harvest data from remote globally distributed sites using the

Internet, and by being NMCI certified, it runs on every Navy and Marine Corp desktop and provides a wide variety of "Smart-Metrics". The specific software application is not a dedicated BSC application but a tool to automate metrics collection, derivation, and visualization of data. TychoMetrics® can be easily adjusted to support an IT environment where you have electronic data to harvest and analyze. The TychoMetrics® Tool Suite uses only Microsoft's operating system environments. There are only two requirements to collect data from any source: the measurement source file must have visibility to the TychoMetrics® Mediator and the Mediator must have the *probe/ probe agent* that corresponds to the tool source. The Mediator is the behind the scenes component that automates the data collection process. The probe/ probe agent specifies the data to be collected. The software tool can then report the data in various configurable formats including the BSC. (www.tyckometrics.com accessed February 2004). According to the company, TychoMetrics strengths include:

- Automated data collection
- Derivation and visualization of data/reporting, data sourcing and integration
- E-mail alerts when metrics exceeds upper or lower control limits or thresholds
- Statistical process control and management by exception

The approach of the BSC is extremely useful in order to track and promote strategic goals at the "enterprise–wide" level. In order to have a sound approach within a service level contract it is necessary to have a performance measurement system in place that has the following characteristics:

- Easily maintained and run by the customer's (Naval) personnel. A single point of control would eliminate duplicate data and remove manning burden.
- Automatic generation of performance analysis and change management reports.

- Automatic up-to-date, accurate and complete data about all computer hardware and software assets, and how and where they are deployed. Profiling data should be updated on a regular basis, i.e. daily, so that the latest profile data is always available to help make performance analysis and other decisions.

- Easy access to reports and data by both the customer's and the service provider's personnel, at any time.

C. HOW THE SERVICE LEVELS ARE MEASSURED

1. Establishment of the NMCI Contract Performance Levels

The performance measures in the SLAs represent the current and validated operational requirements of the DoN. The NMCI SLAs evolved from the pre-established Measures of Effectiveness (MOEs) during the negotiation phase, which in turn were based on the NMCI Design Reference Mission (DRM). The DRM approach was used in order to fully define the user mission environment and the general operating envelopes that the NMCI solution should support – thereby leaving to the service provider the ability to use best practices, new technology, innovation, and cost avoidance. The DRM describes the Navy and Marine Corps "use environments", both tactical and non-tactical. A combined DoN operational, engineering and acquisition team was specifically formed to ensure a succinct capture of operational requirements for NMCI and an accurate translation of these into contract requirements developed all of these products. (NMCI Report to Congress, 30 June 2000, p. D-6-4)

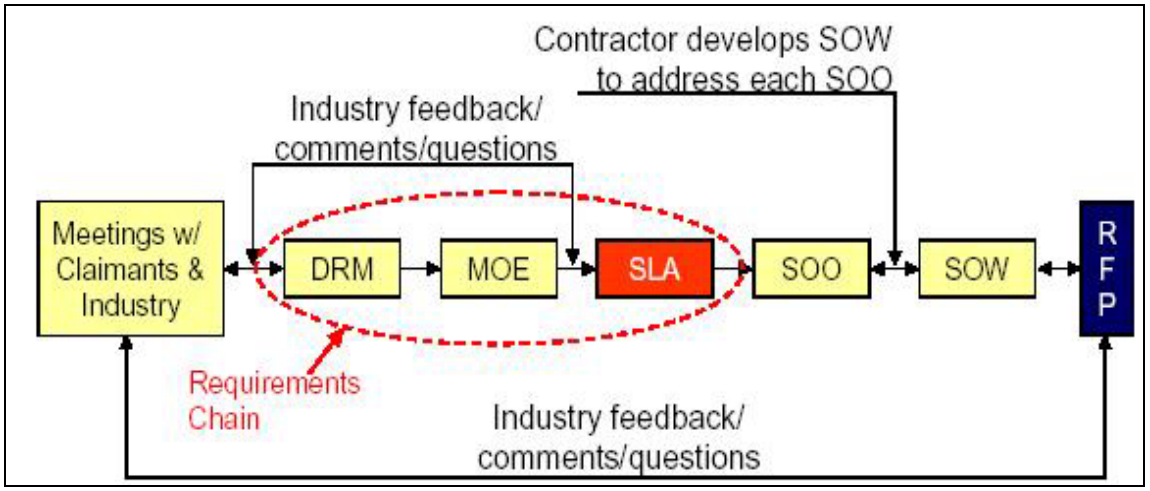


Figure 49: Establishment of SLAs, from the NMCI Report to the Congress.

a. Measures of Effectiveness (MOE)

The DRM provided the necessary details to articulate IT services needed for individual elements within the DoN to accomplish its mission. References to performance aspects of IT were narrowed down to the major factors that would significantly impact mission accomplishment. Critical factors to establish the necessary IT environment were identified, prioritized, and assessed as to the ability to serve as a MOE. The MOE was the government provided performance curve and the SLA is a reference point on that curve which the contractor would propose. To qualify as an MOE, that factor had to:

- Be a meaningful indicator of the end-to-end NMCI service delivery performance (or provide an indication of how proactively the provider is addressing infrastructure performance needs)
- Represent a factor or a specific group of factors that could be addressed and influenced by the provider
- Be measurable

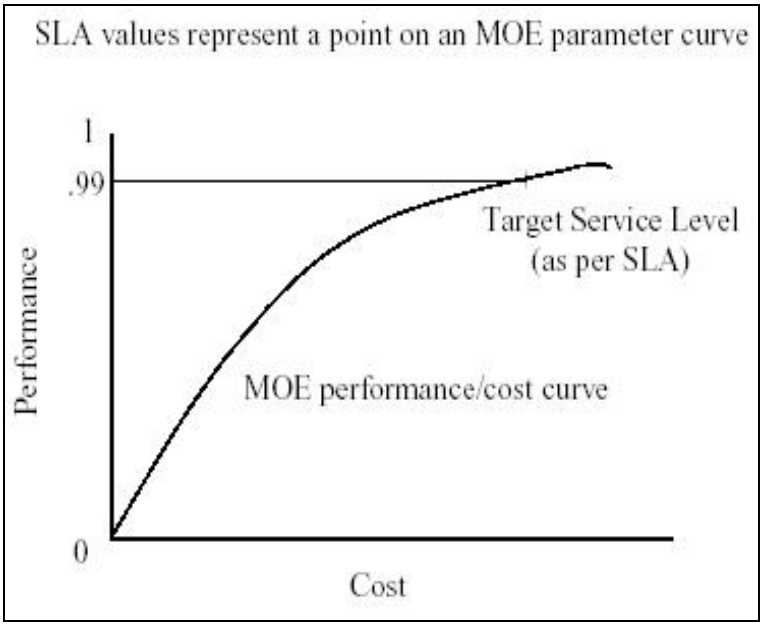


Figure 50: MOE Performance Curve, from the NMCI Report to the Congress

SLAs completely define the metrics that are be used to evaluate the network performance and the level of service provided by the contractor. Three tiers of the MOE hierarchy are presented. Three top-level SLA components, Assurance, Capacity

and Responsiveness, collectively define all of the relevant characteristics and performance of NMCI and are used as the first tier of a multi-tiered series of measurable units. The second tier, Availability, Survivability and Integrity, provide increasing specificity and detail in defining measurable areas of performance.

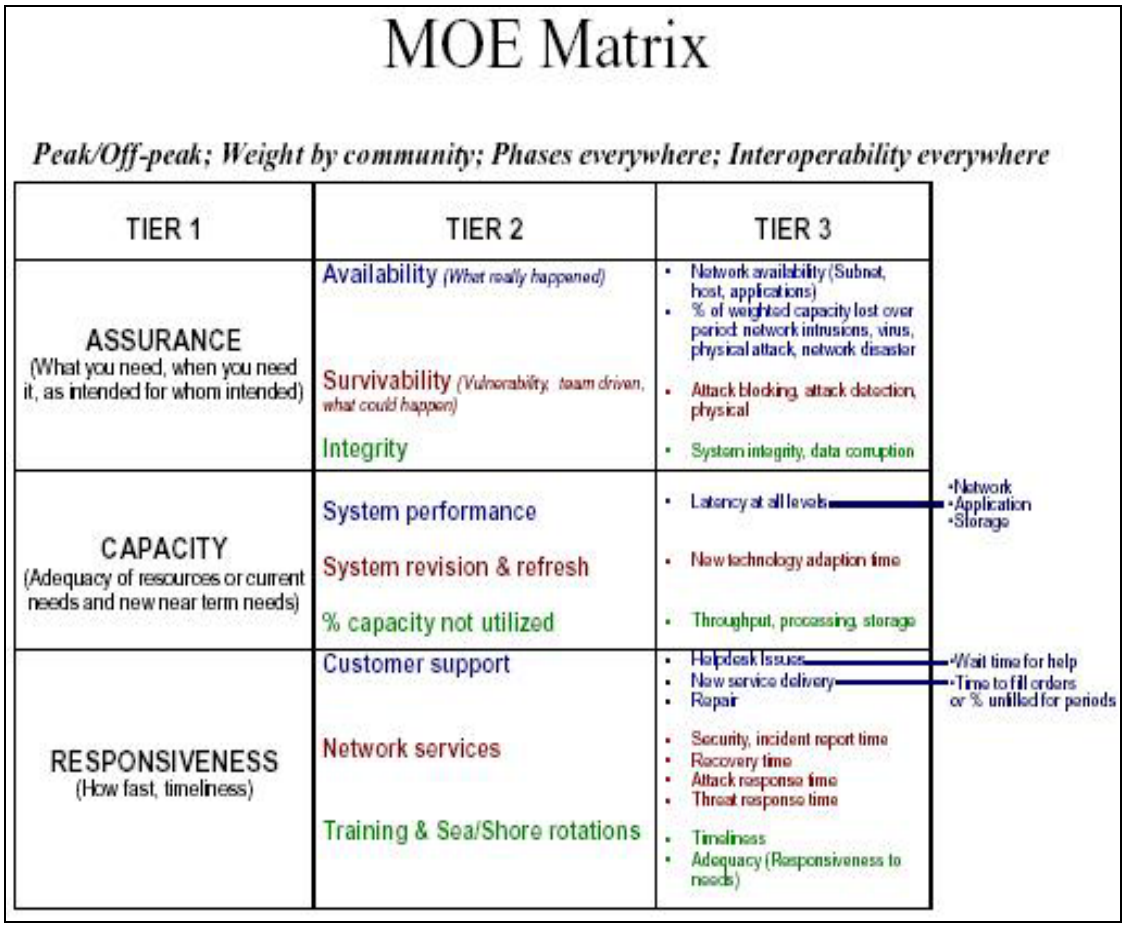


Figure 51: MOE Analysis to Determine SLAs, from the NMCI Report to Congress

b. NMCI SLAs

During the development of the NMCI Request For Proposal (RFP) a decision was made to shift from providing the vendors with only MOEs towards adopting the industry standard practice of using SLAs. The DoN requirements were established with the focus on the maximum reliable communications and WAN performance (such that the WAN would operate as an effective extension of the LAN) in combination with maximized cost savings making therefore the obvious selection of setting the level of measurements at the knee of the industry cost performance curve. Benchmark values for the MOEs were translated to SLAs, and the breadth of coverage of these SLAs expanded to cover areas of IT service consistent with good seat management contracting practice.

Recognizing the evolving nature of IT infrastructure, the final definition of requirements related to NMCI is a process that has included evaluation of existing best business practices as well as military system performance parameters supporting both business and military applications. This process is iterative and sufficiently flexible to allow procurement of a "best value" service that is both consistent with current and emerging technologies and military uses of those infrastructure services.

2. NMCI Performance Level Measures

The Clinger - Cohen Act requires the establishment of performance measures to assess how well NMCI supports mission accomplishment and to provide accountability and evaluation of investment post-deployment. Baseline service level performance for each of the domains in question and baseline cost for services under the previous DoN's IT environment were assessed in the BCA for the NMCI and were documented in the "As-Is" Total Cost of Ownership (TCO) analysis section. Analysis of the technique currently in place to support the evaluation of the NMCI performance can be further broken down into distinct categories.

a. Service Efficiency

The economic effectiveness of NMCI is determined by comparing its cost versus the level of service provided. NMCI can increase its efficiency by either providing more services for the same cost, or it can reduce the price paid for the same level of services. The ratio of cost to services provided is the key indicator used to decide whether the contract is cost-effective. Service efficiency is a measure of the cost associated with supplying IT services to the DoN. The NMCI's efficiency is monitored through the cost per service level, and not simply through costs or services total independently of one another. Two measures are used to judge the effectiveness of NMCI in achieving service efficiency:

- Direct cost per specified level of service
- Indirect costs

Costs include both direct costs (i.e., annual cost per seat) and indirect costs (as a monetary representation of productivity gains or as an indicator of IT system efficiency from an end-user perspective). Direct costs measure the costs that are typically

included in the IT budget. These include the costs of hardware and software, as well as the costs of network operations and administration, including labor costs. Direct seat costs are roughly comparable to the costs covered by the NMCI outsourcing effort. Indirect costs include many of the impacts of IT services on the end user that affect productivity, but are not explicitly covered in the IT budget. These costs include: (NMCI Report to Congress, 30 June 2000, p. J-5-5)

- Informal computer support—time the end user spends either by himself or with peers supporting basic information management (IM)/IT services because help desks are not responsive
- Learning—both formal and casual
- Downtime—lost productivity due to network or software problems

Basic user services (covered by different SLAs) that for the time being are used to measure performance include:

- Standard office automation software
- E-mail
- Web access
- Intranet performance
- Internet access
- Desktop access to Government Applications
- User training
- Search engine services
- Directory services
- News groups
- Print services
- Unclassified remote access
- NIPRNET/SIPRNET access

- Portable workstation wireless dial-in
- Software distribution
- Mainframe access

b. Interoperability

Information interoperability is a key enabler necessary to share information throughout the DoN enterprise. The DoN, in order to ensure that the level of collaboration either within the Navy domain or with other external services would not be undermined under NMCI, put a lot of interoperability tests into the first increment of the contract to help erase these fears. [Note 1] Interoperability within the NMCI contract is defined, as the ability of the related with the NMCI IT systems to provide services to and accept services from other armed forces and facilitate communication and sharing of information.

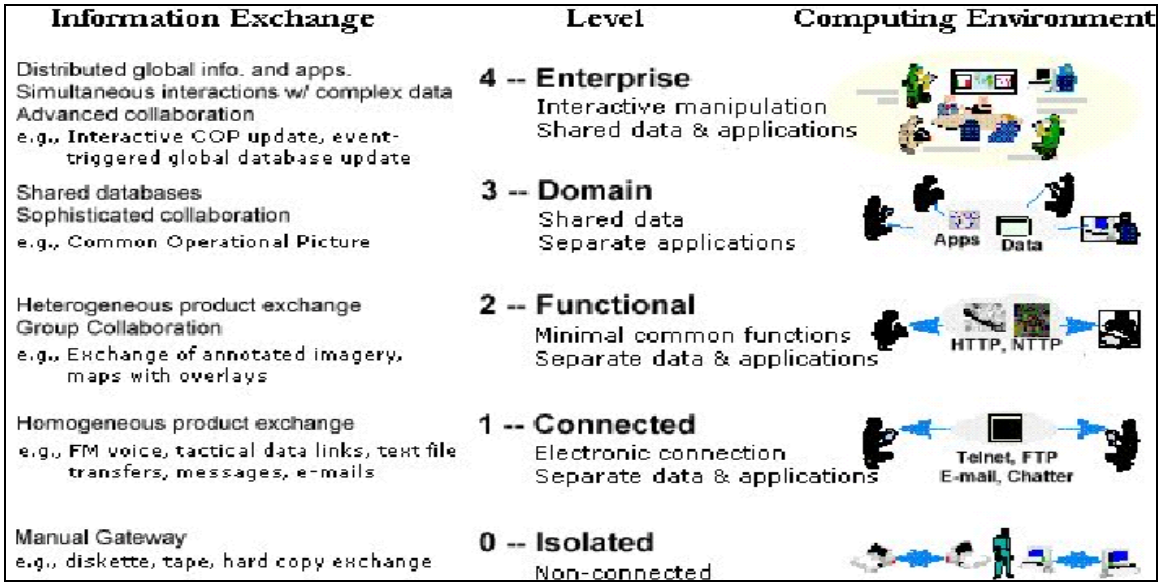


Figure 52: DoD Levels of Information Systems Interoperability (LISI), from the NMCI Contract N00024-00-D-6000, (Confirmed Contract P00080)

In order to achieve interoperability, applications need to achieve both connectivity and the capability to share data. For the time being, NMCI provides the connectivity required to enable the DON to achieve LISI level 2. Levels in the upper level of the hierarchy can only be achieved through integration of applications and a shared data environment. The NMCI is a critical component of the DoN's vision of a network-centric force, where a single secure, integrated network delivers all voice, video,

and data IT services to more than 360,000 seats in more than 300 locations. Through the standardization of hardware and software suites, and employment of common, multi-layered security architecture, the NMCI will greatly improve interoperability and security across the Navy and Marine Corps.

c. Security

NMCI provides security services for protection of the Information System (IS), IS Domains (Communities of Interest) and Information Content (at rest, in use, and in-transit) in accordance with DoD's IA policies and procedures. Security services protect both unclassified and classified information and the aim is to achieve full integration with the DoD Public Key Infrastructure (PKI) services. (www.nmci.navy.mil (Security Services), accessed February 2004) Security measures are used to compare the performance of the enterprise pre- and post-NMCI operations. The measures focus on:

- The ability to detect and respond to security intrusions
- The level of compliance and successful execution of good security practices (i.e. compliance with INFOCONs, IAVAs, PKI and Smart Card).

The first set of measures (attacking the NMCI) is the "Red Team" approach, which will focus on quantitative evidence of how NMCI performs on protecting information and networks. This includes the results of exercises identifying vulnerabilities, numbers of intrusions, reasons for intrusions, and response time for correcting security problems identified by intrusions. The second set is analogous to the "Green Team"("hardening" the security structure of NMCI). These measures address compliance with already established by the DoD security and information assurance procedures. They include such measures as the number of seats with smart card capability and utilization of public key infrastructure, evaluations of current practices and policies, and compliance time for such actions as INFOCONs and IAVAs.

Specific IA SLAs are representative of the target performance measures for the range of IA functionality provided with NMCI. The IA SLAs are in two categories: Security Planning Services and Security Operational Services. Because of their critical role in the DON, two of the operational services–PKI and SIPRNET–have

been broken into separate SLAs. Utilizing a "defense in depth" strategy, NMCI is designed to provide confidentiality, integrity, authenticity, identification, access control, non-repudiation, survivability, and availability of the information and information technology (IT) systems in a network centric warfare environment.

d. Network Operations and Maintenance

Network management services include such disciplines as virus detection and repair, low impact upgradeability, scalable architecture, change management, and maintenance of the Local Area Network hardware and software. Systems management services include asset management, software/hardware inventory, software distribution, and systems management.

NMCI Performance Measures			
Perf. Measure	Baseline	Goal	Metric
Service Efficiency			
Direct Cost/Service Level	$824	$600	Obtained from post contract award IT manager survey, contract performance monitoring, and actual contract cost
Indirect Costs/ Seat	$8,619	$3,642	Obtained from post contract award IT manager survey, contract performance monitoring, and actual contract cost.
Interoperability			
Joint and Industry Network Interoperability	Partially Exhibits Required Service Levels	Fully Exhibits or Exceeds Required Service Levels	Obtained from post contract award IT manager survey, contract performance monitoring, and actual contract cost
Security			
Security Services	Partially Exhibits Required Service Levels	Fully Exhibits or Exceeds Required Service Levels	Obtained from post contract award IT manager survey, contract performance monitoring, and actual contract cost
Network Operations and Maintenance			
Network Management Services	Exhibits majority of NMCI Service Levels	Fully Exhibits or Exceeds Required Service Levels	Obtained from post contract award IT manager survey, contract performance monitoring, and actual contract cost
System Management Services	Partially Exhibits Required Service Levels	Fully Exhibits or Exceeds Service Levels	Obtained from post contract award IT manager survey, contract performance monitoring, and actual contract cost

Table 8: NMCI Performance Measures, from www.nmci.navy.mil (Performance Measures), accessed February 2004

3. Automated Tools Used

The service levels are monitored using an enterprise management system located at the NMCI network operations centers in Norfolk, Va., San Diego and Hawaii. (www.fcw.com (Navy, EDS to refine performance metrics), accessed March 2004) These facilities are where EDS and subcontractor's personnel work alongside Navy personnel to monitor, maintain, repair and protect the network that comprises NMCI. EDS is deploying Cisco® Info Center to manage its service-level agreements (SLAs) with the NMCI. By using this automated tool, the NMCI administrators can more easily manage the daily operations of the intranet and demonstrate to the executive oversight committees how the network is performing on an ongoing basis and in real time.

> We are dedicated to providing the optimum level of service for NMCI, and this tool will help us monitor the system to verify that the elements of the enterprise network are performing, as they should
>
> Bill Richards, EDS' NMCI Enterprise Client Executive

Cisco Info Center, developed by Cisco and Micromuse, enables users to centrally manage and control infrastructure services. Through sophisticated service-level alarm monitoring and diagnostics capabilities, the system provides impact analysis, situational awareness and service assurance for SLA management and reporting. It also provides application, system, and network fault and performance monitoring; network trouble isolation; and real-time service-level management for enterprises. By interacting with other management tools, the specific automated tool has the ability to provide service-level monitoring and network partitioning for virtual private network and customer network management services. Cisco Info Center provides real-time end-to-end visibility and accurate business impact analysis on IT-related faults. With direct and easy access to such vital intelligence, NMCI administrators are able to quickly prioritize workflow and focus on the most mission-critical problems first. (www.cisco.com (Products), accessed March 2004)

Norfolk is the primary operations center; the San Diego facility also monitors the systems and is there for backup in case anything happens, no matter how major or minor. At each NOC facility there is a room — physically the heart of the center — where technicians monitor the vital signs of the systems at work. Overhead screens use traffic-

light images to let everyone know the status of services by location, while individual monitors track each component in more detail. Availability of services within the network is defined as the percentage of time any service is available to the end user or the end user community. For the time being, EDS must meet roughly 200 metrics, ranging from help desk support to network response time.

4. Conclusions and Recommendations for the Performance Monitoring Methodology Currently Used

a. Development of SLAs

A service level agreement (SLA) gives both the DoN and vendors a baseline by which to determine whether the service contracted for is being delivered and a way to measure performance. It may have been difficult to get all user groups to totally agree on the requirements, however extensive risk mitigation techniques and feedback from a variety of end-user groups was used to deliver the final result. No matter that the approach to negotiate for the NMCI contract was established by a government agency (DoN) with minimum services contract experience, the procedures used to develop and define the SLAs were sound based on proven concepts already followed by the commercial/private sector business. Every aspect of the multi-billion NMCI outsourcing contract that covers voice, video and data services is outlined in a SLA with extensive details. A summary of the challenges involved and conclusions is shown in Figure 53:

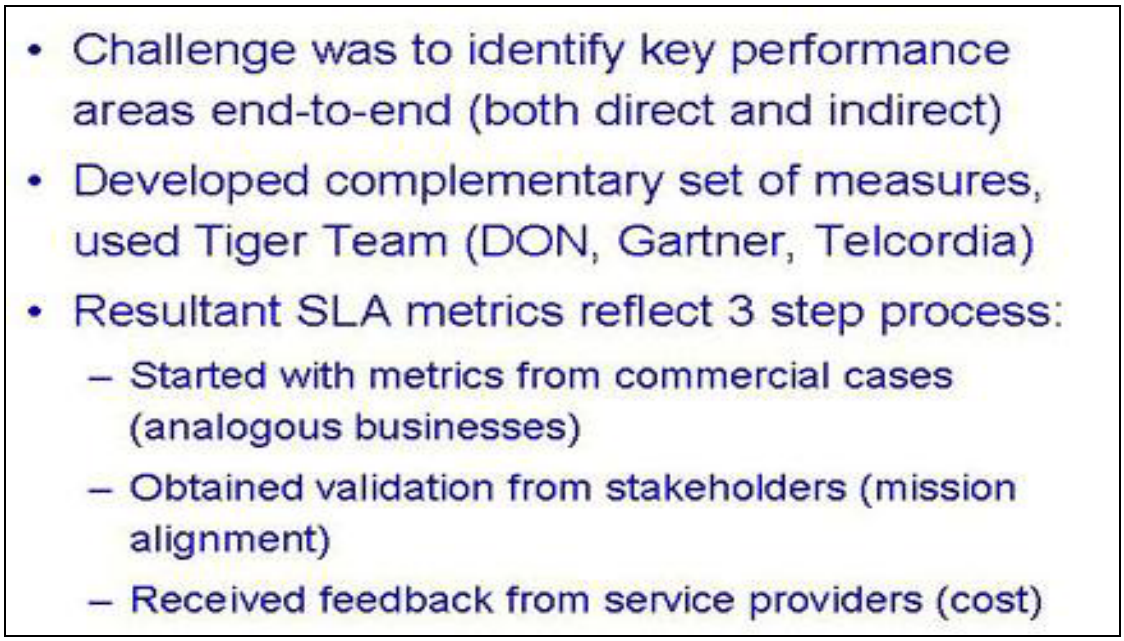


Figure 53: NMCI Challenges in the Development of the SLAs

b. SLAs and Related Metrics

When the initial contract was written down it included 135 metrics within 37 SLAs. Through the process of continuous adjustment there is now a total of 44 SLAs with 197 metrics. The complete description of the metrics involved can be found in Table D in Appendix D; however a breakdown with a short analysis of the metrics currently in use is shown in figure 54:

SLA	DESCRIPTION	SERVICE EFFIC.	CUST. SATISF.	INTEROPER.	SECUR.- IA	NETWORK OPER.	NUM. METRICS
1	DT HW and OS	YES	YES			YES	5
2	St. Office SW	YES	YES	YES		YES	4
3	E-mail Services	YES	YES	YES		YES	5
4	Directory Services	YES	YES	YES		YES	7
5	File Shared Services	YES	YES			YES	6
6	Web Access Services	YES	YES	YES		YES	4
7	Newsgroup Services	YES	YES	YES		YES	5
8		MULTIMEDIA CAPABILITIES: Deleted					
9	Print Services	YES	YES				4
10	NMCI Intranet Performance	YES	YES	YES	YES	YES	5
11	NIPRNET Access	YES	YES	YES			4
12	Internet Access	YES	YES	YES			3
13	Mainframe Services Access	YES	YES	YES			3
14	Desktop Access to Gov. Apps	YES	YES	YES	YES	YES	3
15	Moves, Adds, and Changes	YES	YES				5
16	SW Distribution and Upgrades	YES	YES			YES	4
17	User Training	YES					3
18	Unclassified Remote Access	YES	YES	YES			4
19	Classified Remote Access	YES	YES	YES			5
20	Portable WS Wireless Dial-in	YES	YES				3
20A	Org. Messaging Service	YES	YES	YES			4
21	Desktop VTC Services	YES	YES	YES		YES	6
22	Voice Communications	YES	YES			YES	10
22A	Voice Mail	YES	YES	YES			4
23	Basic Help Desk Services	YES					7
24	WAN Network Connectivity	YES	YES	YES		YES	5
25	BAN/LAN Com. Services	YES	YES	YES		YES	5
26	Moveable VTC Seat	YES	YES	YES		YES	7
26A	Proxy and Caching Services	YES	YES	YES		YES	4
27	External Networks	YES	YES	YES		YES	6
28	Network Management Services	YES			YES	YES	5
29	Operational Support Services	YES				YES	4
30	Capacity Planning	YES				YES	3
31	Domain Name Server (DNS)	YES				YES	4
32	Application Server Connectivity	YES				YES	4
32A	Network Operations Display	YES	YES		YES	YES	2
33	NMCI Security Oper. Services	YES	YES	YES	YES	YES	9
34	NMCI Sec. Oper. Services PKI	YES	YES	YES	YES	YES	4
35	NMCI Sec. Services -SIPRNET	YES	YES	YES	YES	YES	4
36	NMCI Sec. Planning Services	YES	YES	YES	YES	YES	4
36A	Integrated Config. Management	YES					1
36B	Integration and Testing	YES		YES	YES		2
36C	Technology Refreshment	YES					4
36D	Technology Insertion	YES	YES				2
37	Sea-Shore Rotation Support	YES					2
Total of SLAs: 44					TOTAL NUMBER :		194
SLAs that Span into all the Domains					To Include ROI, Financial Ratios		:197

Figure 54: The SLAs and Performance Measurements Matrix Currently in Use.

The initial idea of this thesis was that a number of metrics at the level of 200 were too many and would only complicate the monitoring activity; therefore a much shorter version should be used. After a thorough examination of the method used to evaluate the NMCI performance, the final conclusion is that an increased number of metrics is needed to precisely describe the level of services provided. Additional validation is provided by the fact that the approach used by the DoN to create the associated metrics was similar to the practices followed by the private sector, and feedback from a variety of sources was used extensively. Finally, the magnitude of the effort and the technical complexity of the specific IT initiative also suggest that a tremendous amount of detail is necessary to fully capture the performance of the network.

It is necessary to note that specific services are monitored via a combination of metrics that span all the categories of performance measures analyzed in the previous section. For example there are specific SLAs that introduce a large number of metrics to provide the full picture of the related activities, such as all of the NMCI security related agreements. Although the vast majority of the necessary metrics to measure and assess performance are already contained within the establish SLAs, with the precondition that periodically adjustments of the level is required to ensure to scope of this IT initiative, as an additional improvement it would be useful to allow the end-users to access the quality of the training services they are receiving by the contractor and to provide feedback on the operation of the helpdesks or their views towards the sea shore rotation policies. Finally, technology insertion and refreshment should account for both the commercial sector and the other military services pace in a joint operations paradigm, making the adjustment of the matrix necessary.

Under the NMCI contract, EDS is paid based on its ability to meet specific service levels on key measures, such as network uptime, availability of applications and help-desk response time. Upgrades to the systems are done on a scheduled basis at no additional cost to the government and payment is tied to service quality and customer satisfaction. The customer accepts less risk because an SLA makes the vendor responsible for meeting the target service levels, while the vendor gains the ability to manage customer expectations in a well-defined manner. Penalties could be imposed

when performance measures are not met. The SLAs generally should have three distinct components:

- What are the services to be provided
- What are the measured targets of service that the customer expects
- What happens if the service provider fails to deliver the service it promises

From the technical point of view, among the items that should be included in the service metrics are network performance and reliability, service availability intervals, mean time to report a failure, message delivery time, the number of closed trouble tickets, completion times for moves-additions or changes, the level of voice services, multimedia capabilities; and user training. Each criterion should include low, medium and high service grades and be priced accordingly. For example, a high network availability guarantee of 99.9 percent uptime would cost more per user than a low network availability of 99.5 percent uptime. NMCI's SLAs conform very closely to the above norm that prevails in the private sector through the distinction of basic, high level and mission critical subdivisions. Finally the metrics currently in use provide sufficient data to analyze the performance of the network with the help of automated software tools. The central point of management activity enforced by the NMCI approach facilitates the seamless monitoring activity of the network. A summary of the conclusions involved with the performance measures analysis is shown in figure 55:

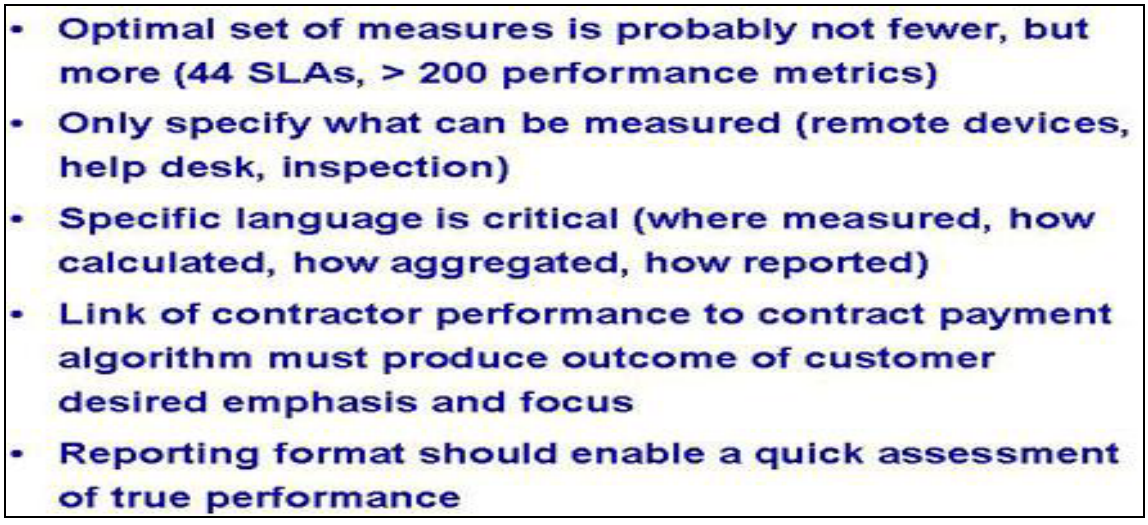


Figure 55: Summary of NMCI Performance Measurements Matrix

D. REASONS WHY THE END-USER IS UNCOMFORTABLE WITH NMCI

Reality as usual is very different from the planned in advance situation and when dealing with a change of that size, it is also logical to expect the creation of very different reactions within the DoN organization. There have been two major hurdles to overcome: the culture issues as people are forced to change the hardware and software they use or where they go for help-desk support and the massive number of existing legacy systems.

1. Cultural Changes Needed

In order to move towards the standard system, the NMCI implementing team must take users off personal computers and put them in front of standardized network terminals, in what is essentially a depersonalization of their desktop. There's a price to be paid for the increased security. You can't put your kids' pictures up as screensavers anymore because it's a security risk. Also there are cases that the idea of worse performance is just related to the end-users luck of knowledge for the whole NMCI concept. People tend to see NMCI only as a desktop rather than a full-service contract providing hardware, software, security, connectivity, service, repair, and the manpower to make it all work. It is the notion that the user "owns" his dektop that the Navy needs to clarify. The Navy needs to clearly explain the ideas involved with NMCI and its "enterprise-level" aproach.

There are many complaints expressed by a variety of users that NMCI has an inferior performance than the previous state of IT operation. To clarify the level of expectetions associated to NMCI, there is a need to stress that the introduction of the Naval Intanet is an effort to create uniform standards and performance for all those under the DoN. For those that were below the desired performance bar as it was determined by the central authority, a new better IT paradigm has emerged. For those that through coordinated activities and funding available were able to deliver a superb IT enviroment, NMCI means that performance is often degraded. For example:

- Longer logon times (often the main source of complaints and regarded by the non experienced user as indication of poorer performance in relation with the previous state of the network)
- Public Key Infrastructure (PKI) logon requires more steps and time associated with

Additionally, with the current state of NMCI, there is a great difference in the culture level expressed in terms of the conflict between increased security and depersonalisation of the desktop. Security might be the main point of focus but research into complaints articles for NMCI indicates that users don't like the NMCI concept or at least not filling comfortable with it because appart from removing the current existing non-secure protocols, it also forces policies that can be regarded as restriction of personal freedom. I will provide a short and certainly not exhaustive list:

- Incoming e-mails screened
- Security lockout after 15 minutes
- Websites blocked if non-secure practices are involved
- NMCI limits wireless and PDA options
- "Top to the Bottom" standardization and centralization, which limits local flexibility and even more creates the impression that the user is not using his/her "personal" computer
- Desktop is "Locked Down"
    - Can not download Freeware, Shareware, or Games
    - No CD ROM installs by individual users

To ease the cultural adjustment and provide training for the new NMCI system, EDS provides both an e-learning system and a two-tiered help desk approach. The web-enabled training system is quite effective. The system is continuously updated with issues derived from user questions to the helpdesk. Help desk tier I takes all user calls, but deals only with problems that tend to be resolved easily. If not, they are escalated to tier II, where staff with more technical experience answers questions, but unfortunately the long waiting time involved with the handling of complex issues are creating the impression that the help-desk is only solving the minor problems and end-users still complain that support is not enough. The current state of the NMCI performance is still lagging from the DoN targets. However, end-user's surveys show that satisfaction level with NMCI increases as time passes and research associated to the introduction of different IT capabilities in large scale organization indicates that customers get accustomed to any new system in the long run; however this process can take a couple of years. Change management practices are necessary to facilitate the transitioning period.

2. The Legacy Applications Issue

A second point of interest is the progress with the legacy applications. The NMCI request for proposals called for a single operating system network. As a result anything that is not functional under a Microsoft Windows 2000 environment must be quarantined or connected via CLIN 32 (external network connection) or CLIN 29 (legacy system support). DoN and EDS officials have been bogged down for a very long time in reviewing applications to determine if they are necessary and, if so, testing them to ensure that they meet security requirements.

The ISF has already established a Legacy Application Working Group to determine the processes necessary to move legacy applications into the NMCI environment. The process will include recommendations to the DoN on where it can reduce reliance on legacy systems. NMCI offers the DoN an opportunity to employ a state-of-the-art infrastructure, reduce the number of legacy applications and expand standardazation throught the whole DoN. Unfortunely it is again the end user that will face all the pain since new restrictions will be effective but he/she will still have to perform all the variety of "old" functions with the means of mismatching tools. The legacy issue also fed the culture issue because NMCI forced users to abandon well-worn applications, and they were often reluctant to do so, often without an alternative option.

E. POTENTIAL WEAKNESSES AND VULNERABILITIES IN TERMS OF INFORMATION ASSURANSE (IA)

NMCI has established a service level management program that monitors the performance of the NMCI network and the related security features. This performance is contractually binding and contains incentives for the contractor to exceed performance, security, and customer satisfaction parameters. Independent government teams monitor performance for compliance to the SLAs and requirements, while special "red teams" routinely assess network security. While perfect security in an information-sharing environment is almost impossible, there is much that can be done to minimize system vulnerabilities or potential threats. DoN uses a Defense in Depth (DiD) strategy that employs state of the art protection technology like content monitoring/filtering, firewalls, intrusion detection systems (IDS), encryption and PKI [Note 2] installed in a layered system of defenses to protect the NMCI.

Protection Tool	Confidentiality	Integrity	Authenticity	Availability
Firewalls and Packet Filtering	Yes		Yes	Yes
Intrusion Detection	Yes		Yes	Yes
Content Filtering		Yes		Yes
Virtual Private Network (VPN)	Yes	Yes	Yes	
DoD PKI Enabled Applications	Yes	Yes	Yes	
Encryption	Yes	Yes	Yes	

Figure 56: NMCI Tools Protection Matrix, from the NMCI Contract N00024-00-D-6000, (Confirmed Contract P00080)

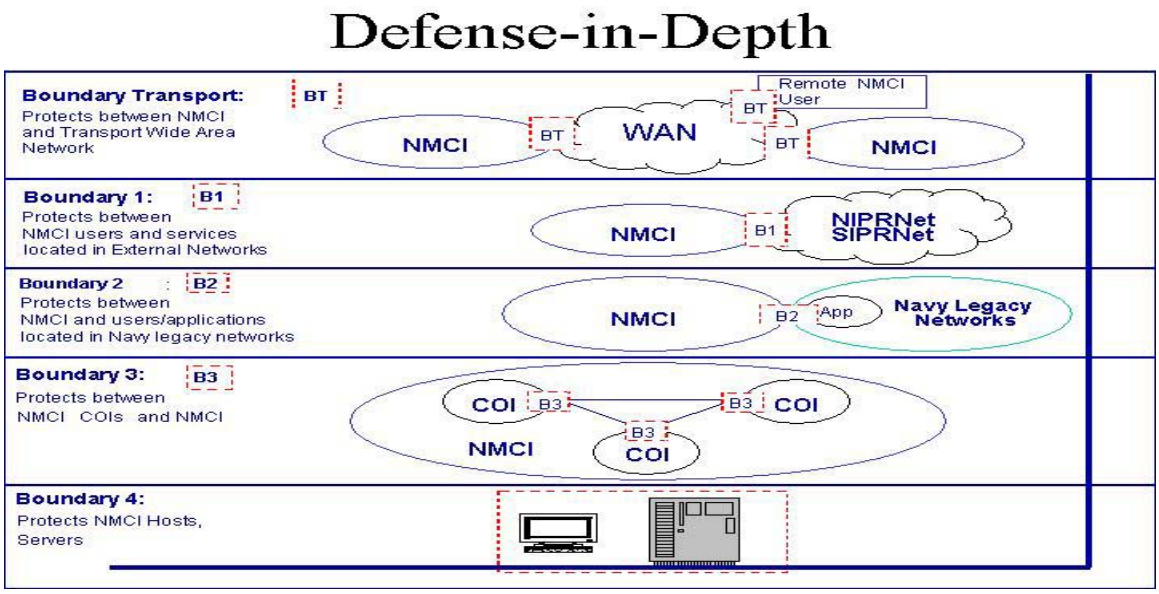


Figure 57: NMCI Layered Defense

The Naval Network Warfare Command (NAVNETWARCOM) determines the overall NMCI IA strategy and ensures its alignment with the equivalent DoD strategy. By focusing on Computer Network Defense (CND), with emphasis on Defense in Depth, the effort is to deliver a sound network. There is a mixture of DoN personnel and EDS' employees within every NOC to facilitate network security activities, both offensive and defensive. Responses to network threats and attacks constitute Information Warfare (IW) defense command decisions that, as a minimum, will be authorized by designated, uniformed DoN personnel. The Navy's command structure retains directive authority over all NMCI threat responses. DoN personnel are also the conduits for authorized responses to directives received from JTF CND (Joint Task Force Computer Network Defense) or joint service regional headquarters for coordinated joint service response to

threats. As the Information Condition (INFOCON) level is raised during time of conflict, DoN personnel will retain the command decision authority. The security safeguards that DoN receives with NMCI include: (www.nmci.navy.mil (IA and Security), accessed February 2004)

- **Detection**
  - 24x7 surveillance against unauthorized intrusions
  - Defense against internal as well as external threats
  - Inoculated system with world-class anti-virus detection tools
- **Inspection**
  - Continually monitoring the network and assessing potential threats to the IT environment
  - New tools and activities to inspect and protect systems
- **Protection**
  - State-of-the-art firewall protection
  - High level of protection standardized across the whole Department of the Navy
  - Comprehensive password procedures to safeguard information
  - Implementing Information Assurance
- **Reaction**
  - Alerts security personnel of virus contamination 24x7.
  - Quarantine contaminated files, limiting potential damage
  - Automated reports of unauthorized intrusions to the Navy and Marine Corps security teams.

The creation, operation and use of information infrastructures for productive ends involve three principal types of activity (Gregory J. Rattray (2001), *Strategic Warfare in Cyberspace.* Massachusetts-USA: The MIT Press, p. 32):

- The development and use of underlying technologies, including hardware and software products and orchestration of standards and protocols used
- Provision of networks and services that link underlying technologies to provide information processing, storage and transmission capabilities for a wide range of users
- Use of information technologies and networks by individuals and organizations to perform desired tasks

An organization like the DoN should conduct all three type of activity simultaneously to optimize an IT system like NMCI for its requirements, but coordination of activities to deliver a completely secure structure is extremely difficult. The complexity of the technologies involved has resulted in the involvement of a multiplicity of different organizations (beyond military control) in the creation of the NMCI and although the approach used might have established a very strong security mechanism, there are still potential threats. A summary is shown in figure 58:

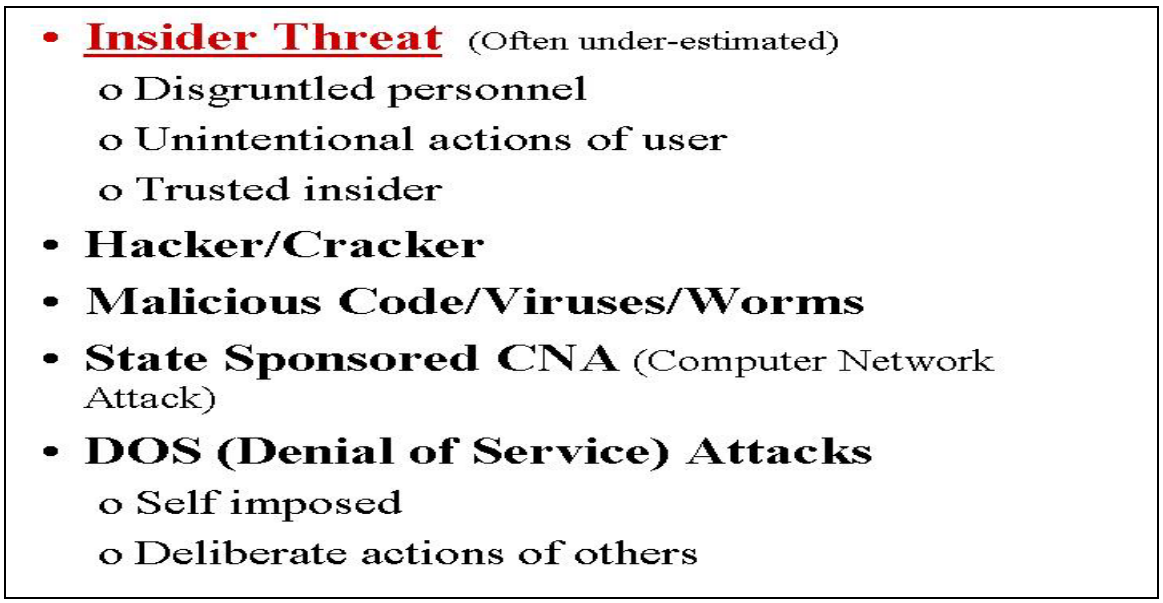


Figure 58: List of NMCI Potential Threats

Naval networks are not immune from hackers or malicious code and are a prime candidate target for state sponsored attacks. A wave of destructive worms has focused attention on the potential vulnerability of the NMCI and other military networks to malicious computer attacks. In particular, the Blaster, SoBig, Welchia and other worms

have spurred concerns about the unintended security consequences of the overwhelming worldwide use of and the increasing military reliance on the software products of a single company, Microsoft. The worms, viruses and Trojan horses mostly spread throughout corporate and personal computer systems through security flaws in the design of products from Microsoft, notably its Windows operating systems. To date, all branches of the U.S. military have consciously decided to standardize their enterprise networks on Microsoft products. As a result, military network engineers are discovering that the biggest threat to the integrity of their enterprise systems comes not from a coordinated cyber war effort, but rather from malicious code designed to spread as quickly and thoroughly as possible via Microsoft design flaws.

In addition to the external threats that any network has to deal with, the Insider Threat to the NMCI should not be discounted or underestimated. Included in that threat are the accidental or unintended actions that can undermine network confidentiality, integrity and availability. Public Key Infrastructure (PKI), client intrusion detections, Active Directory Control and a host of other systems provide protections against the insider threat; however an "authorized user" can always undermine the security effort. It is still under question the level of the end –user training and their adaptation in the "best use" practices that can both make a significant difference. Additional, there is always the question of a dissatisfied EDS' employee holding administrative privileges over the NMCI.

While IT increases capabilities in the military domain, it also creates an increased reliance on the infrastructure necessary to support the associated networks. The threat to the GIG is extensive, increasingly sophisticated and a real danger to [the U.S.] national security. The threat includes nation-states, more than 40 of which have openly declared their intent to develop cyber warfare capabilities. It includes transnational and domestic criminal organizations, amorphous groups of hackers who sympathize with America's enemies, and terrorist organizations, as shown by what the DoD has learned by forensic analysis of captured computers. It may also include insiders—trusted Americans who become traitors. (Major General J. David Bryan (Vice Director of Defense Information Systems Agency), article *"IA: Holistic View, Targeted Response"*, Military Information Technology, September 2003).

F. ENDNOTES

1. An interoperability test plan to test the validity of each segment was provided by the contractor. The test plan provided measures of interoperability with respect to: Services such as Standard Office Automation Software, E-mail Services, Directory Services, Web Access Services, Newsgroup Services, NMCI Intranet Performance, NIPRNET Access, Internet Access, Mainframe Access, Desktop Access Government Applications, Unclassified Remote Access, Classified Remote Access, Organizational Messaging Services, Desktop VTC, Voice Communications, Wide Area Connectivity, BAN/LAN Communications Services, Moveable Video Teleconferencing Seat, Proxy and Caching Services, External Networks, SIPRNET, and Public Key Infrastructure (PKI).

2. A firewall is a collection of hardware and software components that is used to provide protection for a defined set of users in a specified DoN's enclave. There are different types of firewalls such as state monitoring firewalls, application layer proxy firewalls, and router-based firewalls. The DoN has chosen to implement application layer proxy firewalls at all entry points of the NMCI, therefore firewalls can be at boundaries 1, 2, 3 and 4.

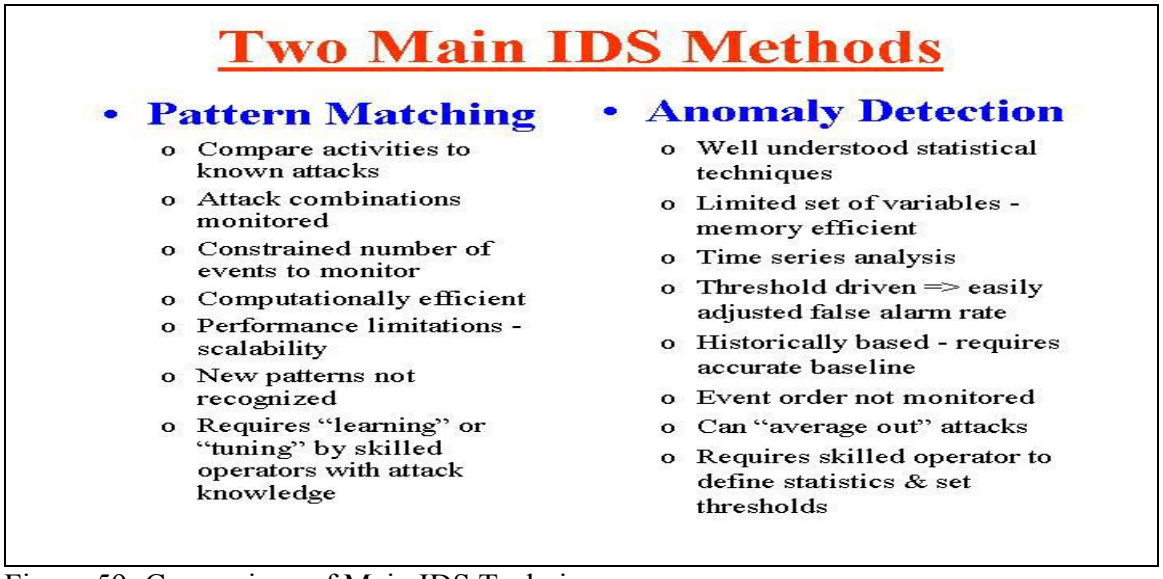


Figure 59: Comparison of Main IDS Techniques

NMCI incorporates both network and host-based IDS as part of the layered defense in depth strategy. Although a host based monitor can examine internal state

information that does not flow over the network, thereby tracking insider misuse and attacks that slip past a network sniffer (Network based IDS), both types of monitors are potentially vulnerable to bypass and sabotage, (Denning, p. 366) [an option open to a determined insider.]

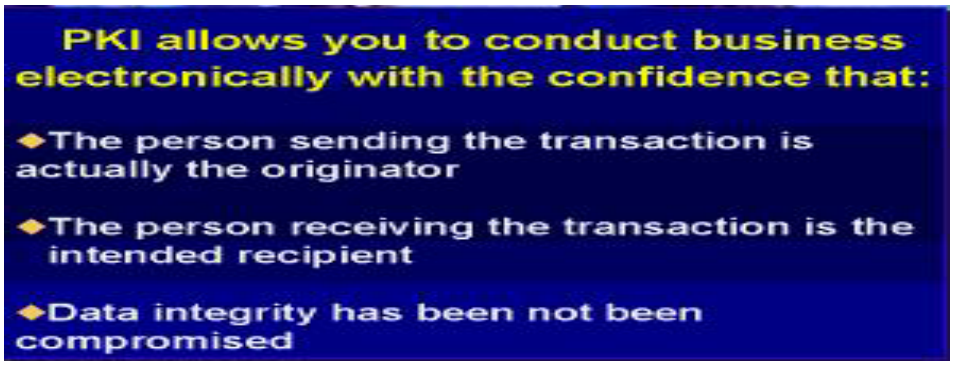


Figure 60: Why NMCI is Using PKI

Figure 61: Service Taxonomy via Encryption-PKI and Digital Signatures

Content monitoring is already used within the NMCI to provide another layer of defense. The NMCI incorporates content filtering products and techniques, because many forms of electronic information can contain harmful content such as viruses, worms, and Trojan horses. This “malicious code” can be transmitted across a network in a number of ways including SMTP email attachments, FTP file downloads, and Java applets. Numerous COTS products exist that can check these routes to identify such potentially harmful content. If properly configured and frequently updated, these tools can identify harmful content before it has the chance to do any damage, and in many cases can repair already damaged files. (NMCI Contract N00024-00-D-6000, (Conformed Contract P00080), Attachment 4, p.12)

V. CONCLUSIONS AND RECOMMENDATIONS

Network-centric warfare (NCW) establishes the idea that networks, as warfare enablers (force multipliers), are becoming increasingly necessary and important to the modern military. FORCEnet is a transformational architecture for the Navy and Marine Corps that integrates sensors, networks, decision aids, weapons and supporting systems into a highly adaptive human-centric maritime system that operates from the seabed to space and from sea to land. To secure future readiness and achieve knowledge superiority requires the horizontal integration of NMCI and IT-21, including an effective management of the associated data flow. FORCEnet is intended to be the seamless link to conduct Joint Forces Operations and even accommodate expansions that fall within the Allied/Coalition Forces domain. The Navy Marine Corp Intranet (NMCI) is a critical element on the path towards FORCEnet by providing synergy through network integration and facilitating knowledge management at the DoN level.

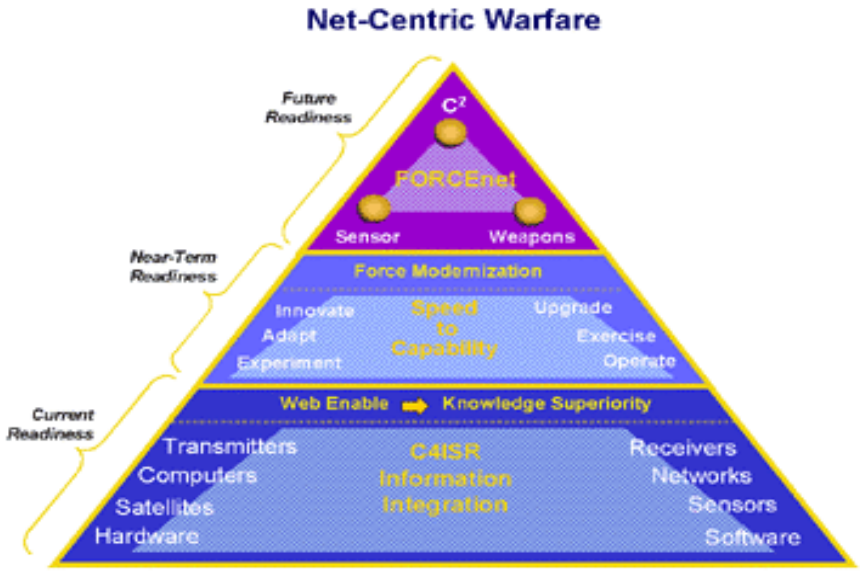


Figure 62: The Road towards FORCEnet, from www.forcenet.navy.mil (What is FORCEnet?), accessed February 2004

NMCI's mission is to plan, coordinate and align the DoN's information infrastructure (enterprise systems and data) under a single, coherent and forward-looking strategy. The driver for NMCI is to provide war-fighters and decision-makers the right

information at the right place at the right time. Through a single service contract, NMCI will provide end-to-end connectivity for all Navy and Marine Corps personnel with voice, video and data services. NMCI is the foundation that will enable DoN-wide web-based processes, knowledge management and e-business solutions. With NMCI and new approach of "IT as a utility", apart from dealing with the "bandwidth-starvation" problem, the DoN is expected to achieve greater efficiency and effectiveness in all facets of naval operations and to become a relevant, current and highly sophisticated player in the new "digital-type" economy. Web-enabling the Navy is vital for access to more effective business and combat applications.

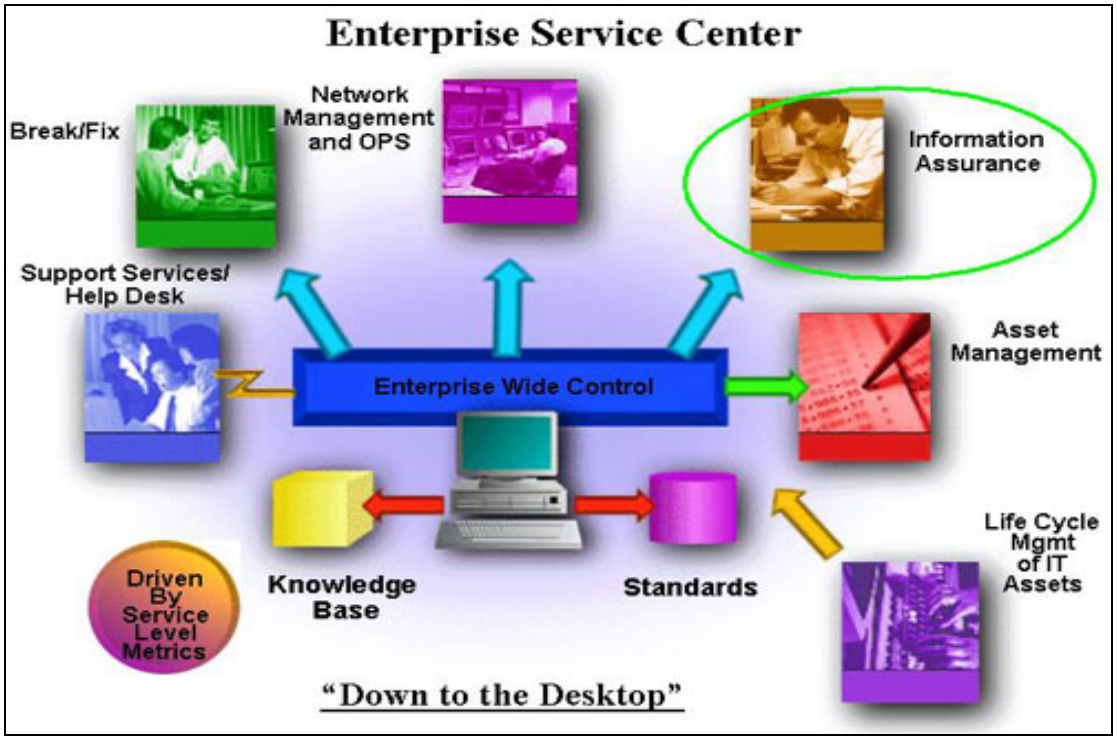


Figure 63: The IT as a Utility Approach

A. NMCI AT THE DON LEVEL

The NMCI implementation effort and the initial performance of the Intranet have often been below the DoN's expectations and visions, therefore offering the opportunity for severe criticism. For example, lack of change management practices resulted in a hostile behavior from specific users, as was the case for those that were forced to use two separate desktops on their desk to perform exactly the same job as before. Obviously, this "dual desktop" phenomenon did not provide a suitable working environment to the workforce and had a negative impact on the users' productivity.

Research of articles that describe end-users' complaints related to the early stage of the NMCI shows that very often requirements or expectations of special users groups were poorly addressed or not taken into account at all. The initial training provided by EDS to the users in the majority of the cases was not sufficient and the help-desk personnel had minimum "hands-on" experience. Often the new procedures were not explained adequately enough to the end users before declaring the operational status of the site. As a result users choose to avoid the help-desk and direct complain to the NOCs personnel with the hope that their demands for technical support would be solved faster.

In a specific number of commands, the IT operational environment was already extremely high and the introduction of NMCI destabilized the already effective IT functionality. As a direct result, the negatively impacted users lost their confidence in NMCI and the reputation of the program within the DoN community diminished. In the next facility scheduled to join the Intranet resistance to accept the implementation was increased and additional time was necessary to overcome "cultural" obstacles. In most of the sites, transition to the "cutover" required additional time and resources than the normal IT staff, resulting in degraded IT support at the early stages. Many times there were inconsistencies among the technicians implementing the infrastructure. Finally, in a variety of sites the EDS processes and instructions to the technicians were incompatible with the DoN practices, and an extended timeframe along with a revised technical approach were necessary.

However, after all the NMCI is an "IT equalizer" effort and an attempt to enforce a centralized decision mechanism on IT acquisition. Complains are still present, because the NMCI introduction has created a certain number of users that under the "cumulative" approach receive a reduced level of IT services than when commands were individually responsible for IT support. Experience of EDS and the DoN with managing the NMCI introduction has improved dramatically within the last year, although some of the same types of mistakes were repeatedly made. Despite some of the negative views that still remain within specific groups of users, NMCI is not only making steady progress but also the DoN is slowly discovering the promised benefits from its decision to tackle information technology acquisition in a more innovative way. The vast majority of NMCI users are satisfied with the new infrastructure, according to survey results released by the

NMCI director's office in the year 2003. Overall satisfaction is higher than 70 percent and is increasing as time goes on and more users are moved over to the system. The end state objectives of NMCI can be summarized as follows:

- Replace diverse Navy networks with single enterprise-wide network
- Improved security across the DoN enterprise
- Common "look" of the desktop
- Regular technical refreshments
- Implementation of Public Key Infrastructure (PKI) and introduction of a records management
- Create shore IT infrastructure to allow conversion to e-business model of common corporate applications and databases
- Affordable IT management within existing DoN budget
- Enable innovation

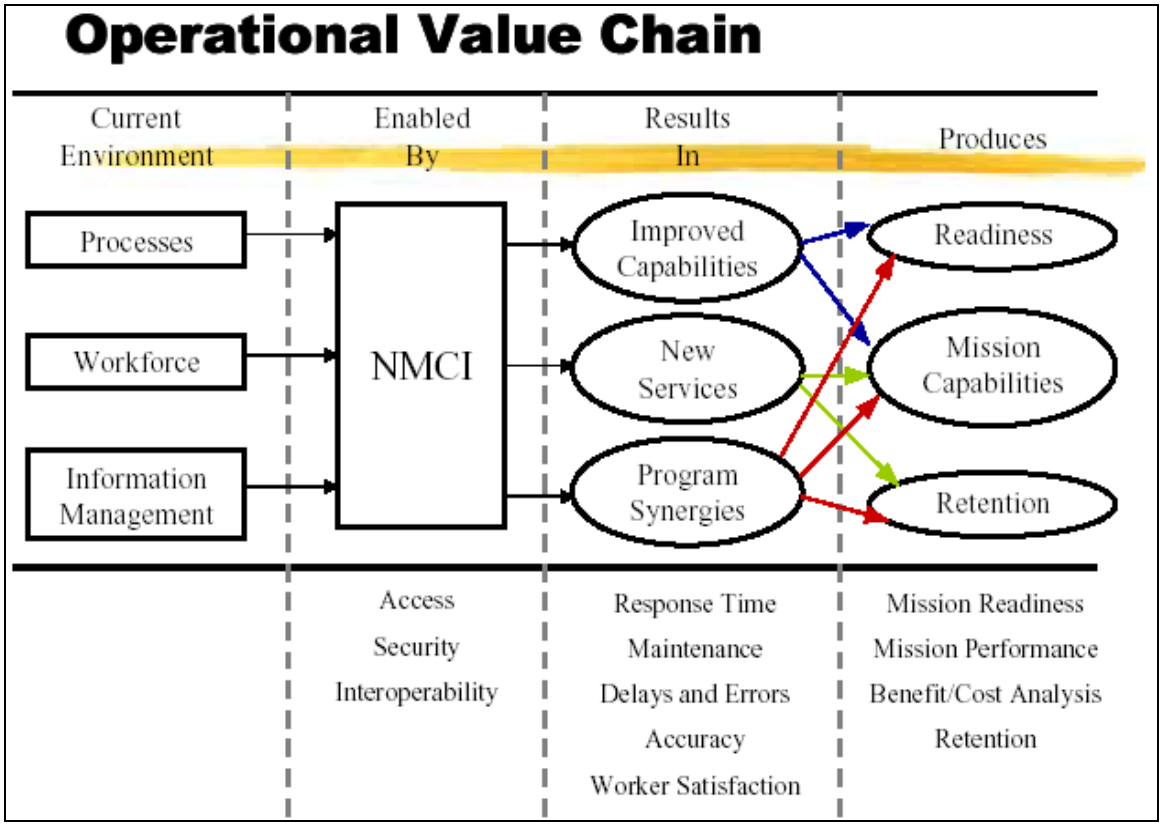


Figure 64: The NMCI Operational Value, from the NMCI Contract

At the moment, NMCI offers:

- Completely automated IT asset management
- Application standardization at the "Enterprise" level
- Increased security posture and improved data management
- Automated backup and restore of data
- Automatic service desk problem management and resolution

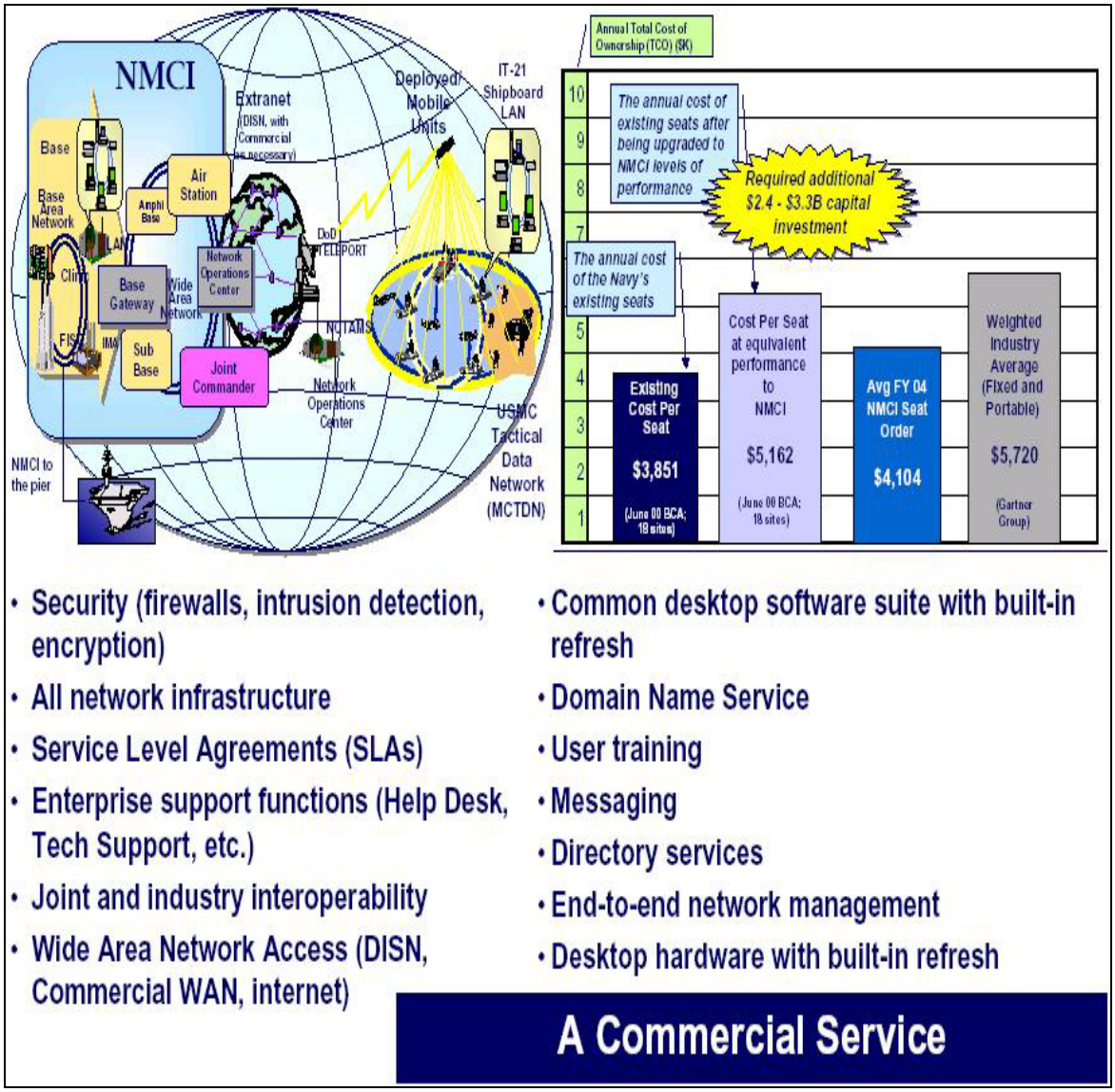


Figure 65: Description and Financial Bennefits of NMCI for the DoN, from Rear Admiral Chuck Munns, U.S. Navy, NMCI briefing at the SPAWAR-Industry Day, San Diego-USA, 23rd October 2003

A summary of the NMCI benefits is shown in Figure 66:

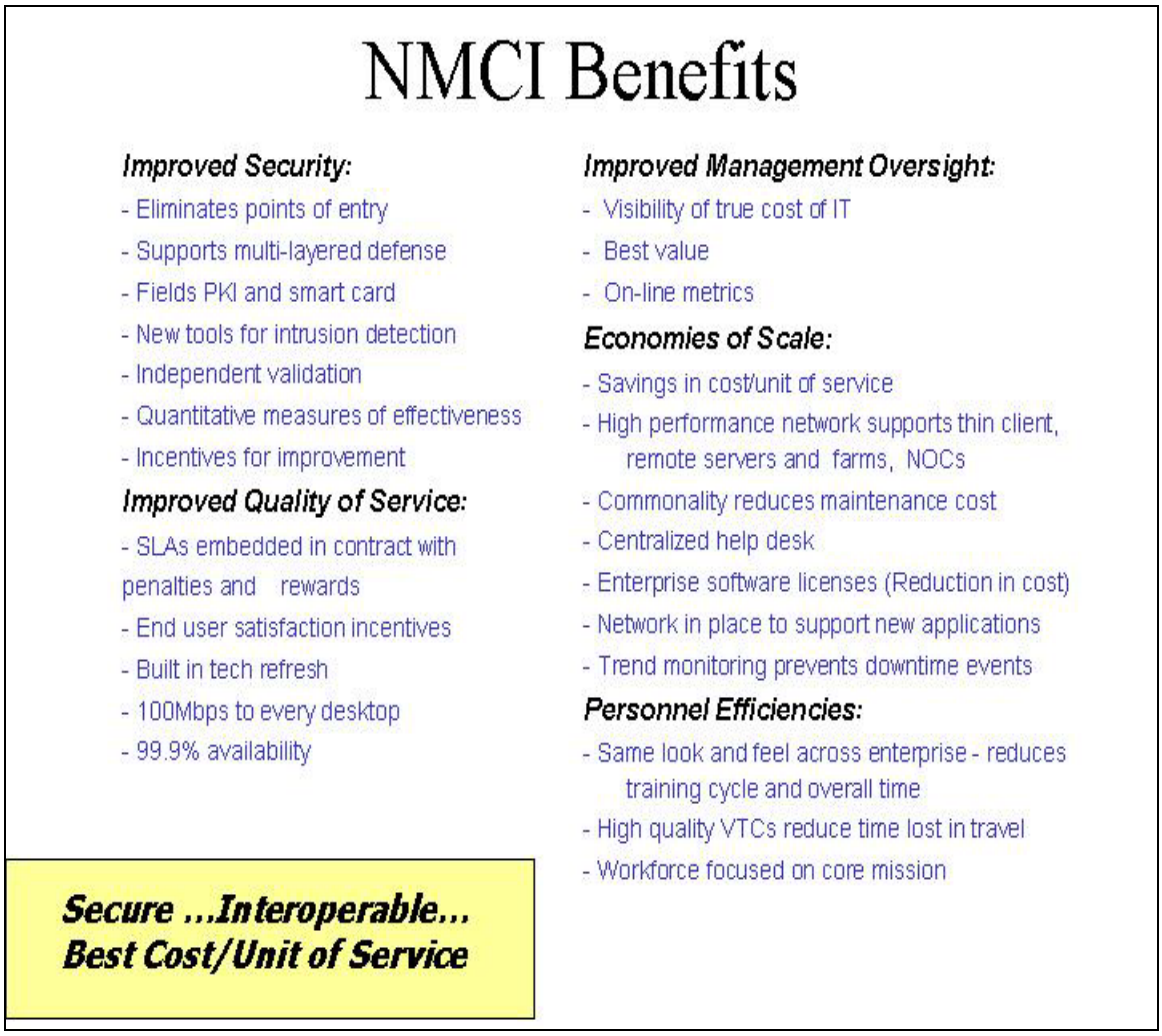


Figure 66: Summary of NMCI's Benefits

Currently in the final stages of deployment, there is a much more mature approach towards the NMCI managing activity. The NMCI enhances security, improves standardization, reduces duplication of data and introduces well-coordinated back-up practices. Finally, the NMCI approach has the potential to reduce IT support costs while giving the Navy and Marine Corps universal access to integrated data communications and videoconferencing capabilities. The Intranet is now operating at a more balanced level and helping to speed up a variety of activities that support the DoN's mission, from administrative tasks to ammunition supply. The common network capability provided by NMCI is finally increasing combat readiness and effectiveness, through an "enterprise-wide" approach. For example, the introduction of the Navy Marine Corps Portal (NMCP)

will provide an integrated, collaborative environment with personalized, role-tailored access of information in real time for the NMCI users. A single integrated portal structure will allow DoN organizations to focus solely on content delivery and avoid the costs of individually developing portal features and functions.

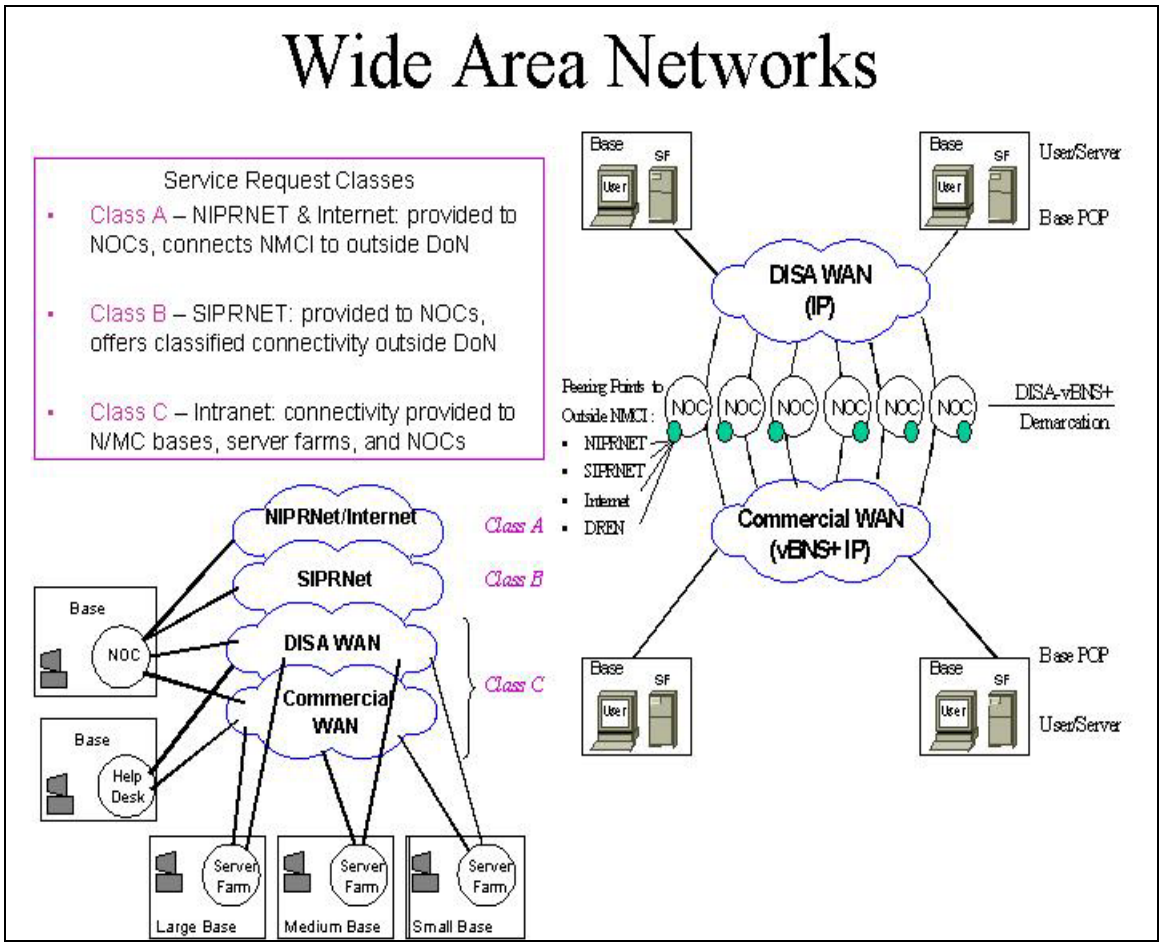


Figure 67: The Architecture and Connection Points of NMCI

After the 360,000-plus data seats for NMCI are completely cut over, which EDS plans to finish within the year 2004, the Navy and the vendor will begin work on the enterprise voice and video components that are another "neglected" critical element within the NMCI approach. The "voice" portion of NMCI has been shifted to a later date of implementation to keep pace with industry's transition of quality voice over Internet protocol (Voice over IP). VoIP means that phone numbers are no longer tied to an individual handset, ideal for workplaces where employees hot-desk. Each person can be

assigned a phone number, which goes to the nearest phone whenever they log into the computer system.

1. The Current Stage of the NMCI Implementation

At the time being, the ISF has assumed responsibility for a little over 300,000 seats, with more than 160,000 seats already moved to the cutover stage. Three network operation centers are fully operational: San Diego, California; Oahu, Hawaii; and Norfolk, Virginia. A center also is almost complete at the U.S. Marine Corps base in Quantico, Virginia and help desks are in place in Norfolk and San Diego. During the startup years of the NMCI program, challenges have surfaced primarily in legacy applications but also in terms of change management. However, by working in a more coordinated manner with the ISF and with the NMCI supervising team now more mature and experienced, the DoN has employed some creative solutions to address these issues, hence the progress of the NMCI continues.

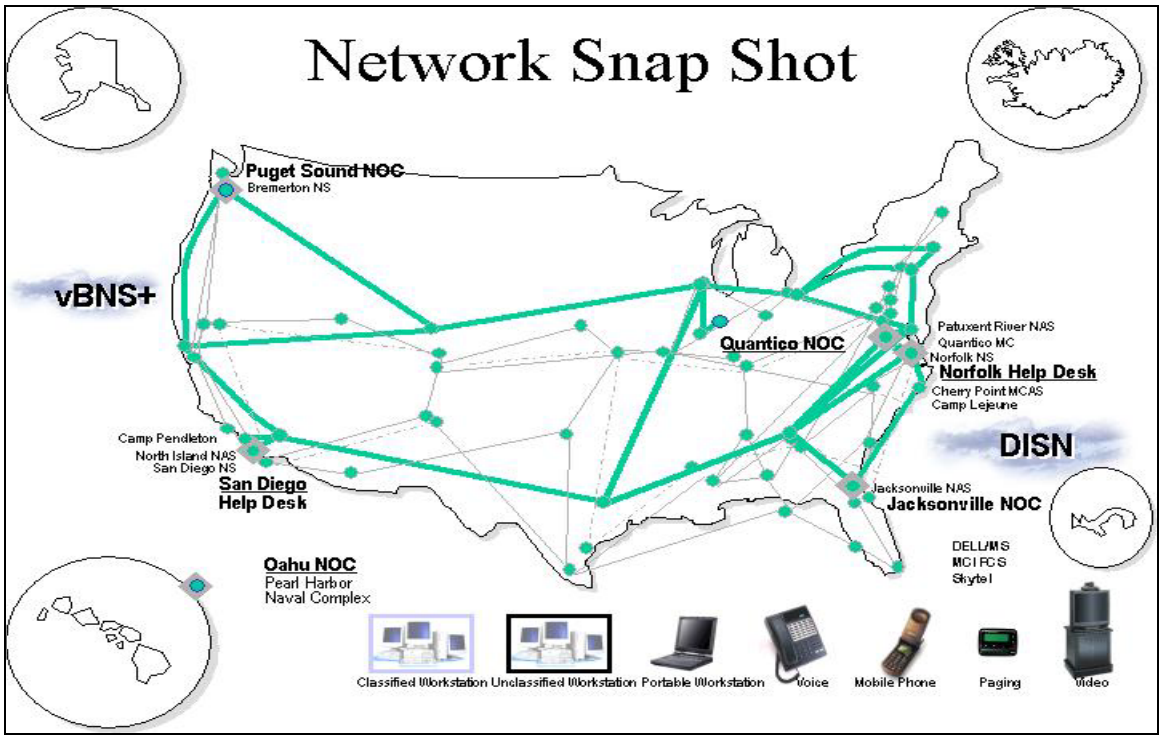


Figure 68: NMCI End State, from Captain Chris Christopher, U.S. Navy, NMCI Briefing for the Joint Logistics Council, USA, 29 March 2001

NMCI contract's coordinator EDS Corp. announced with its last dismal quarterly financial report that the company never expects, up to the seventh year of the contract, to

realize a profit from the multibillion-dollar project, and the company is now in a relatively weak financial position. Improving the NMCI's service levels should be a top priority for EDS, which can receive significant financial rewards if 85 percent or more of NMCI users report that they are satisfied with such items as help-desk responsiveness and network performance.

Many times, the EDS' approach was flawed or unrealistic, and in dealing with the entire Navy and Marine Corps all at once, the company faced severe resistance and in the majority of the cases outright hostility. Changing the paradigm from computers as individual property to a point of service is a major shift, and it has been an issue that had to be addressed at every site. Each installation facility had its own history and culture that resulted in a peculiar behavior regardless of what the DoN guidelines were. EDS also plowed into a thicket of legacy applications. However, the blame is not only for the EDS side. The biggest problem with NMCI, which the company won in October 2000, was that neither EDS nor the Navy knew the full scope of the challenge.

The discovery of thousands of legacy applications on obsolete computers vastly complicated the project. Neither the DoN nor the vendor had any idea how many applications would have to be dealt with and unfortunately it turned out to be at the 100,000 level. In order to deal with the problem and continue with the creation of the Intranet a variety of techniques like the "quarantined seat" and "dual desktops" approach [Note 1] were used as shown in figure 69.

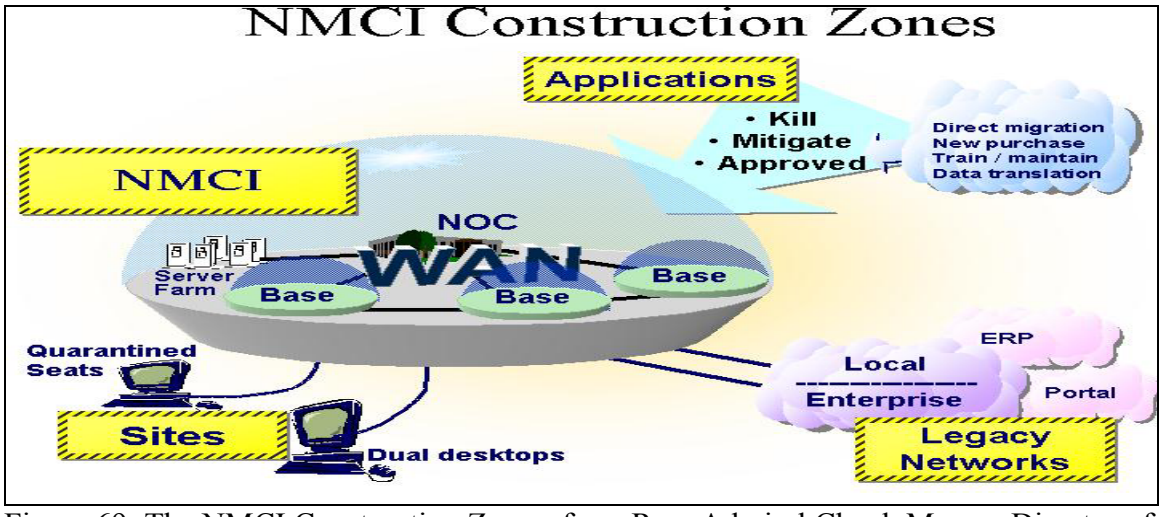


Figure 69: The NMCI Construction Zones, from Rear Admiral Chuck Munns, Director of NMCI, NMCI Progress Briefing, at the NMCI – Industry Symposium 17 June 2003

Finally, EDS may have underestimated Navy and Marine Corps network configurations complexity or undervalued its bid on purpose, hoping to a stream of profits from the additional services offered to the DoN. EDS wouldn't be the first company to price products on a large project at a loss, counting on customers to load up on expensive options. But the slow pace of the NMCI implementation resulted in very few additional services to be ordered by the individual commands and the NMCI bid evaluators weren't fools. The DoN got a great price on a truly transforming project that forced what the senior leadership believed was necessary changes. The SLAs have worked in favor of DoN up to now and the logical conclusion is that even with the various mishaps and inconveniences, the Intranet is an extreme valuable asset to the Department, which should be willing to continue its business relationship with EDS. The experience that EDS has already acquired through implementing and operating the NMCI is the most valuable foundation for the future NMCI success. It would take a tremendous amount of time to rebuilt "trustworthy" relations with a different vendor, (who might also repeat EDS' mistakes).

Both vendors and government agencies should be realistic in pursuing outsourcing and performance contracts. Winning only to lose isn't a formula for sustained success on either side. Based on the idea that the NMCI project and the associated benefits are extremely valuable for the DoN, whatever the NMCI's ultimate outcome, there's a lesson here: There's a lot more to service-level agreements (SLA) than gathering metrics or monetary incentives and penalties. There should be a strong involvement from the DoN personnel in the technology selection/refresh of the contract. Planning and continuous reviews are necessary in order to insure that the NMCI approach is executed properly. At the initial launch of NMCI, there was an over reliance on EDS to deal with all aspects without any strong support from the DoN. As a buyer of services to be delivered under an SLA, the DoN must be as involved and proactive as it would be under a normal service contract.

IT managers should consider when buying services under an SLA (www.computerworld.com (How to Buy the Best IT Performance), accessed March 2004):

- Technology proposed for a project
- Measurement criteria for the SLA
- Frequency of measurement
- Frequency in reporting
- Request regular periodic reviews

The execution of the NMCI contract has proven a financial drain for EDS' resources. There is always the possibility that it is the contractor not the DoN that might step away from NMCI. Setting realistic SLA goals will go far in achieving overall success. Making it too easy usually means that users or the parent organization aren't getting their money's worth; making it too difficult will increase expenses and cause problems in the relationship with the vendor. The data gathered from the operational evaluation must be compiled with other information that is being collected and used to determine how to make improvements by adjusting the SLAs if necessary.

The conclusions of the operational evaluation should be the new basis to establish a feasible SLA level that fully conforms to the DoN requirements and at the same time delivers value to EDS. Along the same lines; there is also a need to provide clarity in the NMCI future budget. Concerns over the difficulty of identifying the total cost of the NMCI effort in the DoN budget documents have been repeatedly expressed. Apart from renegotiating the SLAs, another possible solution for the NMCI future would be to provide additional finance by using funds already allocated for older IT procurement programs that the NMCI will supersede. Renegotiation the Voice and Video aspect of the NMCI might also be necessary, because of the delays involved. Also economies of scale could be present via reducing telephony costs through the VoIP introduction.

The main idea of this thesis is that that the IT initiative is very close to the point to deliver the promised intangible benefits and added value to the DoN enterprise. If necessary, additional resources can be allocated to further stabilize and improve the operational state. NMCI will enable connection to the U.S. national infrastructure, extend sharing and creation of knowledge and expertise worldwide, and change the way training is conducted. On the other hand, there still are a significant number of related activities

that need to be completed before enjoying the full NMCI benefits and justifying the need for an increased budget:

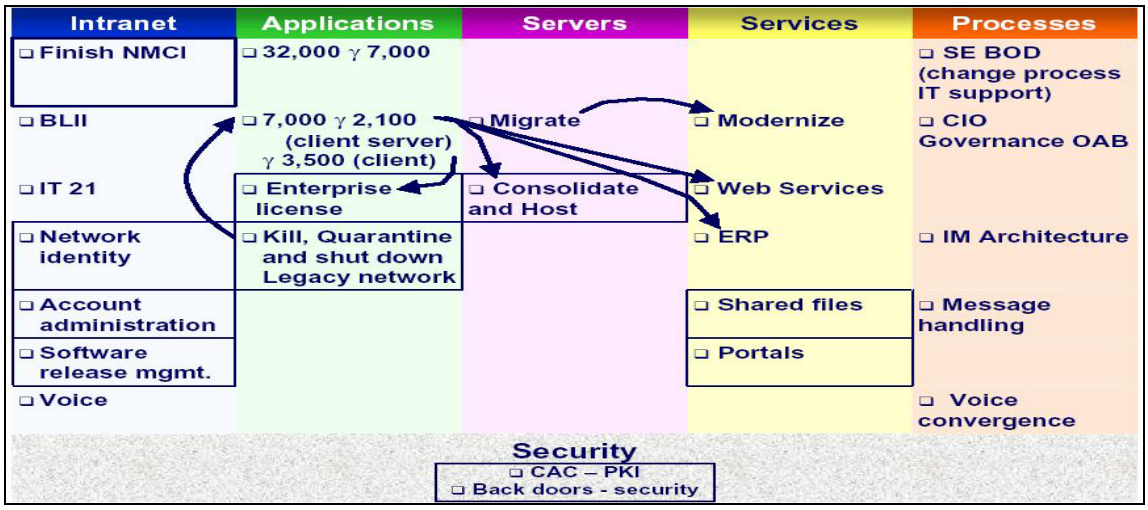


Figure 70: Activities to Supplement the NMCI, Rear Admiral Chuck Munns, U.S. Navy, NMCI Director, at the SPAWAR Industry Day, San Diego-USA, 23rd October 2003

2. Cultural Adjustment and the Legacy Issue

It is necessary to demonstrate crystal clear to the end users that the future will be better. Up to the year 2003, DoN had whittled down its 100,000 legacy applications to almost 30,000, through a process of eliminating duplicate or obsolete software. That's still not enough, when you consider that the Marine Corps are now operating with only 320 legacy applications.

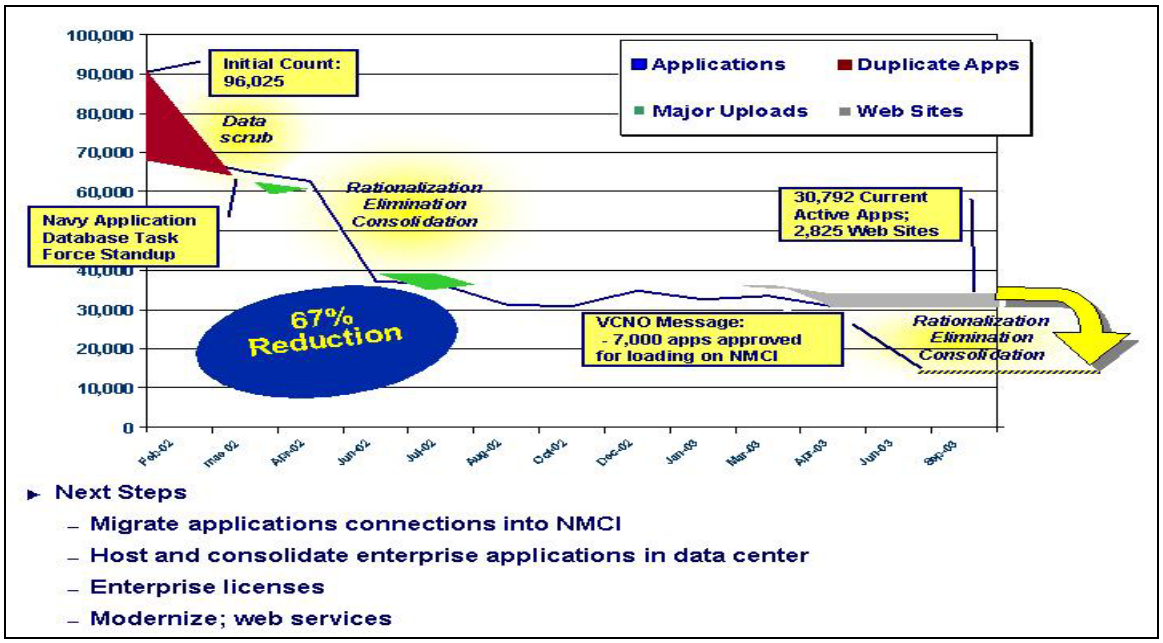


Figure 71: The Reduction of Legacy Applications

It is crucial to point out the importance of the legacy integration. The longer the DoN supports systems outside of the NMCI security umbrella, the longer a potential malicious entity could take advantage by exploiting those vulnerabilities. So there's a real need for speed to get everything inside the NMCI boundaries. Even if everything is not working perfectly in NMCI, being inside that security perimeter is the really important for security and probably the only way to significantly raise the defense levels.

But it is not only necessary to remove applications logistically from the inventory. Based on the results of the FAM evaluation that was described in chapter three, effort should be given in order to develop new applications in the NMCI setting to replace those legacy ones that are considered of extremely high value. The users then will be more willing to embrace NMCI if they have tools necessary to do the job and adequate training is given. Instead of managing the "Legacy Inventory" in a top to bottom approach, there is the solution to redesign and deploy the necessary applications within the Windows OS environment of NMCI, by adapting commercial available tools as the basis of the business rules used. That means that instead of conforming software to the DoN business rules, there is also the option of slightly adjusting the business rule to conform to the already available applications of the commercial sector. Enterprise Resource Planning (ERP) could be the best example of this type of activity, and the DoN should be committed to make the current pilot programs a complete success.

Another point of interest is the help-desk function provided by EDS. It is not only necessary to improve the quality of service by the personnel involved, but also to consider the user's view. The user needs support right now without having to wait in a telephone line. If the majority of questions cannot be answered locally then a highly specialized team should be created to deal with complicated tasks. Even more they will be able to take advantage of lessons learned, since statistically the same type of problems will happen again, and they will have the necessary experience by solving it the first time. In addition phone based or web based automated guides should be provided to the user in the form of "self-help", with the option to talk with help-desk representatives, if the user is still facing a problem. What I am suggesting is an organization of help-desk service in a form of multiple tier, where the central zone has the talented people for the difficult tasks and the middle zone a high number of operators to facilitate the large

number of requests, while the automated voice or web based systems in the outer zone provide problem screening.

3. The Security and IA Aspect

> The 21st century presents new challenges for continued maritime dominance and national security. We have crafted an approach we call *full dimensional protection*. Joint Vision 2020 states that full dimensional protection is achieved "*through the tailored selection and application of multi-layered active and passive measures*." For the DON, that protection takes three forms: (1) protecting knowledge pathways through information assurance and defense in depth, (2) protecting our centers of knowledge through critical infrastructure protection, and (3) protecting our knowledge workers through efforts to protect individual privacy.
>
> David M. Wennergren, DoN Chief information Officer (DON CIO)

From the technical point of view, NMCI provides the DoN with enterprise-wide continuity of operations. NMCI's state-of-the-art facilities and high-availability architecture eliminate significant vulnerabilities, such as maintenance-related outages and single points of failure. 24x7-monitoring activity protects the Intranet against emerging threats, and business continuity planning aims to assure its safe future. An analysis of the NMCI approach to protect the preserve data and systems is shown in figure 72.

	BEFORE THE EMERGENCY	DURING THE EMERGENCY	AFTER THE EMERGENCY
BUILD FOR BEST RESULTS	Redundant Power and AC	Backup Power	Power Restoration
	Access Control and Intrusion Detection	Detection and Notification	Remote Facilities Monitoring
	Resilient Wide-Area Communications	Continuous Communication	Communication Restoration
	Distributed Help Desk Services	Uninterrupted Support	Continued Customer Support
	Redundant and Distributed Services	Survivable Services	Dynamically Redistributed Services
	Distributed Information Security	Continued Information Assurance	Consistent Security Posture
	Distributed Resources	Confined Operational Impact	Critical Service Recovery
	Off-Site Data Protection	Safeguarded Business Data	Critical Process Recovery
PLAN FOR WORST	Risk Assessments	Operations Center Activation	Disaster Recovery Execution
	Command Center Planning	Pre-Planned Response Execution	Business Resumption Activities Initiated
	Emergency Response Planning	Emergency Communication	After-Action Assessments Performed
	Disaster Response Planning	Damage Assessment	Plans Improved
	Business Resumption Plan		
	Plan Testing and Maintenance		

Figure 72: The NMCI Approach to Ensure Continuity of Operations, from EDS Corp.

When each subordinate command had its own network, many had poor security and some had none. The NMCI initiative is rooting out vulnerabilities and provides uniform security standards. Although protecting all the type of information and data flow can be a challenge, because the NMCI network carries many types of messages (from service members' personal e-mail messages to highly classified intelligence data, combating orders or even wartime decision-making videoconferences among officials), with the defense-in-depth (DiD) approach security protection mechanisms are employed in multiple locations within the network architecture. Through the enterprise-wide network, the Navy can conform to the DoD requirements. When a threat is identified, a defensive measure can be pushed out to the entire Intranet quickly, via the Network operations Centers (NOCs). Of course a layered approach to defense can always be improved. For example, defense in depth could mean layering link encryption over network protocol encryption, and further layering it over application layer encryption. Another example would be to use two different anti-viral packages, one at the firewall/application server and another (from a different vendor) installed at the end-user workstation.

a. Additional Efforts from the DoN Needed

Figure 73: A Breakdown of the Necessary Component for the Defense in Depth Strategy.

As shown in figure 73, there is a very important element within the DiD strategy that is currently underestimated, namely the human factor contribution. Apart from the increased number of qualified IT administrators necessary to support the secure operation of the Intranet, the magnitude of NMCI and the excessive number of users associated indicate that computer security training should be included at the Basic

Training Level for all DoN personnel. In order to ensure adequate security and "best practices" behavior from the end user, there is a need to establish adequate training and practice at the very early stages of building qualifications. There is the opportunity to create the necessary "cultural" foundation to promote effective safeguards and behaviors, by educating the end user early enough and before even allowing him/her to use the DoN's IT systems.

To facilitate IA responsiveness, additional technical capabilities are required, including the ability to observe and identify risks in the NMCI operational environment. There is the need to predict potential malicious activity and take actions to proactively adapt the environment to prevent potential threats. If the NMCI is attacked, the DoN should be able to identify the attempt in real-time and prevent the malicious activity from being successful. Trace-back capabilities to identify the attacker and gain attribution of the source of the attack to a legal degree of certainty are also necessary. The NMCI configuration, because of a climate of constant change associated to dealing with a variety of newly discovered or continuously evolving weaknesses, requires a network management system that is flexible, expandable and designed to meet current and future threats.

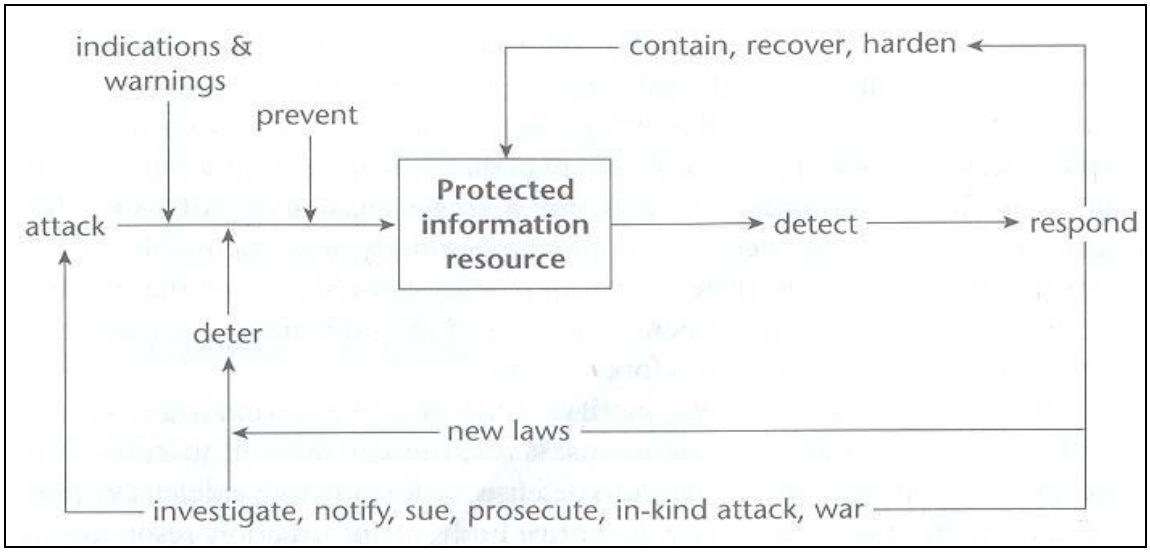


Figure 74: Elements of Defensive Information Warfare and Information Assurance, from Dorothy E. Denning, p. 38

Internal network security is still the most pervasive threat. After building a strong defensive posture for the external threat, the next important element is to deal with

the insider's threat. As shown in figure 74, it is possible with a combination of adequate warnings and through introduction of a more strict policy related to the use of NMCI systems to deter an insider user from inappropriate or insecure behavior. Content monitoring is currently used within the NMCI to ensure availability and proper usage of government assets and bandwidth, and to provide another layer of defense. Now, more than ever, striking the delicate balance between personal privacy and national security is a challenge and the DoN should take aggressive measures to ensure the protection of the NMCI. There is always the option to allow preemptive randomly monitoring of the end user to discourage malicious internal activity. Of course this type of monitoring will have some negative impact to the workforce-DoN relationship and an additional thesis is needed to determine the effects of declaring to the end users that some of them will be the subjects of monitoring. The idea of randomly monitoring the activity of a selected NMCI user establishes an approach similar to random urinalysis, currently used to prevent the use of illegal drug by the DoD personnel.

Spyware is a generic term typically describing software whose purpose is to collect demographic and usage information from a computer, usually for advertising purposes. The term is also used to describe software that "sneaks" onto the system or performs other activities hidden to the user. In general, Spyware is any technology that aids in gathering information about a person or organization without their knowledge. Data collecting programs that are installed with the user's knowledge are not, properly speaking, Spyware, if the user fully understands what data is being collected and with whom it is being shared. The official statement placed on NMCI computers is as follow:

> This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access and access to restricted sites) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to

> monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Although the current official statement is also sufficient, a possible solution in order to reflect the new policy of "Preemptive Monitoring" is to change the warnings for the end -user to read:

> This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access and access to restricted sites) are provided only for authorized U.S. Government use, AS DESCRIBED IN XXXXXXXXXX. DoD computer systems ARE RANDOMLY monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. ALL USERS ARE REMINDED THAT THEY SHOULD HAVE NO EXPECTATION OF PRIVACY IN THEIR USE OF GOVERNMENT INFORMATION SYSTEMS. USE OF GOVERNMENT INFORMATION SYSTEMS, INCLUDING USE OF THE INTERNET AND E-MAIL, IS SUBJECT TO MONITORING, INTERCEPTION, ACCESSING AND RECORDING. During monitoring, information may be copied and used for ALL authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may RESULT IN DISCIPLINERY ACTION BY DOD AND MAY BE PASSED TO LAW ENFORCEMENT subjectING you to criminal prosecution, IF APPLICABLE. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

b. Efforts Needed from Actors outside the DoN Influence

In the beginning of year 2004, Microsoft Corp., which provides the OS and a large variety of applications within the "Gold Disk", released its first monthly security update, following a new schedule that attempts to ease the load on overburdened system administrators. The software giant's move to a monthly from a primarily weekly patch release schedule is a major change for system administrators bogged down by a to-do list of fixes to apply to Windows computers. The software giant believed that the new

schedule would help administrators deal with the workload. However, on the 2nd of February 2004, Microsoft broke its once-a-month schedule to fix a critical flaw in Internet Explorer that could allow malicious coders to take control of an unwary user's PC. (www.news.com (Microsoft releases early IE fix) accessed February 2004) This action alone is the obvious proof that the patching activity is not working and enforcing a more organized introduction of delivering software code is necessary for the safeguard of IT systems.

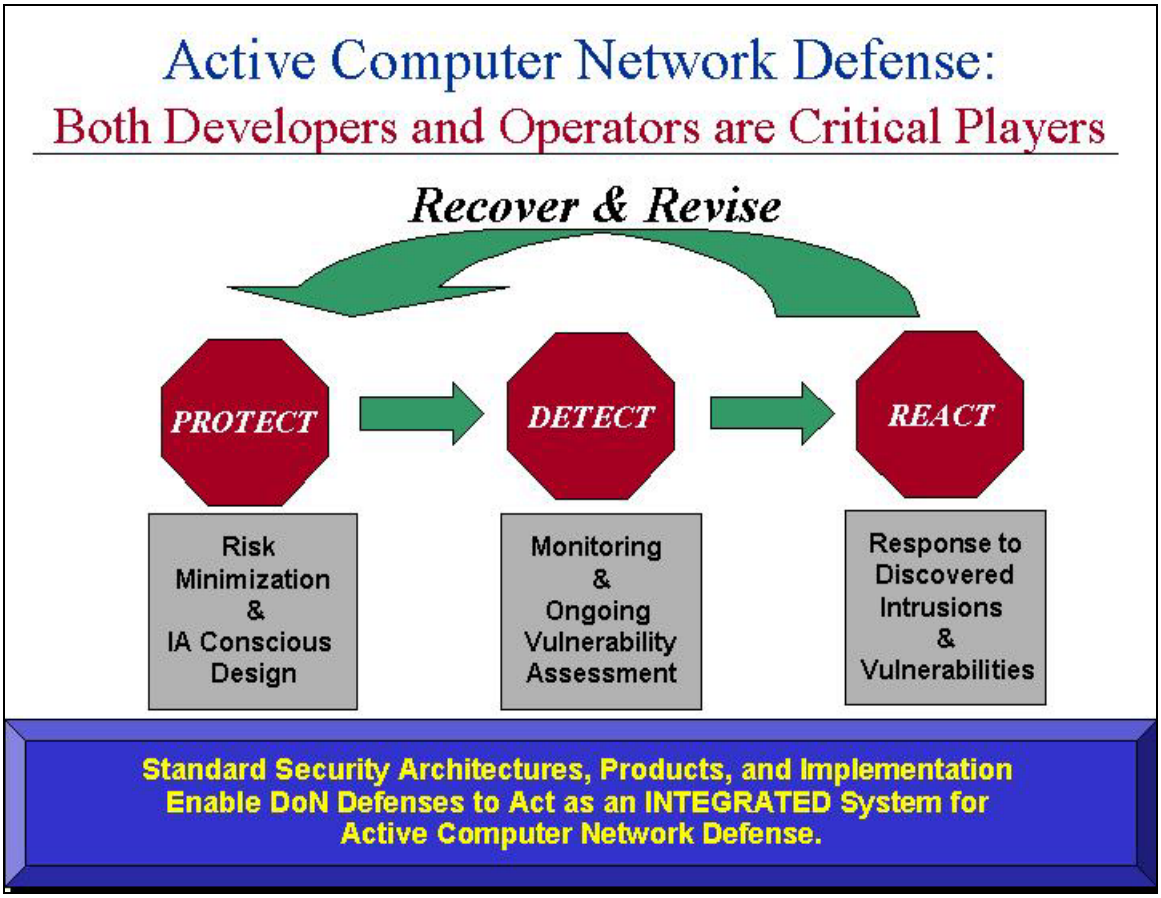


Figure 75: Components of CND

The components necessary to create a secure network are described in Figure 75 In order to fully "secure" NMCI, there is a need to stress that software should be designed to be secure. Until now, Microsoft's efforts have largely centered on improving the way it writes its code and then fixing holes as they emerge. However, recent worm and virus attacks have repeatedly shown that many customers remain vulnerable long after patches have been released. The software giant is already committed to deliver more secure products and has launch its "trustworthy computing

initiative" with the goal to deliver the level of trust and responsibility that is expected from the computing industry: security, privacy, reliability, and business integrity. EDS as a business partner with the power of administering 3.3 million desktops and related software licenses worldwide has a significant interest to use more secure products and should welcome the delivery of a better quality product from Microsoft.

4. More Technical Challenges to Come

More technical challenges for NMCI lay ahead. Under the DoD new policies, all IT acquisitions in support of the Global Information Grid (GIG) must be IPv6-compatible starting October 1, of the fiscal 2004. Improved end-to-end network security will be one of the major benefits of the DoD's planned shift to the "next generation" Internet technology known as Internet protocol version 6 (IPv6). DoD Chief Information Officer John Stenbit announced in June 2003 that the department would upgrade to the new version of the Internet by the end of fiscal 2008.

With IPv6, the sender of information could decide to classify it in a certain way, allowing a receiver to decode the data only if he or she has the proper encryption capacity. Such authentication is optional under IPv4, but it is a vital part of IPv6. The Internet Engineering Task Force (IETF) designed IPv6 security to provide a uniform method of security across all applications and systems by implementing authentication with the IP security protocol. IP security protocol enables authentication at the network layer, layer 3, of the open systems interconnection (OSI) model for computer networks. The network layer is lower than the transport layer, layer 4, where much of the encryption for solutions such as secure hypertext transfer protocol (SHTTP), secure shell (SSH), and secure socket layer (SSL) occurs.

The military services and other DoD components must set up IPv6 addresses and naming conventions with the assistance of the Defense Information Systems Agency (DISA) by the end of the year. Major information technology manufacturers, such as Microsoft and Cisco Systems, already manufacture equipment and software compatible with both IPv4 and IPv6. Stenbit identified the major reasons for the commercial transition to IPv6 as a shortage of IP addresses, quality of Internet service, and security. IPv6 replaces the 32-bit addresses of IPv4 with 128-bit addresses, creating a nearly limitless range of address combinations rather than the few billion permitted by IPv4. The

increase in addresses is also designed to assist with the deployment of wireless devices. (Mickey McCarter, article: *"Internet Shift Boosts Network Security"*, -Military Information Technology, 1st of September 2003)

The Ipv6 introduction and technical challenges topic was selected to demonstrate that NMCI would be an evolving entity and will also involve dealing with a series of technical challenges in the years to come. Careful planning in advance is necessary with extensive analysis of risks involved. The high value of this DoN IT asset indicates that the current managing team should be allocated a more extended timeframe in the same position, in order to take full advantage of their experiences.

B. NAVAL POSTGRADUATE SCHOOL (NPS) AND NMCI

The Naval Postgraduate School (NPS) mission underscores the importance of advanced education and research to the future security of the U.S. and the world. Advanced education and research in the 21st century is rooted in and enhanced by IT functionality as an enabling tool for scientific discovery, learning, and communication. Every goal and strategy defined in the NPS mission is dependent either directly or indirectly on IT. At the time this thesis was near completion, it was made known to the public that NPS would join the NMCI soon.

The NPS Information Technology Strategic Plan for the year 2003 raises serious concerns over the NMCI:

- The academic environment is based on experimentation, testing, and development of new operating systems, software, and middleware. This requires putting things on the university network that would violate NMCI integrity.
- Academic work is fundamentally based on peer review and collaborative work. As a result, NPS faculty and students engage in research projects with other universities, research centers and laboratories and access databases and research sources that would undermine NMCI standards.

As already discussed, NMCI is a top to bottom approach to enforce uniform standards and create a centralized control mechanism for the acquisition and support of IT systems. NMCI introduction has improved the operational performance of many

facilities ashore; however the migration towards NMCI is a very delicate procedure involving many risks. To begin with, NPS is at the highest level of IT functionality among the DoN. NPS is already operating its "private" NOC and the current very high level of IT support is far above the average. NPS students are already IT aware when they begin their studies, and they expect their expertise to increase significantly as a result of their post–graduate education, therefore necessitating a superior IT support. Remote access from off-campus housing must also be considered within any discussion of network infrastructure and joining the NMCI. Faculty members at NPS are involved with research and educational programs that require advanced networking infrastructure, sophisticated user support, and access to high performance computing. NPS operates with clear and concise IT policies and procedures that support an uninterrupted operational state of the NPS' Intranet and the introduction of a solely "educational" network is included in the strategic plans for the future.

No matter that the NMCI offers many economies of scale in terms of maintenance and technology refresh or software license acquisition and the opportunity to upgrade the infrastructure, by being a member of an "equal capabilities" initiative, there is always the danger that the end result for NPS will be to deliver inferior IT services. NPS has a different type of mission when compared with other ashore installations. Also, there are issues relating to supercomputing access and support. The Defense Research and Engineering Network (DREN) provides adequate service for DoD connectivity, but it suffers slowdowns and inefficiencies in connectivity to the commercial Internet. This creates problems for the NPS mission, as expanded capacity and speed are an immediate strategic priority. A main point of concern is that NPS is a research facility with a need to use Internet 2. [Note 2]

There should be extensive planning in advance in order to determine which activities the NMCI infrastructure will support and which of those that will remain in the previous state of IT operation. Additionally NPS must not only deal with the "legacy issue", but with the software it produces. Under the NMCI umbrella, new software production is a security issue, requiring a very time consuming and complex procedure to evaluate software applications for security problems. A possible solution could be to separate the IT support into two different segments: One will be supporting the Academic

and Research activities and the second separate network will be supporting the Administrative Tasks. However, the NPS functionality includes a plethora of "Special User" groups that were often excluded from the original NMCI approach. An opportunity for a series of research activities is present to address all the issues related to the NPS IT future, which should be considered urgent and of great importance. Risk reduction techniques and every alternative option should be examined before the final decision for the NPS migration to the NMCI is made.

C. ENDNOTES

1. Quarantined: Preserve the previous state of desktop configurations even if the whole site was declared operational within NMCI.

Dual Desktop: Use of one desktop with NMCI standard configuration and a second one for the same user to support functionality that was NMCI incompatible or a potential security threat.

2. Internet2 is a consortium being led by 205 universities working in partnership with industry and government to develop and deploy advanced network applications and technologies, accelerating the creation of tomorrow's Internet. Internet2 is not a separate physical network and will not replace the Internet. Internet2 brings together institutions and resources from academia, industry and government to develop new technologies and capabilities that can then be deployed in the global Internet. Close collaboration with Internet2 corporate members will ensure that new applications and technologies are rapidly deployed throughout the Internet. Just as email and the World Wide Web are legacies of earlier investments in academic and federal research networks, the legacy of Internet2 will be to expand the possibilities of the broader Internet. The purpose is to: (www.internet2.edu (About Internet2) accessed March 2004)

- Create a leading edge network capability for the national research community
- Enable revolutionary Internet applications
- Ensure the rapid transfer of new network services and applications to the broader Internet community.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

A. BOOKS

1. Dorothy E. Denning (1999). *Information Warfare and Security*. Massachusetts: Addison Wesley Longman, Inc.

2. Gregory J. Rattray (2001), *Strategic Warfare in Cyberspace.* Massachusetts: The MIT Press.

B. ARTICLES

1. Vice Admiral. Arthur K. Cebrowski, U.S. Navy and John J. Garstka, article *"Network Centric Warfare: Its Origins and Future"* -Naval Institute Proceedings, 1997.

2. Vice Admiral Richard W. Mayo and Vice Admiral John Nathman, U.S. Navy, article *"FORCEnet: Turning Information into Power"*- Naval Institute Proceedings, February 2003.

3. Cheryl Gerber, article: *"Field Test Highlights FORCEnet Advances"*- Military Information Technology, November 2003.

4. Gail Repsher Emery, article: *"After slow start, Congress learning to like NMCI"*, Washington Technology magazine, February 2002.

5. Christopher J. Dorobek, article*: "Navy, EDS to refine performance metrics"*-Federal Computer Week, September 2002.

6. Matthew French, article: *"NMCI Testing shows mixed results"*- Federal Computer Week, December 2002.

7. Matthew French, article: *Survey says... NMCI users satisfied***,** Federal Computer Week, 24 March 2003.

8. Major General J. David Bryan (Vice Director of Defense Information Systems Agency), article *"IA: Holistic View, Targeted Response"*, Military Information Technology, September 2003.

9. Mickey McCarter, article: *"Internet Shift Boosts Network Security"*, - Military Information Technology, September 2003.

10. Jim Garamone (American Forces Press Service), article *"Joint Vision 2020 Emphasizes Full-spectrum Dominance"*, (**www.defenselink.mil (Joint Vision 2020),** accessed January 2004.

11. COTS Journal, Interview of [U.S.] Captain Dan Busch, *Cooperative Engagement Capability*, August 2001

C. DOD AND DON RELATED OFFICIAL CONGRESSIONAL REPORTS AND CONFIRMED CONTRACTS

1. Year 2003 Secretary of Defense Annual Report to the President and the Congress.

2. Year 2003 Secretary of the Navy Annual Report for the President and Congress.

3. NMCI Report to Congress, 30 June 2000.

4. Ronald O'Rourke, Congressional Research Service Report: *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress***,** Order Code RS20557, 6th of June 2001.

5. Revised NMCI Contract N00024-00-D-6000, (Conformed Contract P00080), 10/6/2003.

6. Booz, Allen and Hamilton Inc., Business Case Analysis (BCA) for NMCI, (Contract GS-23F-0755H), 6/30/2000.

7. NMCI Public Key Infrastructure (PKI) User Guide, 2nd July 2003.

8. GAO's Report *Improvements Needed in the Reliability of Defense Budget Submission* to the Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services, House of Representatives, December 2003.

9. Major General David Bryan, Vice Director of the Defense Information Systems Agency and the Commander of the Joint Task Force Computer Network Operations, *Testimony to the Congressional subcommittee on the Department of Defense responsibility for the protection of its computer networks from cyber attack*, 17th of May 2001.

D. WORLD WIDE WEB

1. www.eds.com (Facts about EDS) accessed February 2004.
2. www.cit.nih.gov (Clinger-Cohen Act (CCA)) accessed February 2004.
3. www.nmci.navy.mil The U.S Navy's official website related with NMCI, accessed March 2004.
4. www.defenselink.mil (DOD News: Contracts for October 30, 2002) accessed February 2004.
5. www.nmci-isf.com (EDS-NMCI Team) accessed February 2004.
6. www.nmci-isf.com (About NMCI) accessed January 2004.
7. www.nmci-isf.com (Golden Disk Contents), updated on the 15th of December 2003, accessed February 2004.
8. www.nmci-isf.com (User Information Main Menu) accessed February 2004.
9. www.washingtontechnology.com (Timeline of NMCI in the startup of the program) accessed January 2004.
10. www.washingtontechnology.com (NMCI testing Moves Forward), accessed February 2004.
11. www.belarc.com (IT as a Utility) accessed February 2004.
12. www.symandec.com (Intruder Alert) accessed February 2004.
13. www.symantec.com (Enterprise security Products) accessed February 2004.

14. www.Searchsecurity.com (SSL Definition) accessed February 2004.

15. www.computerworld.com (GAO says inaccuracies in 2004 Pentagon IT budget) accessed February 2004.

16. www.mit-kmi.com (NMCI: Now for the Networks) accessed February 2004.

17. www.msdinc.com accessed February 2004.

18. www.tyckometrics.com accessed February 2004.

19. www.fcw.com (Navy, EDS to refine performance metrics) accessed March 2004.

20. www.cisco.com (Products) accessed March 2004.

21. www.forcenet.navy.mil (What is FORCEnet?), accessed February 2004.

22. www.computerworld.com (How to Buy the Best IT Performance) accessed March 2004.

23. www.news.com (Microsoft releases early IE fix) accessed February 2004.

24. www.jta.disa.mil (Frequently Asked Questions Section), accessed February 2004.

25. www.Searchsecurity.com (SSL Definition), accessed February 2004.

26. www.internet2.edu (About Internet2) accessed March 2004.

E. VARIOUS

1. Joint Knowledge Development and Distribution Capability (JKDDC) Briefing, in the Worldwide Joint Training Conference, USA, September 2003.

2. RADM Mike Sharp, U.S. Navy, Vice Commander Space & Naval Warfare Systems Command, NMCI Briefing at the NMCI – Industry Symposium, 19 June 2003.

3. Captain Chris Christopher, U.S. Navy, NMCI Briefing for the Joint Logistics Council, USA, 29 March 2001.

4. Navy Marine Corps Intranet Site Deployment Guide Version 1.2, 07 March 2003.

5. Joseph Cipriano, PEO for IT, NMCI briefing at the Armed Forces Communications and Electronics Association, San Diego-USA, 16 February 2000.

6. Rear Admiral J. P. Cryer, U.S. Navy, Commander of Naval Network and Space Operations Command, NMCI Operations Brief at the NMCI – Industry Symposium, 18 June 2003.

7. Rear Admiral Chuck Munns, Director of NMCI, NMCI Progress Briefing, at the NMCI – Industry Symposium 17 June 2003.

8. EDS Corp.: Profits Review for the year 2003.

9. Rear Admiral Chuck Munns, U.S. Navy, NMCI Director, NMCI Briefing at the SPAWAR Industry Day, San Diego-USA, 23rd October 2003.

10. Naval Postgraduate School Information Technology Strategic Plan for the year 2003, http://intranet.nps.navy.mil (NPS IT Strategic Plan), accessed March 2004

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

NMCI CONTRACT LINE ITEM NUMBERS (CLINS)

CLIN	Description	Last Posted
0001AA	Fixed Work Station, Red	Nov 13, 2003
0001AB	Fixed Work Station, White	Nov 13, 2003
0001AC	Fixed Work Station, Blue	Nov 13, 2003
0001AD	Fixed Work Station, Thin Client	Aug 4, 2003
0001AE	Remote User Credit (Moved to CLIN 004105)	Feb 19, 2003
0001AF	Fixed Workstation, Classified Thin Client	Dec 15, 2003
0002AA	Portable Seat	Nov 13, 2003
0002AB	Ultra-Lightweight Portable Seat	Nov 13, 2003
0003AA	Embarkable Work Station, Full Service	Nov 13, 2002
0003AB	Embarkable Work Station, Limited Service	Mar 26, 2002
0004AA	Embarkable Portable Seat, Full Service	Dec 15, 2003
0004AB	Embarkable Portable Seat, Limited Service	Mar 26, 2002
0004AC	Non-Ruggedized Deployable Portable	Nov 13, 2003
0005AA	Basic Hybrid Seat	Nov 13, 2003
0005AB	Enhanced Hybrid Seat	Nov 13, 2003
0005AC	Reserved	Jan 16, 2002
0005AD	Personal Access Package - 100% Concurrent Use	Aug 12, 2002
0005AE	Personal Access Package - 30% Concurrent Use	Aug 21, 2002
0006	Additional Standard Wall Plug Service	May 21, 2003
0006AA	Additional Standard Wall Plug Service	May 21, 2003
0006AB	Unclassified Wall Plug - Service Only	May 21, 2003

0006AC	Classified Wall Plug - Service Only	May 21, 2003
0006AD	Unclassified Wall Plug	May 27, 2003
0006AE	Classified Wall Plug - Inside a Controlled Access Area	May 27, 2003
0006AF	Classified Wall Plug - Outside a Controlled Access Area	May 27, 2003
0006AG	Project Wall Plug	Nov 4, 2003
0006AH	Switch Port - Low Bandwidth Service	Sep 22, 2003
0006AJ	Switch Port - High Bandwidth Service	Sep 22, 2003
0006AK	Sub-Device IP Address Management Service	Sep 22, 2003
0007	High-End Upgrade Packages	N/A
0007	For CLIN 0001AA Fixed Workstation Red	Nov 13, 2003
0007	For CLIN 0002AA & 0002AB Portable	Nov 13, 2003
0007	For CLIN 0003AA Full Service Embarkable	Nov 13, 2002
0007	For CLIN 0004AA Full Service Embarkable Portable	Dec 12, 2001
0008AA	Mission-Critical Upgrade Package - Single Connection	May 21, 2003
0008AB	Mission-Critical Upgrade Package - Dual Connection	May 23, 2003
0009AA	Classified Connectivity Upgrade Package	Apr 22, 2003
0009AB	Switchable Classified Connectivity (Thin Client Solution)	Oct 22, 2003
0009AC	Switchable Classified Connectivity (Dual CPU Solution)	Mar 26, 2002
0009AD	Re-Bootable Classified Connectivity Upgrade Package	Mar 6, 2002
0009AE	Switchable Classified Connectivity Upgrade Package (Dual CPU Solution/White)	Mar 26, 2002
0009AF	Switchable Classified Connectivity Upgrade Package (Dual CPU Solution/Blue)	Mar 26, 2002
0009AG	Switchable Classified Connectivity Upgrade Package (Dual CPU Solution/Portable)	Mar 26, 2002

0009AH	Switchable Classified Connectivity Upgrade Package (Dual CPU Solution / Non-Ruggedized Deployable Portable)	Jul 24, 2002
0010AA	Basic Voice Seat	Dec 4, 2000
0010AB	Business Voice Upgrade Package	Dec 4, 2000
0010AC	Mission-Critical Voice Seat Upgrade Package	Apr 9, 2001
0010AD	Pier Voice Line	Dec 4, 2000
0010AE	Pier Voice Trunk	Dec 4, 2000
0010AF	Commercial Voice Seat	Dec 4, 2000
0010AG	Commercial Voice Connectivity	Dec 4, 2000
0011	Secure Voice Seat	Dec 4, 2000
0012	Mobile Phone Seat	Dec 4, 2000
0013	Personal Paging Service Seat	Jul 24, 2002
0014	Fixed Video Teleconference Seat	Nov 4, 2003
0015	Moveable Video Teleconference Seat	Dec 4, 2000
0015AA	Basic Moveable VTC Seat	May 22, 2002
0015AB	High-End Moveable VTC Seat	May 22, 2002
0015AC	Mission-Critical Moveable VTC Seat	Dec 4, 2000
0015AD	Premium Moveable VTC Seat	May 22, 2002
0016AA	Additional File Share Services - Unclassified (10Gb)	May 21, 2003
0016AB	Additional File Share Services - Classified (10Gb)	May 21, 2003
0016AC	Email Storage - Unclassified (25Mb)	Aug 1, 2003
0016AD	Additional Email Storage - Classified (25MB)	May 21, 2003
0017	Internet Access for Mobile Phone Seat	Dec 4, 2000
0018	Classified Remote Access Service	Mar 26, 2002

0019	Reserved	Jul 2, 2000
0020	Data Seat Voice Communications Upgrade	Apr 9, 2001
0021	Defense Messaging System Data Seat Upgrade	Mar 6, 2002
0022AA	Basic Desktop VTC	Aug 1, 2003
0022AB	High-End Desktop VTC	Aug 1, 2003
0023	Optional User Capabilities	Nov 03, 2003
0024	Additional Non-Classified Account	Apr 9, 2001
0025	Additional Classified Account	Apr 9, 2001
0026	Additional Moves, Adds, Changes	May 21, 2003
0026AA	Additional Moves, Adds, Changes	Jun 26, 2003
0026AB	Physical MAC Group of 50	Jun 26, 2003
0026AC	Physical MAC - Group of 250	Jun 26, 2003
0026AD	COI MAC	Jun 26, 2003
0026AE	Voice Moves, Adds, and Changes	Sep 22, 2003
0026AF	VTC Moves, Adds, and Changes	Jan 5, 2001
0026AG	Annual Administrative MAC	May 21, 2003
0026AH	Annual Physical MAC	May 21, 2003
0026AJ	Annual Physical MAC (Needing a Wall Plug)	May 21, 2003
0026AK	Annual Embarkable MAC	May 21, 2003
0026AL	Administrative MAC (Single)	Jun 26, 2003
0026AM	Physical MAC (Single)	Jun 26, 2003
0026AN	Embarkable MAC (Single)	Jun 26, 2003
0026AP	Project MAC (Single)	Nov 4, 2003
0027AA	Standard Low Bandwidth Application	May 21, 2003

0027AB	Standard Medium Bandwidth Application	May 21, 2003
0027AC	Standard High Bandwidth Application	May 21, 2003
0027AD	Mission-Critical Low Bandwidth Application	Dec 4, 2000
0027AE	Mission-Critical Medium Bandwidth Application	Feb 6, 2001
0027AF	Mission-Critical High Bandwidth Application	Dec 4, 2000
0027AG	Legacy Application Server Connection	Jun 26, 2003
0028	Data Warehousing	Nov 4, 2003
0029	Legacy Systems Support	Nov 4, 2003
0030	Network Operations Display	Jan 16, 2002
0031	Military Personnel Core Competency Development (Sea-Shore Rotation and Operating Forces/Supporting Establishment Rotations)	Jan 25, 2002
0032	External Network Interface	Nov 4, 2003
0033	Information Technology/Knowledge Management Retraining Program	Feb 6, 2001
0034	Satellite Terminal Support	Nov 4, 2003
0036	OCONUS Service	Jun 6, 2003
0038AA	Developer Fixed Workstation Upgrade	Jan 16, 2002
0038AB	Developer Portable Workstation Upgrade	Mar 26, 2002
0038AC	S&T Terminal Services	Sep 22, 2003
0038AD	S&T Fast Ethernet Wall Plug	Jan 16, 2002
0038AE	S&T Wall Plug Service - Modified Gigabit Ethernet Network Transport-Lots of 4	Jan 16, 2002
0038AF	S&T Wall Plug Service - Modified Gigabit Ethernet Network Transport-Lots of 8	Jan 16, 2002

0038AG	S&T Wall Plug Service - Modified Gigabit Ethernet Network Transport-Lots of 16	Jan 16, 2002
0038AH	S&T Network Transport - Other	Nov 4, 2003
004101	Desktop Support	Feb 19, 2003
004102	Desktop Refresh	Feb 19, 2003
004103	Desktop Refresh With NMCI Gold Disk Software	Feb 19, 2003
004104	Assumption of Responsibility	Feb 19, 2003
004105	Remote User Credit	Feb 19, 2003
004106	Remote User Credit (Japan)	Jun 6, 2003
0043	Asbestos Material Abatement	Aug 1, 2003
0044	Department of Defense Mentor-Protégé Program (0044AA - 0044AF)	Dec 23, 2003

Table A: List of CLINs Related with the NMCI Contract, (www.nmci-isf.com (Services and Contract Line Item Number (CLIN)), accessed February 2004)

APPENDIX B

NMCI SERVICE LEVEL AGREEMENTS (SLA)

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
SLA 1: Desktop Hardware and Operating System								
Installation Accuracy	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Availability	99.7%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.7%	99.7%			> 99.7%
Problem Resolution	2 Business Days			> 2 Business Days	2 Business Days	≤ 2 Business Days		
SLA 2: Standard Office Automation Software								
Installation Accuracy	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Software Currency	≤ 1 year and or Two Revisions			> 1 Year and or Two Revisions	≤ 1 year and or Two Revisions			
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 3: E-Mail Services								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Problem Resolution	1 Hour			> 1 Hour	1 Hour	< 45 Minutes		
Performance of E-Mail Transfer	≤ 5 Minutes			> 5 Minutes	5 Minutes	< 5 Minutes		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 4: Directory Services								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Responsiveness – Network Connected	≤ 2 Seconds	> 10 Seconds	> 4 ≤ 10 Seconds	> 2 ≤ 4 Seconds	2 Seconds			< 2 Seconds
Responsiveness - Dial In	≤ 20 Seconds	> 40 Seconds	> 30 ≤ 40 Seconds	> 20 ≤ 30 Seconds	20 Seconds	< 20 ≥ 15 Seconds	< 15 ≥ 10 Seconds	< 10 Seconds
Timeliness of Directory Updates	Within 4 hours 99.9%	Within 4 Hours < 90%	Within 4 Hours ≥ 90% < 95%	Within 4 Hours ≥ 95% < 99.9	Within 4 Hours 99.9%			Within 4 Hours > 99.9%
Accuracy of Global/Local On-Line Directory	< .5% of Users			> .5 % of Users	.5 % of Users	< .5% of Users		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
SLA 5: File Shared Services								
Availability to Required Users	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Data Integrity	.05%			> .05%	.05%	< .05%		
Time to Recover Lost Files	95.0% One Day			< 95.0% One Day	95.0% One Day	> 95.0% One Day		
Shared File Performance - Network	2 Seconds	> 10 Seconds	> 4 ≤ 10 Seconds	> 2 ≤ 4 Seconds	2 Seconds			< 2 Seconds
Shared File Performance - Dial In	30 Seconds	> 50 Seconds	> 40 ≤ 50 Seconds	> 30 ≤ 40 Seconds	30 Seconds	< 30 ≥ 25 Seconds	< 25 ≥ 15 Seconds	< 15 Seconds
SLA 6: Web Access Services								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Performance of NMCI Web Access	15 Seconds			> 15 Seconds	15 Seconds	< 15 Seconds		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 7: Newsgroup Services								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Interoperability	95.0%			< 95.0%	95.0%	> 95.0%		
Performance	90.0%			< 90.0%	90.0%	> 90.0%		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 8: Deleted								
SLA 9: Print Services								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
SLA 10: NMCI Intranet Performance								
Availability	99.8%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.8%	99.8%			> 99.8%
Latency/Packet Loss	70-100 ms			> 100 ms	70-100 ms	< 70 ms		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
Problem Resolution	30 Minutes/3 Hours		> (60 Minutes/6 Hours)	> (30 Minutes/3 Hours) ≤ (60 Minutes/6 Hours)	30 Minutes/3 Hours			< 30 Minutes/3 Hours
SLA 11: NIPRNET Access								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
Latency/Packet Loss	30 ms/ 1%			> 30 ms/1%	30 ms/1%	< 30 ms/1%		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 12: Internet Access								
Availability	98.0%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 98%	98%			> 98%
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 13: Mainframe Services Access								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 14: Desktop Access to Government Applications								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			>99.5%
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 15: Moves, Adds and Changes								
Responsiveness	≤ 6 Days		> 8 Days	> 6 Days < 8 Days	6 Days		< 6 Days	
Incidence of Repeat Calls	2%			> 2%	2 %	< 2%		
Performance	96%			< 96%	96%	>96%		
SLA 16: Software Distribution and Upgrades								
Upgrade Backouts	≤ 3.0%			>3.0%	3%	<3.0%		
Upgrade Currency	98%			< 98%	98%	> 98 %		
Patches Currency	98%			< 98%	98%	> 98 %		
SLA 17: User Training								
Security Training Execution	95.0%			< 95.0%	95.0%	> 95.0%		
User Training Execution	95%			< 95%	95%	> 95 %		
User Training Availability	80%			< 80%	80%	> 80 %		
Quality	80.0%			< 80.0%	80.0%	> 80.0%		
SLA 18: Unclassified Remote Access								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
Capacity	30.0%			<30.0%	30.0%	>30.0%		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 19: Classified (Secure) Remote Access								
Availability	> 99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Capacity	30.0%			<30.0%	30.0%	>30.0%		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 20: Portable Workstation Wireless Dial In								
Mean time to repair/replace for hardware components	98% Within 3 Business Days			< 98% Within 3 Business Days	98% Within 3 Business Days	> 98% Within 3 Business Days		
SLA 20A: Organizational Messaging Service								
Availability	99.50%	< 90%	≥ 90.0% < 95%	≥95.0% < 99.5%	99.5%			> 99.5%
Problem Resolution	1 Hour			> 1 Hour	1 Hour	< 45 Minutes		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 21: Desktop Video teleconference Services								
Availability	99.50%	< 90%	≥ 90.0% < 95%	≥95.0% < 99.5%	99.5%			> 99.5%
Audio and Video Quality (Integrity)	≥ 15 Frames/ sec			<15 Frames/ sec	15 Frames/ sec	> 15 Frames/ sec		
System Performance	70.00%	< 60%	≥60% < 65%	≥ 65% < 70%	70.0%	> 70% < 75%	≥75% <80%	≥ 80%
Gateway Capacity	80%			< 80%	80%	> 80%		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
Reliability of Session Initiation	85%		< 75%	< 85% ≥ 75%	85%	> 85%		
SLA 22: Voice Communications								
Availability	99.99%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.99%	99.99%			> 99.99%
Dial Tone Delay	Not more than 1.5% calls offered encounter delay > 3 Seconds			> 1.5% of calls offered encounter delay > 3 seconds	Not more than 1.5% calls offered encounter delay > 3 Seconds	< 1.5% of calls offered encounter delay > 3 seconds		

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
Grade of Service -End User to End User Calls	P .05			P > .05	P .05	P < .05		
Grade of Service -End User to External Networks	P .01			P > .01	P .01	P < .01		
Latency	120 MS			> 120 MS	120 MS	< 120 MS		
Delay Variation/Jitter	60 MS			> 60 MS	60 MS	< 60 MS		
Trouble Repair Times	24 Hours		> 48 Hours	> 24 Hours ≤ 48 Hours	24 Hours	< 24 Hours ≥ 8 Hours	< 8 Hours	
Operator Assisted Calling	< 2 Minutes			> 2 Minutes	2 Minutes	< 2 Minutes		
Absolute Echo Path Delay	< 25 MS			> 25 MS	25 MS	< 25 MS		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 23: Basic Help Desk Services								
Responsiveness (Time to Answer Call)	Prime Time Average ≤ 40 Seconds	> 120 Seconds	> 60 Seconds ≤ 120 Seconds	> 40 Seconds ≤ 60 Seconds	Prime Time Average 40 Seconds	< 40 Seconds		
Responsiveness (% of Calls Abandoned)	< 7.0%		> 9.0%	> 7.0% ≤ 9.0%	7.0%	<7.0% ≥ 5.0%	< 5.0%	
Responsiveness (General Administration)	1day/2hrs 95.0%			1day/2hrs 95%	1day/2hrs 95%	1day/2hrs 95%		
Responsiveness (% of Call Resolved on First Contact)	65.0%		< 50.0%	< 65.0% ≥50.0%	65.0%	> 65.0% ≤ 75.0%	> 75.0%	
Responsiveness (Notification of Unplanned Service Outage)	Within 15 Minutes			> 15 Minutes	15 Minutes	< 15 Minutes		
SLA 24: WAN Network Connectivity								
Availability (WAN Connectivity)	99.99%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.99%	99.99%			> 99.99%
% Bandwidth Used	40.0%			>40.0%	40.0%	< 40.0%		
Problem Resolution (Response Time)	30 Minutes/ 3 hours	> 60 Minutes	>45 Minutes ≤ 60 Minutes	>30 Minutes ≤ 45 Minutes	30 Minutes/3 hours			< 30 Minutes
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 25: BAN/LAN Communications Services								
Availability	99.9%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.9%	99.99%			>99.9%
Latency	10 ms			> 10 ms	10 ms	< 10 ms		

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
% Bandwidth Utilization on Shared Network Segments	40.0%			>40.0%	40.0%	< 40.0%		
Problem Resolution	30 Minutes/3 Hours		> (60 Minutes/6 Hours)	> (30 Minutes/3 Hours) ≤ (60 Minutes/6 Hours)	30 Minutes/3 Hours			< 30 Minutes/3 Hours
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 26: Movable VTC Seat								
Availability	99.50%	< 90%	≥ 90.0% < 95%	≥95.0% < 99.5%	99.5%			> 99.5%
Video Quality	128 Kbps/15 fps			<128 Kbps/15 fps	128 Kbps/15 fps	> 128 Kbps/15 fps		
Gateway Capacity	95%			< 95%	95%	> 95%		
Multipoint Capacity	85%			< 85%	85%	> 85%		
Reliability of Session Initiation	85%/95%			< 85%/95%	85%/95%	> 85%/95%		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 26A: Proxy and Caching Service								
Availability	99.50%	< 90%	≥ 90.0% < 95%	≥95.0% < 99.5%	99.50%			> 99.5%
Average Hit Ratio	40.00%			< 40%	40%	> 40%		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 27: External Networks								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			> 99.5%
Implementation Time	< 6 Working Days		> 10 Working Days	> 6 Working Days ≤ 10 Working Days	6 Working Days		< 6 Working Days	
Problem Resolution	1 Hour/3 Hours		> (2 Hours/6 Hours)	> (1 Hour/3 Hours) ≤ (2 Hours/6 Hours)	1 Hour/3 Hours			< 30 1 Hour/3 Hours
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 28: Network Management Services (Asset Management)								
Time to Implement Asset (% Implemented Within 5 Days)	85.0%	< 70.0%	≥70.0% < 80 .0%	≥80 .0% < 85.0%	< 85%	>85% ≤ 92%	> 92.0%	

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
Time to Remove Asset	25 Business Days			> 25 Business Days	25 Business Days	< 25 Business Days		
Accuracy of Asset Inventory	98%		< 85.0%	≥ 85.0% < 98%	98%			> 98%
SLA 29: Operational Support Services								
Quality and Timeliness of Reports	100%			< 100%	100%			
Data Back-up recovery and Archiving Effectiveness	99.9%	< 90%	≥ 90.0% < 95%	≥95.0% < 99.9%	99.9%			> 99.9%
Data Base Audits and Maintenance effectiveness	99.9%			< 99.9%	99.9%			> 99.9%
SLA 30: Capacity Planning								
SLA 31: System Services – Domain Name Server								
Availability	≥ 99.7%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.7%	99.7%			>99.7%
Latency	<100ms			> 100ms	100ms	< 100ms		
SLA 32: Application Server Connectivity								
Availability	99.5%	< 90.0%	≥ 90.0% < 95.0%	≥ 95.0% < 99.5%	99.5%			>99.5%
Implementation Time	< 5 Working Days			> 5 Working Days	5 Working Days	< 5 Working Days		
MTTR Backbone to Server Network Segment	≤ 6 Hours		> 8 Hours	> 6 Hours ≤ 8 Hours	6 Hours	< 6 Hours ≥ 3 Hours	< 3 Hours	
SLA 32A: Network Operations Display								
Availability	99.5%			< 99.5%	99.5%			> 99.5%
SLA 33: NMCI Security Operational Services-General								
Accreditation	85.0%			< 85%	85.0%	> 85%		
Security Integrity – Third Part Physical Inspections-Unclassified	95.0%			< 95%	95.0%	> 95%		
Security Integrity – Third Part Physical Inspections-Classified	99.0%			< 99%	99.0%	> 99%		
Security Integrity – Security Measures-Unclassified	0.2%			> .2%	0.2%	< .2%		
Security Integrity – Security Measures-Classified	0.1%			> .1%	0.1%	< .1%		

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
SLA 34: Information Assurance Operational Services-PKI								
Certificate Revocation-Unclassified	1 Hour			> 1 Hour	1 Hour	< 1 Hour		
Certificate Revocation-Classified	30 Minutes			> 30 Minutes	30 Minutes	< 30 Minutes		
Ability of one NMCI user to obtain the DOD public key infrastructure X.509 certificate of another NMCI user for purpose of sending electronic mail-Unclassified.	5 Minutes, 99.7% Unclassified			> 5 Minutes, 99.7%	5 Minutes, 99.7%	< 5 Minutes, 99.7%		
Ability of one NMCI user to obtain the DOD public key infrastructure X.509 certificate of another NMCI user for purpose of sending electronic mail-Classified.	2 Minutes, 99.9%			> 2 Minutes, 99.9%	2 Minutes, 99.9%	< 2 Minutes, 99.9%		
User Registration for DOD public Key Infrastructure within NMCI-Unclassified	85% 1 Week, 100% 2 Weeks Unclassified			< 85% 1 Week, 100% 2 Weeks	85% 1 Week, 100% 2 Weeks	> 85% 1 Week, 100% 2 Weeks		
User Registration for DOD public Key Infrastructure within NMCI-Classified	85% 1 Week, 100% 2 Weeks Classified			< 85% 1 Week, 100% 2 Weeks	85% 1 Week, 100% 2 Weeks	> 85% 1 Week, 100% 2 Weeks		
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 35: Information Assurance Operational Services-SIPRNET								
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SIPRNET Access Availability	98.0%			< 98%	98.0%			> 98%
Interoperability	Within 1 Day			> 1 Day	Within 1 Day		< 4 Hours	
SLA 36: Information Assurance Planning Services								
Security Incident Reporting Unclassified	1 Week			> 1 Week	1 Week	<= 3 Days		
Security Incident Reporting Classified	1 Day			> 1 Day	1 Day	<= 4 Hours		
Security Incident Response Unclassified	1 Day			> 1 Day	1 Day	<= 4 Hours		

Service Level Measurement								
SLA Category	**Metric (SPM)**	**-4**	**-2**	**-1**	**0**	**+1**	**+2**	**+4**
Security Incident Response Classified	1 Day			> 1 Day	1 Day	<= 4 Hours		
Security Product Refresh - Unclassified	6 Months			< 6 Months	6 Months	> 6 Months		
Security Product Refresh - Classified	6 Months			< 6 Months	6 Months	> 6 Months		
Security Vulnerability Remediation – Unclassified	1 Day			> 1 Day	1 Day	<= 4 Hours		
Security Vulnerability Remediation – Classified	1 Day			> 1 Day	1 Day	<= 4 Hours		
SLA 36A: Integrated Configuration Management								
SLA 36B: Integration and Testing								
Time to Configure Asset	4 Days			> 4 Days	4 Days	< 4 Days		
SLA 36C: Technology Refresh								
Workstation Refreshment	36 Months			> 36 months	36 months	< 36 months		
Refreshment Timeliness	85%	< 65%	> 75% < 65%	< 85% > 75%	85%	> 85% < 90%	> 90% < 95%	> 95%
Average Relative Performance of Refreshment Workstations	75%	< 65%	=> 65% < 70%	=> 70% < 75%	75%	> 75% <= 80%	> 80% <= 90%	> 90%

Table B: Monitoring Performance Criteria and SLAs, from the NMCI REVISED contract N00024-00-D-6000, 6 Oct 2003, p.120-127

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

NMCI'S "GOLD DISK" REVISION HISTORY

Revision History

Version	Date Posted to Web	Item	Revision
1.0	03/01/02	MS Office Suite	Old: MS Office Pro 2000 SR-1a New: Standard Office Automation Software Included on the Gold Disk MS Word MS Excel MS PowerPoint MS Access
2.0	9/19/02	Operating System	Old: MS Windows 2000 Build 2195 SP1 New: MS Windows 2000 Build 2195 SP2/SRP1
		Internet Browser	Old: Internet Explorer MS 5.5 SP-1 128 bit New: Internet Explorer MS 5.5 SP-2 128 bit
		PDF Viewer	Old: Acrobat Reader v.4.05c New: Acrobat Reader v. 5.05
		Terminal Emulator	Old: Reflection 8.0.5 New: Reflection 8.0.5 – Web Launch Utility
		Compression Tool	Old: WinZip v8 New: WinZip v8.1
		Multimedia	Old: Windows Media Player v7.00.1956 New: Windows Media Player v7.01.00.3055
		Electronic Records Management	Old: Trim Captura v4.3* New: N/A
		Web Controls	Old: Apple QuickTime Movie and Audio Viewer v4.12 New: Apple QuickTime Movie and Audio Viewer v5.0
		Software Management	Old: Radia Client Connect New: Radia Client Connect v2.1
		Dial-Up Connectivity	Old: PAL New: PAL v4.1.1.306
		VPN	Old: VPN Client New: VPN Client v3.0
3.0	1/23/03	Electronic Records Management	Old: N/A New: Trim Context

Version	Date Posted to Web	Item	Revision
4.0	2/19/03	Dial Up Connectivity	Old: PAL v4.1.1.306 New: PAL v4.3
		VPN	Old: VPN Client v3.0 New: VPN Client v4.1
5.0	4/9/03	Security	Old: Intruder Alert 3.5 New: Intruder Alert v3.6
6.0	6/2/03	Operating System	Old: MS Windows 2000 Build 2195 SP2/SRP1 New: MS Windows 2000 SP3
		Desktop Management	Old: N/A New: Diskeeper 7.0413 Executive Software
		Security	Old: Intruder Alert v3.6 Axent New: Intruder Alert v3.6 Symantecc
		Security	Old: ESM v5.1 Axent New: ESM v5.1 Symantec
7.0	12/15/03	Multimedia	Old: Windows Media Player v7.01.00.3055 New: Windows Media Player v9

Table C: "Golden Disk" Revision History, from www.nmci-isf.com (Golden Disk Contents), updated on the 15th of December 2003, accessed February 2004

APPENDIX D

NMCI PERFORMANCE MEASUREMENT METRICS

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
0001	DT HW and OS	V-prov DT HW and OS	Fxd & Por (B, HE, MC), Emb Por,	B, HE, MC	Installation Accuracy	Percentage of HW or OS installations/ upgrades successful on first use.	Monthly	(1) 0.995 (2) 0.995 (3) 0.995
					Availability	Basic DT, including HW and OS, is up and capable of running SW apps.	Monthly	(1) 0.997 (2) 0.997 (3) 0.999
					Problem Resolution	Elapsed time from outage until DT HW and OS are restored to normal operating performance.	Continuous monitoring, reported monthly	(1) 1 bus day (2) 1 bus day (3) 4 hours
					Problem Resolution (Remote Users Only)	Elapsed time from outage until DT HW and OS are restored to normal operating performance.	Continuous monitoring, reported monthly	(1) 2 bus days (2) 2 bus days (3) 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0002	Standard Office Automation SW	V-prov standard DT integrated SW	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Installation Accuracy	Percentage of OA SW installations/ upgrades successful on first use.	Monthly	(1) 0.995 (2) 0.995 (3) 0.995
					SW Currency	OS SW currency relative to industry standards (OS SW standard across the enterprise).	Quarterly	(1) <=1yr and/or 2 versions (2) <=1yr and/or 2 versions (3) <=1yr and/or 2 versions
					Interoperability	Full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded.	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0003	E-mail Services	V-prov svcs for e-mail and multimedia e-mail attachments.	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Availability	Portion of time V-prov e-mail server has up time.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.997

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Problem Resolution	Elapsed time from outage until svc is restored to normal operating performance.	Continuous monitoring, reported monthly	(1) 1 hour (2) 1 hour (3) 30 minutes
					Performance of E-mail Transfer	Avg. time V-pro e-mail system keeps message in their system (a) before depositing in user's mailbox (on server) for incoming mail and (b) before delivering to Internet or other NMCI domain for outgoing mail.	Annual	(1) <=5 minutes (2) <=5 minutes (3) <=5 minutes
					Interoperability	Full interoperability and seamless interface within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0004	Directory Services	V-maintained global information svcs delivering distributed computer apps across the NMCI.	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid, Voice, Video	B, HE, MC	Availability	SDP accessibility to NCMI global information svcs.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.997
					Responsiveness – network connected	Time it takes to search on-line directory info for LAN-attached end-user within NMCI domain.	Monthly	(1) <=2 seconds (2) <=2 seconds (3) <=2 seconds
					Responsiveness – Dial-in	Time it takes to search on-line directory info for dial-in-attached end-user within NMCI domain.	Monthly	(1) <=20 seconds (2) <=20 seconds (3) <=20 seconds

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Timeliness of Directory Updates	Responsiveness and completeness of data in on-line directory resources add, change, or delete to individual directory info reflected within four hours 99.9% of time.	Monthly	(1) within 4 hours, .999 (2) within 4 hours, .999 (3) within 4 hours, .999
					Accuracy of Global/Local On-line Directory	Maintain directory accuracy across NMCI infrastructure. Excludes any inaccuracies due to updates that may not be under the control of the vendor.	Monthly	(1) <=.001 of users (2) <=.001 of users (3) <=.001 of users
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0005	File Shared Services	V-prov end user access to shared, controlled access storage media	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Availability to Required Users	Availability of shared file svcs.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.997
					File Share Data Integrity	Number of unrecoverable data lost incidents per month to user ratio.	Monthly as reported to HD	(1) 0.0005 (2) 0.0005 (3) 0.0003
					Time to Recover Lost Files	Begins with notification to help desk, through completion of file restoration.	Monthly	(1) 1 day .95 (2) 1 day .95 (3) 4 hours .98
					Shared File Performance – Network	Time to retrieve or post 1 MB file for LAN-attached user.	Monthly	(1) 2 seconds (2) 2 seconds (3) 2 seconds
					Shared File Performance – Dial-in	Time to retrieve or post 100 KB file for dial-in user.	Monthly	(1) 30 seconds (2) 30 seconds (3) 30 seconds

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0006	Web Access Services	V-prov end user access to in-house and external web content	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Availability	Web server availability to customer.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.997
					Performance of NMCI Web Process	Avg. time to access NMCI-site to maintain required level per user requirements change.	Monthly	(1) <=15 seconds (2) <= 10 seconds (3) <= 5 seconds
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0007	Newsgroup Services	V-prov access to public and private newsgroups	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Availability	Newsgroup svcs availability for account holders.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.997
					Interoperability	Interoperability successes for newsgroup svcs.	Monthly	(1) 0.95 (2) 0.975 (3) 0.985
					Performance	Successful vs. total transfer trials to newsgroups.	Monthly	(1) 0.90 (2) 0.95 (3) 0.99
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Customer Satisfaction	Separately queried, analyzed, and reported capability.	Quarterly	(1) 0.85 (2) 0.85 (3) 0.85
0008 DELETED	Multimedia Capabilities Services							
0009	Print Services	V-supplied end user ability to produce hard copies.	Fxd & Por (B, HE, MC), Emb, Emb Por	B, HE, MC	Availability	Printer up time.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.997
					Accessibility	Supporting printer located within 50 feet of all supported WSs.	Acceptance of installations	(1) Yes (2) Yes (3) Yes
					Average Density	Avg. number of users per NMCI printer, not to exceed 20 (avg. < or = 10).	Acceptance of installations	(1) Yes (2) Yes (3) Yes
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0010	NMCI Intranet Performance	External to base combined svc level for networking of voice, video, or data via NMCI Intranet	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Availability	Connectivity across NMCI.	Measured periodically, summarized hourly, reported daily	(1) 0.998 (2) 0.998 (3) 0.998
					Latency and Packet Loss	Packet latency across Internet to other NMCI sites and commercial sites.	Measured every 5 minutes, reported monthly	(1) 70-100 ms/<1.0% (2) 70-100 ms/<1.0% (3) 70-100 ms/<1.0%
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Problem Resolution	Elapsed time from outage until service is restored to normal operating performance.	Continuous monitoring, reported monthly	(1) 30 minutes/3 hours (2) 15 minutes/1 hour (3) 3 minutes/30 minutes
					Customer Satisfaction	User satisfaction of latency of network apps, interoperability (reachability) to DON and DoD sites.	Quarterly	(1) 0.85 (2) 0.85 (3) 0.85
0011	NIPRNET Access	End user point of entry for voice, video, or data device into NIPRNET	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid, Voice, and seats w/classified option.	B, HE, MC	Availability	NIPRNET connectivity.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.998
					Latency and Packet Loss	Packet latency across Intranet to other NMCI sites and commercial sites.	Continuously monitored, reported monthly	(1) 30 ms/<1.0% (2) 30 ms/<1.0% (3) 30 ms/<1.0%
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	User satisfaction of latency and network apps, interoperability (reachability) to DON and DoD sites.	Quarterly	(1) 0.85 (2) 0.85 (3) 0.85
0012	Internet Access	End user point of entry for voice, video, or data device into Internet	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Availability	Internet connectivity.	Measured continuously, summarized daily, reported monthly	(1) 0.980 (2) 0.980 (3) 0.996
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Customer Satisfaction	User satisfaction of latency and network apps, interoperability (reachability) to DON and DoD sites.	Quarterly	(1) 0.85 (2) 0.85 (3) 0.85
0013	Mainframe Services Access	V-prov access to mainframe data and apps.	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Availability	Required mainframe applications and data access.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.997
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Performance to support mission requirements (end user satisfaction level).	Baseline survey followed by annual surveys	(1) 0.85 (2) 0.85 (3) 0.85
0014	Desktop Access to Government Apps	V-prov desktop access to Government systems and apps.	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Availability	Full functionality of system/app at end user's desktop.	Monthly reports on the system/ application availability	(1) 0.995 (2) 0.995 (3) 0.997
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Performance to support mission requirements (end user satisfaction level).	Baseline survey followed by annual surveys	(1) 0.85 (2) 0.85 (3) 0.85
0015	Moves, Adds, and Changes	V-prov MACs as specified in SOO	Fxd (B, HE, MC), Emb, Emb Por	B, HE, MC	Responsiveness	Time to complete from initial notification to help desk.	Each occurrence	(1) <=6 days (2) <=5 days (3) <=2 days
					Government Operational Direction	Time to complete from initial notification to help desk.	Each occurrence	(1) (2) (3) <=1 hour

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Incidents of Repeat Calls	Percentage of repeat calls to help desk regarding previously requested MACs.	Each occurrence	(1) 2% (2) 2% (3) 2%
					Performance	Percentage of work done at scheduled time.	Each occurrence	(1) 0.96 (2) 0.96 (3) 0.98
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0016	Software Distribution and Upgrades	V-prov svc to distribute SW to SDPs and appropriate NMCI infrastructure.	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Upgrade Backouts	Attributed to SW upgrades performed via network svcs to a whole local domain not previously scheduled.	Monthly	(1) <0.03 (2) <0.03 (3) <0.03
					Upgrades Currency	Number of installed SW releases that are at least equal to or current to most current SW release.	Monthly	(1) 0.980 (2) 0.980 (3) 0.980
					Patches Currency	Number of released patches installed divided by number of patches available.	Monthly	(1) 0.980 (2) 0.980 (3) 0.980
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0017	User Training	Scope and effectiveness of user and security training.	All end users	All	Security Training	Formal training (8-hr. min. per year).	Tracked continuously, reported monthly	(1) 0.95 (2) 0.98 (3) 1.00
					User Training Availability	Proportion of population identified as requiring training against those that have received training.	Tracked continuously, reported monthly	(1) 0.80 (2) 0.90 (3) 0.95
					Quality	Evaluation of courses conducted within 30 days after course completion.	Tracked continuously, reported monthly	(1) 0.80 (2) 0.80 (3) 0.80
0018	Unclassified Remote Access	End user remote access to NMCI	Por, Emb Por	B, HE, MC	Availability	RAS availability of NMCI infrastructure via dial-in	Monthly	(1) 0.995 (2) 0.995

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
		data network via dial-up link.				capability.		(3) 0.995
					Capacity	RAS connectivity surge capacity available beyond normal peak load.	Monthly	(1) 0.3 (2) 0.3 (3) 0.3
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0019	Classified Remote Access	End user remote access to NMCI data network via dial-up link.	Por & Emb Por w/classified connectivity	B, HE, MC	Availability	Secure RAS availability of NMCI infrastructure via dial-in capability.	Monthly	(1) 0.995 (2) 0.995 (3) 0.995
					Capacity	RAS connectivity surge capacity available beyond normal peak load.	Monthly	(1) 0.3 (2) 0.3 (3) 0.3
					Performance	CRAS modem data rate.	Annually	(1) Yes (2) Yes (3) Yes
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0020	Portable WS Wireless Dial-in	V-supplied ancillary device supporting wireless, mobile connectivity to NMCI.	Por and Emb Por w/full svc	B, HE, MC	Mean Time Between Failure	Rate of failure of wireless devices.	???????	??????
					Mean Time to Repair/Replace HW components	Time to repair wireless connection devices.	Per event basis, reported monthly	(1) 98% within 3 bus days (2) 98% within 3 bus days (3) 99% within 1 bus day
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0020 A	Organization-al Messaging Service	NMCI-provided DMS capabilities.	All four Data Seats and associated Upgrades	B, MC	Availability	DMS up time.	Measured continuously, averaged hourly, reported monthly	(1) 0.995 (2) (3) 0.997
					Problem Resolution	Elapsed time from outage until svc is restored.	Continuously monitored, reported monthly	(1) 1 hour (2) ? (3) 15 minutes
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) (3) 0.85
0021	Desktop VTC Services	V-coordinated VTC svcs for full duplex video/ audio/data.	WS seats w/optional svcs	B, HE	Availability	VTC up time.	At implementation and yearly	(1) 0.995 (2) 0.995 (3)
					Audio and Video Quality (Integrity)	Clarity of voice and video.	At implementation and yearly	(1) >=15 frames/sec (2) >=30 frames/sec (3) ?

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					System Performance	Desktop VTC performance relative to current state of the shelf available systems.	Quarterly	(1) 70% relative capability (2) 90% relative capability (3)
					Gateway Capacity	Sufficient gateways to support on-line VTC users (capable of connectivity between dissimilar algorithms, bandwidth speeds, etc.).	Measured continuously, reported monthly	(1) 0.80 (2) 0.95 (3)
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) within 1 day (2) within 1 day (3)
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3)
0022	Voice Communi-cations	User capability to send and receive voice calls to and from other users within and external to NMCI domain.	Voice Seats	B, Bus, MC	Availability	Voice svc availability to end user.	Measured continuously, reported monthly	(1) 0.9999 (2) 0.9999 (3) 0.9995
					Dial Tone Delay	Time from off-hook to provision of dial tone during the Busy hour.	Monthly and randomly on 1% of total voice seats	(1) Not more than 1.5% calls offered encounter delay >3 sec (2) Not more than 1.5% calls offered encounter delay >3 sec (3) Not more than 1.5% calls offered encounter delay >3 sec

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Grade of Service (GOS)-End User-to-End User Calls (Intra-NMCI)	Proportion of calls that cannot be completed during the Busy hour.	Measured every 5 minutes, reported monthly	(1) P.05 (2) P.05 (3) P.01
					GOS End User External Networks	Proportion of calls that cannot be completed during the Busy hour.	Measured every 5 minutes, reported monthly	(1) P.01 (2) P.01 (3) P.01
					Latency	User-to-user latency for voice calls across the NMCI voice network.	Measured every 5 minutes, reported monthly	(1) 120 ms (2) 120 ms (3) 120ms
					Delay/Variation/Jitter	Variation from when packet was expected to be received and actual receipt.	Measured every 5 minutes, reported monthly	(1) 60 ms (2) 60 ms (3) 60ms
					Trouble Repair Times	Time from notification to vendor or discovery by vendor (whichever is earlier) until restoration of voice svc.	Each occurrence	(1) 24 hours (2) 24 hours (3) 2 hours
					Operator-assisted Calling	Operator svcs to include directory assistance (i.e., 411), enhanced 911 capabilities, and 24-hour operator assisted calling including DISN OCONUS calls.	Sample and report monthly on a representative sample size.	(1) 2 minutes (2) 2 minutes (3) 2 minutes
					Absolute Echo Path Delay	Twice the one-way transit time delay of a signal through a switching system connection path.	Continuously monitored, reported monthly	(1) 25 ms (2) 25 ms (3) 25 minutes
					Customer Satisfaction	Includes performance of user svcs and voice quality.	Initial: 6 mos for 1st yr, yearly thereafter Monthly	(1) 0.85 (2) 0.85 (3) 0.85
0022 A	Voice Mail	V-prov IVMS including voice messaging transmission, reception, and voice message storage 24/7. Interoperable	All Voice & Data Seats w/Voice capability	B, Bus, MC	Voice Mail GOS	Proportion of calls that cannot be completed during the Busy hour.	Measured every 5 minutes, reported monthly	(1) N/A (2) P.05 (3) N/A

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
		with DSN.						
					Voice Mailbox Size	Storage space allocated per user for incoming, outgoing, and archived messages.	Initially measured at system implementation, then sampled monthly	(1) N/A (2) 10 minutes (3) N/A
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded	(1) N/A (2) within 1 day (3) N/A
					Customer Satisfaction	Includes performance of user svcs and voice quality.	Initial: 6 mos for 1st yr, yearly thereafter Monthly	(1) N/A (2) 0.85 (3) N/A
0023	Basic Help Desk Services	V-prov end user technical assistance to solve NMCI issues to end user's satisfaction.	All Voice, Video, and Data WSs	B, HE, MC	Responsiveness (1)	Number of rings before connect, avg. time in queue until appropriate technician is contacted.	Monthly	Responsiveness (1): Prime Time: Avg is <=40 seconds. 90% of calls answered within 60 seconds and 100% of calls in 120 seconds Non-Prime Time: Avg <=55 seconds. 90% of calls answered within 120 seconds and 100% answered in 240 seconds
					Responsiveness (2)	Caller disconnect.	Monthly	Responsiveness (2) (1) less than 7% (2) less than 7% (3) less than 5%
					Responsiveness (3)	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter Monthly	(1) 0.85 (2) 0.85 (3) 0.85
					Responsiveness (4)	Time spent establishing user accounts and updating/resetting passwords.	Monthly	(1) 1 day/2 hrs (95%) (2) 4 hrs/1 hr (98%) (3) 1 hr/15 min (99.5%)
					Responsiveness (5)	Calls resolved on first contact to help desk.	Monthly	(1) 0.65 (low priority) (2) 0.65 (normal priority) (3) 0.80 (high priority)
					Responsiveness (6)	Compliance with escalation procedure.	Annually	(1) Satisfactory (2) Satisfactory (3) Satisfactory
					Responsiveness (7)	User notification by help desk for unplanned svc outages, and return to svc status prior to restore.		(1) within 15 mins (2) within 15 mins (3) within 15 mins
0024	WAN Network Connectivity	V-prov connection to geographically separated Navy and Marine Corps users/devices.	NMCI Infrastructure, Organizations, NMCI OP Center, Pierside SDP, Fleet Teleports, Non-DON organizations	B, HE, MC	Availability	Connectivity/capacity to WAN portal.	Continuous monitoring, 24-hr averaging, with monthly reporting	(1) 0.999 (2) 0.999 (3) 0.999
					Percent Bandwidth Used	Average utilization compared with available, useable capacity.	Measured continuously, summarized hourly, reported monthly	(1) 0.4 (2) 0.4 (3) 0.3
					Problem Resolution	Elapsed time from outage until svc is restored.	Continuous monitoring, reported monthly	(1) 30 mins/3 hrs (2) 15 mins/1 hr (3) 3 mins/30 mins
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded.	(1) within 1 day (2) within 1 day (3) within 4 hours

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr; yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0025	BAN/LAN Communi-cations Services	V-prov connection to geographically co-located Navy and Marine Corps LANs and BAN-attached devices.	For DoN organizations: BANs, NMCI Infrastructure, Organizations, NMCI OP Center, Pierside SDP, Fleet Teleports For Non-DoN organizations: LANs, Data/ Voice/Video seats, Organization	B, HE, MC	Availability	Availability of connectivity between Navy and Marine Corps LANs, BANs and attached devices.	Continuous monitoring, 24-hr averaging, with monthly reporting	(1) 0.999/0.999 (2) 0.999/0.999 (3) 0.9999/0.9999
					Latency	Percent Bandwidth Utilization on Shared Network Segments.	Measured every 5 minutes, reported monthly	(1) 10 ms (2) 10 ms (3) 10 ms
					Problem Resolution	Elapsed time from outage until svc is restored.	Monthly surge capacity check	(1) 0.4 (2) 0.4 (3) 0.3
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded.	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr; yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0026	Moveable VTC Seat	V-prov audiovisual equipment allowing users mobility and easy relocation to selected VTC svcs.	Specified Government site/facility	B, HE, MC	Availability	VTC up time and end user access.	At implementation and yearly	(1) 0.995 (2) 0.995 (3) 0.997

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Video Quality	Absence of distortion, tiling, and latency.	At acceptance and yearly	(1) 128 Kbps/15fps (2) 384 Kbps/30 fps (3) 768 Kbps/30 fps
					Gateway Capacity	Sufficient gateways to support on-line VTC users (capable of connectivity between dissimilar algorithms, bandwidth speeds, etc.).	Measured continuously, reported monthly	(1) 0.95 (2) 0.95 (3) 0.99
					Multi-Point Capacity	Provide entire network with capability to perform multipoint conferences.	Measured continuously, reported monthly	(1) 0.85 (2) 0.85 (3) 0.95
					Reliability of Session Initiation	Connectivity on first try, and continuous up time for duration of VTC with sites connected to NMCI.	Measured continuously, reported monthly	(1) 0.85/0.95 (2) 0.85/0.95 (3) 0.95/0.99
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded.	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr; yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0026 A	Proxy and Caching Services	V-prov user capability for caching and proxy to enhance Internet access/performance.	Each DON Facility	Enterprise	Availability	Proxy server up time.	Measured daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.997
					Average Hit Ratio	Successful http requests fulfilled by cache.	Measured daily, reported monthly	(1) 0.40 (2) (3)

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded.	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr; yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0027	External Networks	Access and interface to networks external to NMCI (includes required security and access control).	Applicable WSs	B, He, MC	Availability	Portal availability to external networks (non-NMCI).	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) 0.995 (3) 0.995/0.998
					Implementation Time	Turnaround time between user request and implementation of access (does not include non-existing circuits).	Monthly avg	(1) <6 working days (2) <3 working days (3) <24 hours
					Percent Bandwidth Used	Avg. utilization compared with available, useable capacity.	Monthly surge capacity check	(1) 0.4 (2) 0.4 (3) 0.3
					Problem Resolution	Help Desk trouble ticket restoration time from outage until svc is restored.	Continuous monitoring, reported monthly	(1) 1 hr/3 hrs (2) 1 hr/3 hrs (3) 15 mins/1 hr
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded.	(1) within 1 day (2) within 1 day (3) within 4 hours
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr; yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0028	Network Management Service	Operations Support of Asset	NMCI Infrastructure, Organization, NMCI	B, HE, MC	Time to Implement Asset	Delivery and installation of asset.	As requested by Government	(1) <=5 days, 92% of time

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
	– Asset Management	Management to include historical data, summary management reports, etc.	OP Center, and Fleet Teleports					(2) <=5 days, 92% of time (3) <=5 days, 92% of time
					Time to Implement Asset Remote Users Only	Delivery and installation of asset.	As requested by Government	(1) <=5 days, 85% of time (2) <=5 days, 85% of time (3) <=5 days, 92% of time
					Time to Remove Asset	Removal of existing asset.	As requested by Government	(1) <=15 days (2) <=15 days (3) <=15 days
					Time to Remove Asset Remote Users Only	Removal of existing asset.	As requested by Government	(1) <=25 days (2) <=20 days (3) <=15 days
					Accuracy of Asset Inventory	Accuracy of inventory and mapped network components.	Quarterly reports	(1) 0.995 (2) 0.995 (3) 0.995
0029	Operational Support Services	V-prov indirect svcs to include data backups and recovery, data archiving, etc.	Infrastructure	Enterprise	Quality and Timelines Reports	Situational report (monthly).	Measured daily, summarized and reported weekly	(1) 100% (2) (3)
					Data Backup/Archiving and Recovery Effectiveness	Specified data backup frequency and data retention periods.	Per Audit	(1) 0.999 (2) (3)
					Database Audits and Maintenance Effectiveness	Audit scheduled database archiving and maintenance.	Annual	(1) 0.999 (2) (3)
					Disaster Recovery Plan Effectiveness	NMCI Disaster Recovery Plan to be presented within one month of contract award.	Initially and annually	(1) 100% (2) (3)
0030	Capacity Planning	V-prov modeling to plan changes to NMCI	NMCI Operation Center	Enterprise	Quality of Planning	Deliver satisfactory (usable) reports that perform capacity planning (assessment of	Annually	(1) 100% (2) (3)

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
		infrastructure, specifically to estimate future volume, usage, and applications characteristics, as well as integration of emerging technology.				processes, trend analysis, requirements assessment, etc.).		
					Availability and Timeliness of Reports	Deliverance of satisfactory (usable) reports that perform capacity planning (assessment of processes, trend analysis, requirements assessment, etc.) as per scheduled intervals.	Monthly reports until baseline established, then quarterly reports using 3, 6, and 12 months of historical measured, functional, and war plans requirements data for re-baselining the NMCI model.	(1) 100% (2) (3)
					Report Integrity	Network performance reporting integrity.	Monthly network performance data, including actual and function, shall be gathered according to requirements for the model	(1) 100% (2) (3)
0031	Domain Name Server (DNS)	Meet all functionality of current DNS svc, to include flexible support for deployed units.	NMCI Infrastructure, Organizations, NMCI OP Center and Fleet Teleports	B, HE, MC	Availability	Availability of DNS svc.	Primary DNS (every 2-5 mins) Secondary DNS (every 10-15 mins)	(1) >= 0.997 (2) >= 0.997 (3) >= 0.998

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Latency	Reflects time for NMCI end users to use their local DNS svcs.	Primary DNS (every 2-5 mins) Secondary DNS (every 10-15 mins)	(1) 100 ms (2) 10 ms (3) 10 ms
					Usage	Percentage of time reports are received and accurate.	Queries/second rate averaged over 15 mins	(1) 100.0% (2) (3)
					Quality of Service	Percentage of time reports are received and accurate.	Avg successful queries/total queries over 15 mins	(1) 100.0% (2) (3)
0032	Application Server Connectivity	V-prov NMCI connectivity for Navy/Marine Corps organizational/operationa/ functional application svcs (*optional* svc).	Selected Government Application Servers	S, MC	Availability	Availability of NMCI network bandwidth from local backbone to connected app server.	Measured continuously, summarized daily, reported monthly	(1) 0.995 (2) (3) 0.997
					Implementation Time	Time between user request and implementation of connectivity between network backbone and app server.	Measured on a per event basis and summarized and reported monthly	(1) <5 working days (2) (3) <24 hrs
					MTTR Backbone to Server Network Segment	Mean time to repair network segment between supporting backbone and app server.	Monitored continuously, summarized and reported monthly	(1) <=6 hrs (2) (3) <=2 hrs
					Network Loading (throughput)	Available bandwidth from server to local backbone.	Monitored continuously, summarized and reported monthly	(1) 0.40 (2) (3) 0.30
0032 A	Network Operations Display	Provides authorized MC users with real-time status of their network assets.	DON NMCI Managers	Enterprise	Availability	Availability of NMCI real-time performance and status information.	Measured continuously, averaged weekly, reported monthly	(1) 0.995 (2) (3)

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Customer Satisfaction	Level of customer satisfaction.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) (3)
0033	NMCI Security Operational Services – General	Provision of security mechanisms, procedures, controls, and operation, as well as compliance with DoD certification and accreditation policies and procedures.	All NMCI Voice, Video, and Data SDPs	B, HE, MC	Accreditation	Follow DITSCAP 5000.40 accreditation requirements. Percentage of success on first attempt of adjudicated packages.	Semi-annual	(1) 0.85 (2) 0.85 (3) 0.90
					Security Integrity- Third Party Physical Inspections	Percentage of third party physical inspections passed.	Annual	Unclass/Class (1) 0.95/0.99 (2) 0.97/100% (3) 0.99/100%
					Security Integrity – Security Measures	Percentage of violation of security measures.	Periodic	Unclass/Class (1) 0.002/0.001 (2) 0.002/0.001 (3) 0.002/0.00
					Blocking of an Intrusion Attack (user level)	Success rate in blocking Red Team intrusions.	Periodic	Unclass/Class (1) 0.99/0.9999 (2) 0.99/0.9999 (3) 0.999/100.00%
					Blocking of an Intrusion Attack (root level)	Success rate in blocking Red Team intrusion attacks.	Periodic	Unclass/Class (1) 0.99/0.9999 (2) 0.99/0.9999 (3) 0.999/100.00%
					Blocking of a Denial of Service (DOS) Attack	Success rate in blocking of DOS attacks.	Periodic	Unclass/Class (1) 0.995/0.9999 (2) 0.995/0.9999 (3) 0.999/100.00%

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Blocking of Data Retrieval Attack	Success rate in blocking Red Team data retrieval attacks.	Periodic	Unclass/Class (1) 0.99/0.9999 (2) 0.99/0.9999 (3) 0.999/100.00%
					Blocking of Data Integrity Attack	Success rate in blocking Red Team data integrity attacks.	Periodic	Unclass/Class (1) 0.99/0.9999 (2) 0.99/0.9999 (3) 0.999/100.00%
					Red Team Attacks	Percentage of Red Team intrusions detected.	Periodic	Unclass/Class (1) 0.995/0.9999 (2) 0.995/0.9999 (3) 0.997/100.00%
0034	NMCI Security Operational Services PKI	Protection of IS to assure confidentiality, integrity, availability, authenticity, and non-repudiation. PKI svcs for e-mail users.	Fxd & Por (B, HE, MC), Emb, Emb Por, Hybrid	B, HE, MC	Certificate Revocation	Timeliness of revoking certificates when required.	Continuous by vendor, random by Government	Unclass/Class (1) 1 hr/30 mins (2) 1 hr/30 mins (3) 1 hr/30 mins
					Ability to Obtain DOD PKI X.509 Certificates for E-mail	Time required for users to successfully obtain (on first attempt) X.509 certificates from the NMCI PKI.	Monthly report	Unclass/Class (1) 5 in, 99.7%/2 min, 99.9% (2) 5 in, 99.7%/2 min, 99.9% (3) 5 in, 99.7%/2 min, 99.9%

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					User Registration for DOD PKI within NMCI	Time from submission of user request to establishing fully functional DOD PKI X.509 certificates.	Monthly report	Unclass/Class (1) 85% (1 wk), 100% (2 wk) /85% (1wk, 100% (2 wk) (2) 85% (1 wk), 100% (2 wk) /85% (1 wk, 100% (2 wk) (3) 90% (3 days), 100% (1 wk) /85% (3 days, 100% (1 wk)
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded.	(1) within 1 day (2) within 1 day (3) within 4 hours
0035	NMCI Security Operational Services -SIPRNET	Protection of IS to assure confidentiality, integrity, availability, authenticity, and non-repudiation. SIPRNET access to users.	Classified Connectivity Upgrade Option	B, HE, MC	SIPRNET Access Availability	Availability of connectivity at SIPRNET portal.	Measured continuously, summarized hourly, reported daily	Normal Ops/Under increased INFOCON (1) 0.98/0.6 (2) 0.98/0.6 (3) 0.996/0/85
					SIPRNET Access Verification	Number of unauthorized users who obtain successful access to SIPRNET svcs.	Continuous by vendor, periodic by Government	(1) 0.00 (2) 0.00 (3) 0.00
					Interoperability	Requires full interoperability and seamless interface both within NMCI and to external customers.	Measured continuously, summarized daily, reported monthly, or when plan threshold value exceeded.	(1) within 1 day (2) within 1 day (3) within 4 hours

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
					Customer Satisfaction	User satisfaction of latency of network apps, interoperability (reachability) to DON and DoD sites.	Continuous by vendor, periodic by Government	(1) 0.85 (2) 0.85 (3) 0.85
0036	NMCI Security Planning Services	Secure strategic svcs that provide for the NMCI to enhance confidentiality integrity, availability, authenticity, and non-repudiation.	All NMCI Voice, Video, and Data SDPs	B, H, MC	Security Incident Reporting	Time required to document and report security incidents.	Continuous, report monthly	Unclass/Class (1) 1 wk/1 day (2) 1 wk/1 day (3) 1 hr/1 hr
					Security Incident Response	Time required to respond to a security incident.	As required	Unclass/Class (1) 1 wk/1 day (2) 1 wk/1 day (3) 1 hr/1 hr
					Security Product Refresh	Time required to distribute new/revised security HW and SW. Note: Not applicable for real time security fixes mandated to be completed in shorter time frames.	As required	Unclass/Class (1) 6 mos/6 mos (2) 3 mos/3 mos (3) 1 mo/1 mo
					Security Vulnerability Remediation	Time required to implement real time system fixes/patches to address security vulnerabilities.	As specified by policy	Unclass/Class (1) 1 day/1 day (2) 8 hrs/8 hrs (3) 1 hr/1 hr
0036 A	Integrated Configuration Management	CM maintenance to include asset inventory of all HW and SW.	All data seats, fixed and secure voice devices, VTC seats, and all NMCI infrastructure and external networks.	Enterprise	Time to Update CM System	Time to update CM system after changes to asset configuration.	Measured daily, reported monthly	(1) 24 hrs (2) (3)
0036 B	Integration and Testing	V-performed adequate level of testing to minimize effects of mods to	All NMCI Components	NMCI-wide	Time to Configure Asset	Based on elapsed time from removal of device from svc to configure until device is returned with updated baseline.	Monthly	(1) 4 days (2) 3 days (3) 3 days

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
		NMCI configuration.						
					Test Coordination with the Government	Systems, products, and svcs coordinated with Government as introduced. V-prov project schedules for roll outs.	Monthly	(1) 5-10% (2) 10-20% (3) >20%
0036 C	Technology Refreshment	Includes periodic replacement of NMCI data seats with more capable machines, to include servers, telephones, telephone switches, network switches, network routers, and other HW and infrastructure.	Fxd & Por (B, HE, MC), Emb (Contractor-provided), Emb Por (Contractor-provided)	B, HE, MC	WS Refreshment	Percentage of seats meeting or exceeding minimum acceptable performance.	Continuously monitored and reported monthly for first 18 mos and quarterly thereafter	(1) 36 Mos (2) 36 mos (3) As applicable
					Refreshment Timeliness	Percentage of refreshments completed within or before quarter scheduled.	Annually	(1) 0.85 (2) 0.95 (3) 0.95
					Refreshment Convenience	Avg. score on user refreshment convenience survey for all technology refreshments completed during the year.	Continuous monitoring, reported monthly	(1) 75% Red 75% White 65% Blue 60% Thin Client 50% (2) 90% (3) As applicable
					Average Relative Performance of Refreshment WSs	Avg. of relative performance of WSs provided for refreshment compared to performance of "stat-of-the-art" WSs available at time of refreshment.	Initial: 6 mos for 1st yr, yearly thereafter	(1) 0.85 (2) 0.85 (3) 0.85
0036	Technology Insertion	V-assistance in	All NMCI	B, HE, MC	Demonstrated Benefit	Number of technology insertion	Annually	(1) .75

SLA #	SERVICE NAME	SERVICE DESCRIPTION	APPLICABLE SERVICE DELIVERY POINTS	SERVICE LEVELS	PERFORMANCE CATEGORIES	PERFORMANCE MEASURED	FREQUENCY MEASUREMENT	SERVICE PERFORMANCE LEVEL (% of Satisfaction)
D		identifying and applying new technologies through increased effectiveness of program and further advance is overall objectives.	Infrastructure			projects completed for which beneficial results can be measured or demonstrated.		(2) .85 (3) .85
					Benefit Significance	Percentage of insertion projects performed in terms of improvement in NMCI cost or relevant technical parameters for technology insertion projects completed.	Annually	(1) 5-1 (2) 10-2 (3) >20%
0037	Sea-Shore Rotation Support Training	V-prov training of Navy and Marine Corps uniformed IT professionals rotating from sea duty to shore duty jobs.	Training Planning	N/A	Skill Maintenance and IT Professional Development	Ability to perform training needs assessment and planning based on evaluation of prior training and experience of each assigned individual.	Measured continuously, updated quarterly	(1) 0.95 (2) N/A (3) N/A
					Core Competency Development	V-performance in training uniformed IT professionals to carry out skills identified as core competencies iaw Attachment 3.	Continuous, coincides with military personnel fitness report cycles	(1) 0.95 (2) N/A (3) N/A

Table D: The SLAs and Performance Measurements Matrix Currently used, from www.nmci.navy.mil, accessed February 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Glenn R. Cook (Code IS)
   Naval Postgraduate School
   Monterey, California

4. Dorothy E. Denning (Code DA)
   Naval Postgraduate School
   Monterey, California

THIS PAGE INTENTIONALLY LEFT BLANK