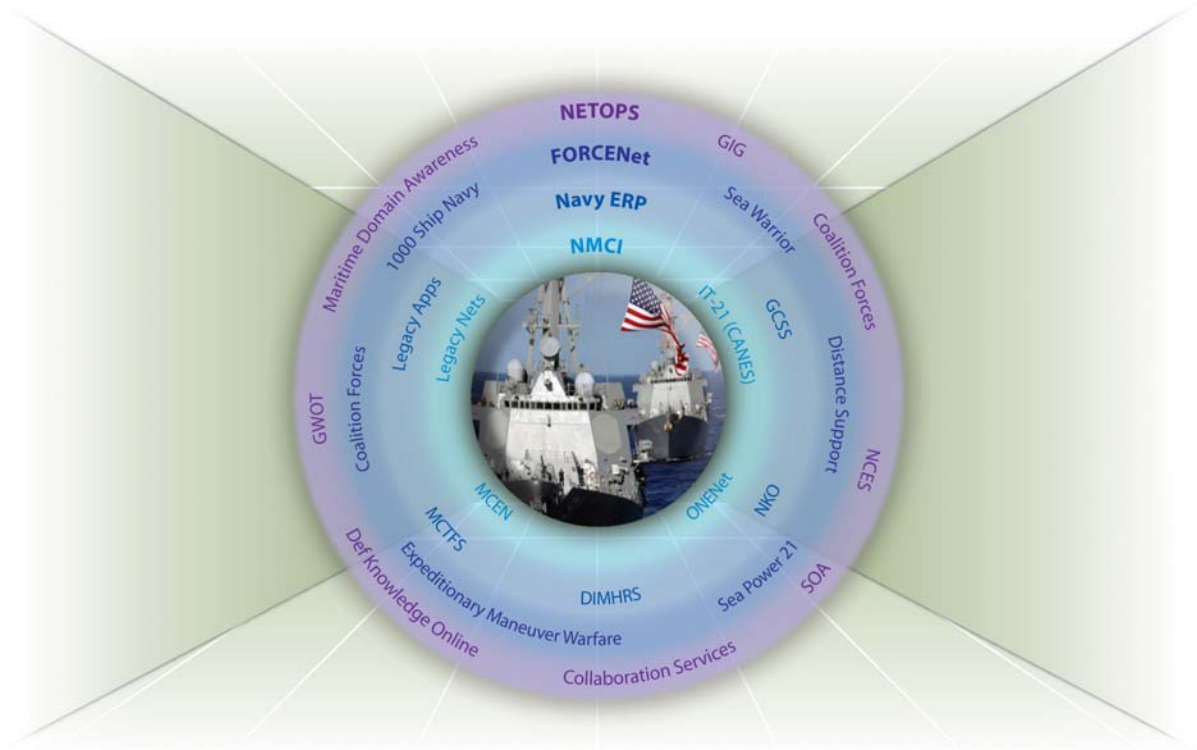
Department of the Navy
Naval Networking Environment (NNE)~2016



Strategic Definition, Scope and Strategy Paper
Version 1.1
13 May 2008

Prepared by:
Department of the Navy Chief Information Officer
(DON CIO) NGEN/NNE Strategy & CONOPS Task Force

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
13 MAY 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Strategic Definition, Scope and Strategy Paper Version 1.1	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of the Navy,Naval Networking Environment ,1000 Navy Pentagon,Washington,DC,20350-1000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**34**	

Table of Contents

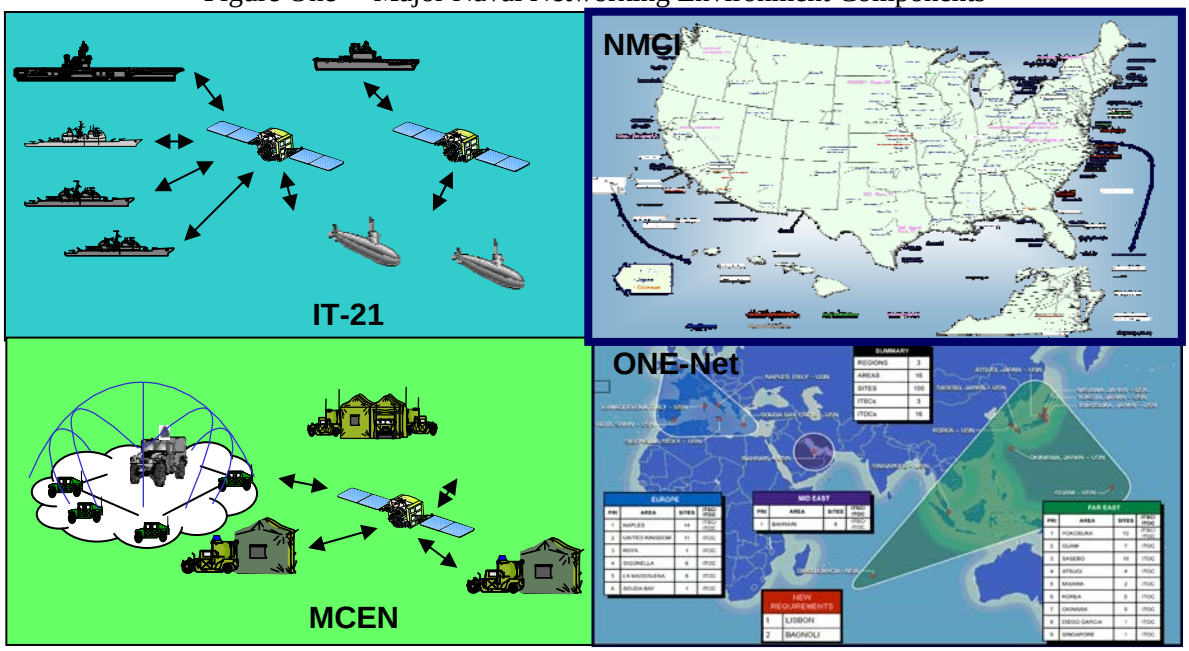
1.0 INTRODUCTION

The Department of the Navy (DON) Chief Information Officer (CIO) has led the effort to define the vision, scope, strategy, and concept of operations (CONOPS), for the Department of the Navy's future Naval Networking Environment (NNE), in the 2016 timeframe. The information contained in this paper will allow the Department to formulate the strategy behind NNE~2016 that is linked to the warfighting and warfighting support needs of the Department.

1.1 Today's Naval Networking Environment

Today's Naval Networking Environment is primarily composed of four enterprise computing and communications environments as shown in Figure One.

Figure One – Major Naval Networking Environment Components



The **Navy Marine Corps Intranet (NMCI)** provides roughly 650,000 Navy and Marine Corps user accounts on 340,000 seats servicing over 3,000 locations across the continental United States, Hawaii, Cuba, Guam, Japan, and Puerto Rico. This contractor owned/contractor operated network was designed to provide secure, universal access to integrated voice, video, and data communications and a common computing environment across the DON, which played a critical role in dramatically improving security across the enterprise.

In addition to the Outside the Continental United States (OCONUS) sites served by NMCI, the **OCONUS Navy Enterprise Network (ONE-NET)**, including the Base Level Information Infrastructure (BLII) efforts, provides roughly 41,000 users at shore installations overseas, a single integrated network with a full range of services, and a centralized control authority. It is a government-owned, government operated, Navy enterprise network that delivers centralized IT, improved security, standard configurations, and increased service levels to commands overseas.

For the afloat forces, the **Information Technology for the 21st Century (IT-21)** portfolio of acquisition programs provides networking capabilities to the fleet. These programs include local area networks (e.g., Integrated Shipboard Network System (ISNS)), services (e.g., Global Command and Control System – Marine Corps (GCCS-M)), routing (e.g., Automated Digital Network System (ADNS)), satellite communications (e.g., Extra High Frequency (EHF), Super High Frequency (SHF) and/or Ultra High Frequency (UHF)), and a shore-based infrastructure that supports global operations (e.g., Tactical Switching).

Within the Marine Corps, the **Marine Corps Enterprise Network (MCEN)** is a portfolio of acquisition programs that provides network services to CONUS, OCONUS, and deployed Marine Air-Ground Task Forces (MAGTFs). MCEN utilizes NMCI and IT-21 capabilities besides its own internal tactical function.

The current Naval Networking Environment is also comprised of over 500 **legacy networks** that typically support specific functions within individual DON organizations or cross-service functions. Since the legacy networks are also typically associated with legacy applications, work continues to reduce and replace legacy applications with applications that are not dependent on specific hardware and software. Other examples of these networks would be the Department's Research and Development and Test and Evaluation networks, each usually carrying large volumes of telemetry, video, and/or computer aided design data across either DON or Department of Defense (DoD) dedicated networks to their bases and stations; the Tri Care and Service Medical networks; the Training Commands and Service Academy classroom training and education networks, and the networks that support the Service's Recruiting Command functions in large and small remote locations across the country.

1.2 Shaping the Naval Networking Future

As the Department evaluates the steps necessary to achieve its net-centric future for NNE~2016, there are several events and programs that are shaping the planning for that future. The **end of the NMCI contract** is the most critical near-term event. The Department of the Navy is currently in the process of identifying requirements and planning for acquisition and implementation of its Next Generation Enterprise Network (NGEN), which will be the replacement for NMCI.

Both the Navy and Marine Corps are pushing for a **reduction of legacy networks**. The Navy's Cyber Asset Reduction and Security (CARS) task force and the Marine Corps' Legacy Network Consolidation (LNC) efforts are charged with identifying and implementing consistent, secure solutions for consolidating legacy networks and systems. It is the Navy and Marine Corps' goal that most of the Navy's and many of the Marine Corps' legacy networks will either be consolidated into existing enterprise networks or eliminated. A limited number of legacy networks will be permitted to continue operations as "excepted" networks.

The **Standup of the Consolidated Afloat Networks and Enterprise Services (CANES)** effort is the Afloat strategy for reducing server footprints and migrating existing shipboard hardware into a centralized, managed process, replacing ISNS and parts of IT-21. It will also provide the Fleet with an ability to collaborate and share information across the warfighter domain with reach-back to the assisting shore establishments.

The **Standup of Marine Corps Enterprise Information Technology Services (MCEITS)**, a core capability within the Marine Air-Ground Task Force Command and Control (MAGTF C2) framework, will provide end-to-end capability by enabling access to enterprise information and providing the ability

to collaborate and share information across the business and warfighter domains within the Marine Corps community of interest.

Lastly, the **Standup of the Maritime Headquarters - Maritime Operations Center (MHQ w/MOC)** concept will provide high-level focus on the Navy's operational level Command and Control (C2) processes and the full capability to perform the Joint Force Maritime Component Commander (JFMCC) role in joint operations.

Each of these, as well as numerous other DoD related efforts (Net-Centric Enterprise Services (NCES), Defense Knowledge Online (DKO), Global Information Grid (GIG) Convergence Master Plan (GCMP), etc.) will play a significant role in shaping the future strategies that will be needed for NNE~2016.

1.3 Immediate Near Term Focus

While this document is primarily focused on the long-term goals of the Department, efforts must also immediately focus on the Department's more immediate opportunity to begin laying the groundwork with NGEN for the NNE~2016 transition. NGEN will be the replacement for the NMCI contract. Without "doing harm" to the Department's existing IT user capabilities, the initial block of NGEN is required to be in place in time to ensure the continuity of the Department's basic shorebased IT services after the NMCI contract ends in September 2010.

The Department has completed a requirements analysis and determination as part of the Functional Area Analysis (FAA), Functional Needs Analysis (FNA), and Functional Solutions Analysis (FSA) to determine what additional NNE~2016 capabilities should be added to the NGEN Block 1 procurement, without injecting an unacceptable level of risk into the transition from NMCI to NGEN Block 1. The transport for Block 1 is intended to be the Defense Information Services Agency (DISA) Defense Information Services Network (DISN) and the Global Information Grid (GIG) provided Non-Classified Internet Protocol Router Network (NIPRNet)/Secret Internet Protocol Router Network (SIPRNet) services, potentially supplemented for the shore establishments where high speed DISA services are not available. NGEN Block 1 will comply with DoD policy, operations, and architecture standards, and mandated use of the enterprise provided services.

As the acquisition strategy for NGEN Block 1 is developed and implemented, the Department will continue to analyze the needs, requirements, and funding for the future "block upgrades," that will bring NGEN closer to achieving the NNE~2016 objectives. By utilizing the block upgrade approach, the Department will be able to evaluate and analyze the advances in technology, requirements, and any changing DoD network architectures at that point in the planned procurement life cycle, allowing any updated/upgraded standards to be rolled down into the NGEN Block 1 technical refreshment cycle. This approach is also in line with the Clinger-Cohen Act's mandated modular improvement strategy.

1.4 Document Life Cycle

This NNE~2016 document is not intended to be static. It highlights several of the major strategy development assumptions that had to be made. It also addresses numerous strategy focus areas that have been identified by the Strategy & CONOPS Task Force and the NGEN Requirements Combined Task Force, in their FNA, as requiring further study or expansion. Several of these focus areas could have a significant impact on both the overall NNE~2016 and on any near-term acquisition actions.

1.5 Enforcement of the NNE Vision

As part of the recently initiated SECNAVNOTE 5000 Gate Review Process, DON CIO will be ensuring that the architecture and plans for all programs and initiatives, within the scope of the NNE, are aligned

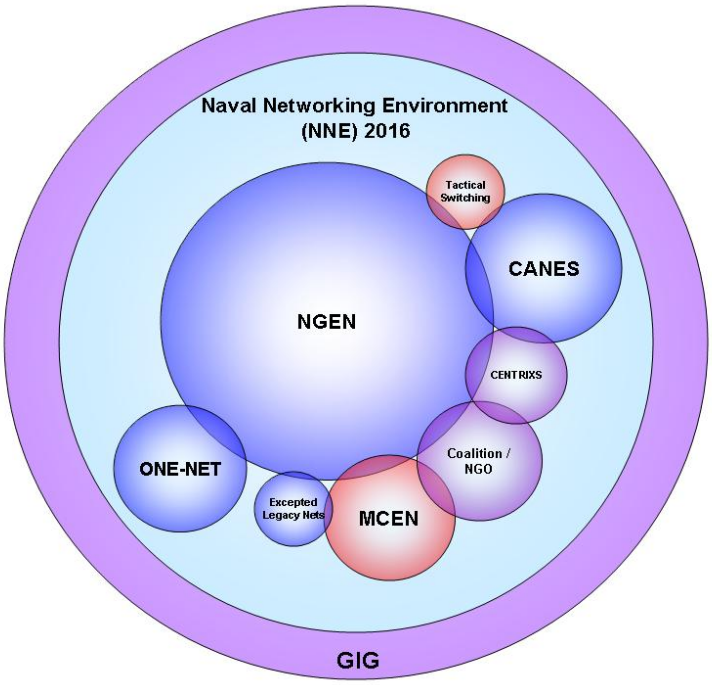
with, and fully supportive of, the Department's NNE vision. In addition, all Integrated Support Plans (ISP) and Clinger Cohen Accreditation requests will be assessed for their alignment and support of the NNE vision.

2.0 NNE Definition and Scope

2.1 Strategic Definition. The Department of the Navy's Naval Networking Environment~2016 is an iterative set of integrated, phased programs that will guide the DON towards a future net-centric enterprise environment. It is a highly secure and reliable enterprise-wide voice, video, and data network environment that focuses on the warfighter first, providing ubiquitous access to data, services, and applications from anywhere in the world. Under the NNE~2016, current enterprise networks, core network services, functional programs and projects, major applications that will reside on the network, and their follow-on efforts, will be bound by a common enterprise architecture and standards, and a common governance and operational construct, consistent with network operations (NETOPS). This will result in an interoperable, Joint enterprise environment that is standardized and enables secure access to data and services across all boundaries of NNE~2016.

2.2 Scope. NNE~2016 includes NGEN (all Blocks), ONE-NET, CANES, MCEN, and the remaining excepted legacy networks approved by the Department. It will also include the enterprise core network services, functional programs and projects, and major applications that will reside on the various Naval networks, guided by a common Enterprise Architecture and standards. Other non-Naval Joint networks will be investigated and integrated on a case-by-case basis if they further the Department's ability to achieve the Operational Forces' desire for Joint, Coalition, and non Government compatibility, as shown in Figure Two, including the Combined Enterprise Regional Information System (CENTRIXS). At a minimum, as part of the development of the NNE~2016, each of the Joint network environments will be documented and governed by a NNE~2016 interface control document in order to achieve a measured degree of collaboration, interoperability, data accessibility, and consistency of Information Assurance (IA) posture.

Figure Two – Scope of NNE~2016



3.0 Development Of The NNE~2016 Strategies

3.1 Discussion As the NNE~2016 will evolve and be refined over time, so too will the strategies associated with it. As part of the multi-phase development of the NNE~2016, the development team evaluated the potential innovative methods that could be employed as part of NNE~2016 based on the recently released Navy and Marine Corps evolving concept of operations in a Joint future force environment. Since the Department was also preparing to update its DON Information Management/ Information Technology (IM/IT) Strategic Plan for submission to the DoD CIO, these methods were compared to existing Department and Service specific IT planning documents to ensure the major operational needs were being addressed.

3.2 Naval Missions, Operational Concepts, and Methods Our U.S. Naval Forces have historically accomplished the important naval missions of forward presence, crisis response, deterrence, sea control, and power projection. In the post 9/11 environment there has been significant increased emphasis on the non-traditional mission areas such as civil-military operations, counterinsurgency, counter-proliferation, counterterrorism, maritime security operations (including drug interdiction), information operations, air and missile defense, security cooperation with an expanding set of partners, and support to humanitarian relief in areas that have limited or no area network support due to natural disasters. We must continuously seek innovative methods to further our contribution to national security. Abbreviated examples of those methods are:

Globally Networked Operations – Establishing a scalable open access/open architecture information system to enhance organizational flexibility and global awareness;… facilitate the rapid information sharing required to expeditiously task-organize and employ….forces from worldwide locations, while appropriately safeguarding sensitive or classified information.

Distributed Operations – Increasing our ability for independent, unified action by geographically separated, yet globally, regionally, or tactically integrated, networked forces….

Adaptive Force Packaging: Right Force, Right Time, Right Place – Optimizing the combination of people and platforms to provide the right force at the right time given a particular operational requirement… proper inclusion of Joint, inter-agency, and private resources …. tailored to a specific mission.

Aggregate, Disaggregate, Re-aggregate – Expanding our ability to re-group capabilities for maximum employment options across the spectrum of operations. …deploy…disperse… merge with Navy, Marine Corps, Joint, or inter-agency elements to assume different missions….

Cross Fleet Standardization – Developing the common tactics, techniques and procedures that will improve the efficiency of globally sourced forces. Standardizing routine procedures associated with planning, communications, intelligence, fires, maneuver, logistics, and force protection will facilitate effective employment of Navy and Marine Corps forces.

Task Focused Training – Increasing the speed and agility of our forces by training to specific operational requirements…

Cultural Awareness – Enhancing our ability to understand how social, political, economic, ethnic, and religious factors impact the operational environment. …

Sea Basing – Providing operational maneuver and assured access to the Joint force while significantly reducing our footprint ashore and minimizing the permissions required to operate from host nations….

Building Partner Capacity – Increasing our capacity to work with foreign counterparts and their ability to work with us….develop the partnerships, protocols, and procedures that will permit nations with similar goals to cooperate for the common good….

Across the Department of Defense, our networks have become the basic operational backbone for all forms of communications and computing. It is the indispensable enabling component to network-enabled warfare, and the transmission medium for all types of voice, video, graphics, text, and sensor data. Provisioning, defending, managing, and optimizing the network has become a warfighting imperative, as recognized by the GIG NETOPS Concept of Operations. NETOPS is the DoD strategy for directing the operations and defense of the GIG consisting of three dependent and mutually supporting missions of GIG Enterprise Management, GIG Network Defense, and GIG Content Staging. To support this strategy, DISA has planned and programmed the converging technologies between now and the 2016 timeframes required to achieve this objective, as outlined in the GCMP.

To achieve interoperability within this environment, the overarching construct of NNE~2016 and the associated integration of currently independent network domains must make NETOPS a centerpiece of the integration and operations strategy. NETOPS provides the transformational impetus that converts networks from simple infrastructure controlled through administrative changes to a global warfighting system that is controlled by the Combatant Commanders (COCOMS) in support of national military objectives. In addition, NNE~2016 will support Joint basing IT services for regions where DON is assigned EA responsibilities. The Department of the Navy will align its NNE~2016 plans with the DoD and DISA's efforts to capitalize on the joint opportunities surrounding the GCMP. The phased convergence strategy of the GCMP (2008 – 2016) will provide increasing amounts of common communications and computing infrastructure and collaborations capabilities to the Navy, Marine Corps, and other Services and should accelerate DoD's transition to a Joint net-centric environment.

4.0 Strategy Development

4.1 Discussion. Since 9/11, the requirements of the commands currently supported by NMCI and ONE-NET have changed as the Department has engaged in the Global War On Terror. Shore based and forward operational commanders in the Fleet view all of the Department's enterprise networks as extensions of their ability to command and control forces and have again stated that coalition and multinational C4 interoperability remains the number one Fleet priority. Given past funding priority challenges, the Fleet forces have also stated that separating the shore-based networking environment from the shipboard or forward deployed networking environment does not support secure, reliable, and redundant global communications for the warfighters. The Department's experience demonstrates that a dual resource track leads to a sub-optimized network environment with many nodes not capable of operating in a globally networked environment. In today's changing environment of network-centric operations, unnecessary diversification at this level cannot happen if the NNE~2016 vision is to be achieved.

To address the needs of all networking and information technology stakeholders, the strategy development efforts focused on investigating three distinct approaches, as follows:

- Top Down
- Focus Areas
- Bottom up

4.2 Top Down Strategies. Based on the review of the Naval Net-Centric CONOPS, and to ensure the requirements of the Fleet and Operational Commanders are met, the following steps must be taken as the NNE~2016 is planned and implemented.

A. The NNE~2016 leadership must aggressively govern the NNE~2016 to determine the right technical solutions, make sure these solutions are affordable, ensure the Department is organized to execute the solutions (buy, build, deploy, maintain and refresh), while making sure that applicable statutes, regulations, and policies are being followed.

NNE~2016 must establish and provide for a scalable open access/open architecture computing and communications environment to enhance the Department's organizational flexibility and global awareness. This environment must facilitate the rapid information sharing required to expeditiously task, organize, and employ forces to and from worldwide locations, while appropriately safeguarding sensitive or classified information.

1. The NNE~2016 must be the impetus to develop the plans, policies, and programs required to functionally integrate the Department's Naval networks and computing and communications environments into an interoperable infrastructure with consistent architecture, standards, and security strategies capable of sustaining both warfare and warfare support functions.

2. The NNE~2016 will utilize, to the maximum extent practical, the capabilities that will be provided to all DoD users under the GCMP. These core capabilities and services will shape NNE~2016 planning.

3. The NNE~2016 must facilitate the collection, dissemination, reuse, and storage of reliable, assured, trusted information and data, transparently across all operational boundaries. To do this, NNE~2016 must make maximum use of the DoD collaboration services provided under Net Centric Enterprise Services (NCES).

4. The NNE~2016 must implement a net-centric data strategy that will support robust, enterprise data sharing consistent with the tenets of net-centric operations and warfare (NCOW).

B. The NNE~2016 will provide the Joint/Naval Commanders with a command and control capability, both ashore and afloat, with assured global reach and reach-back capabilities.

5. The NNE~2016 must provide a secure, responsive, agile, integrated, and defendable worldwide network environment that will support C2 operations in theater, in remote locations, and in support of disaggregated forces and occasionally connected ground units involved in operations from crisis response to security cooperation.

6. The NNE~2016 must provide for seamless connectivity across all of its physical network environments or communities of interest.

C. Due to the continuing and growing presence of terrorists and other national and trans-national threats, along with the use of irregular and disruptive techniques to defeat networks and critical information infrastructure, the NNE~2016 must create a computing and communications environment that will be under positive control, and is secure and defendable.

7. The NNE~2016 will incorporate the procedures and protocols needed for the assurance and resilience of Open Architecture (OA) networks targeted by an increasingly sophisticated enemy (e.g., Information Warfare) and for secure, assured information sharing across the full spectrum of multi-national, federal, state, local, and private sector entities.

8. The NNE~2016 will leverage and utilize the Joint capabilities and security services provided under the National Security Agency (NSA) IA plans and GCMP to ensure a joint information assurance/information security posture.

D. The NNE~2016 will provide the U.S. Naval forces with the ability to employ complementary information operations to support the Combatant Commanders' objectives and exert coordinated global influence, regardless of the size, scope, nature, or duration of these missions.

9. The NNE~2016 will utilize Joint capabilities and services (GIG & GIG-Bandwidth Expansion (BE), NCES, etc.), and integrate/expand on DON enterprise initiatives (NMCI, ONE-NET, CANES, MCEITS, Enterprise Shared Data Environment (ESDE), Distance Support, etc.) to ensure complimentary, cost effective capabilities across its netted force.

10. The NNE~2016 must ensure that the resultant computing and communications environment will directly support the ability to provide for an electronic "quality of life" for its Sailors and Marines.

E. The NNE~2016 must provide for constructive interdependence between the Navy and Marine Corps operational forces, as well as our Joint and Coalition allies.

11. The NNE~2016 will integrate the unique capabilities resident in the both the Navy and Marine Corps by establishing and controlling the enterprise architecture and standards that will govern the phased roll out of the NNE~2016 capabilities, consistent with DoD Enterprise Architecture (EA) and operational standards.

F. The NNE~2016 will provide for a computing and communications environment that will enhance our security state of readiness in an environment characterized by a combination of traditional, irregular, catastrophic, and disruptive challenges.

12. The NNE~2016 will leverage OA and Service Oriented Architecture (SOA) concepts to enable highly adaptive, agile, and flexible access to all available data and service sources. The SOA environment will conform to "open," non-proprietary standards and will dictate the adoption of approved software tools to be used whenever application logic is designed or maintained.

13. To ensure uninterrupted operations, the NNE~2016 will make use of redundant rollover and backup capabilities between all shore-based and shipboard computing and communications environments, to include all Continuity of Operations Planning (COOP) needs. Within the NETOPS construct, COOP must be an integral capability which is engineered into the design, in order to ensure there are no single points of failure within any part of the NNE~2016 to include but not limited to the Regional Network Operations Security Centers (RNOSCs), terrestrial infrastructure nodes, satellite or earth station nodes, or forward-deployed supportability nodes for any of the SOA services.

14. NNE~2016 will investigate expanded use of web clients as a part of the proposed architecture. This will include web client desktops, laptops, PDAs, and cell phones.

15. NNE~2016 will implement techniques and approaches for logically segregating our networks and information from the public Internet, without impacting the ability of DON personnel to accomplish their missions and functions. NNE~2016 will provide commanders the tools necessary to manage their bandwidth utilization.

G. The NNE~2016 will allow US Naval Forces to partner, communicate, and share information with a diverse array of multi-national, federal, state, local, and private sector entities given a particular operational requirement… proper inclusion of Joint, inter-agency, and private resources … tailored to a specific mission.

16. The NNE~2016 will implement a net-centric data strategy and enterprise shared data environment, consistent with the tenets of NCES, MCEITS, and CANES, which will be responsive, agile, and provide authenticated data to support effective decision making in both naval and Joint/Coalition engagements. This data will be made available to all authorized users, independent of network environment or location.

16. Separate classes of official communications will be established for access and uses of NNE~2016 by coalition forces. Only official traffic will be allowed and access will be limited to designated servers. In all such cases communications shall be archived in accordance with statute and policy.

4.3 Strategy Focus Areas. The Department of the Navy has identified numerous focus areas that are being investigated and will result in other strategies or alterations/enhancements to the requirements for the NNE~2016. Cross functional teams have been established to address each of the areas shown below.

- Support of Warfighting Missions and Functions
  - Exercise Command Leadership
  - Leverage Mission Partners
  - Monitor Execution and Adapt Operations
  - Operational Planning
  - Synchronize Execution Across All Domains
  - Communicate Commander's Intent
  - Establish and Adapt Command Structures
- IT Workforce
  - User Training and Learning Management
- Level of Design and Operational Control of the Network
  - Legal Authority
  - Visibility and Reporting
  - C2 Capability
- Information Assurance
  - Protect Information
  - Transform and Enable IA Capabilities
  - Provide Integrated IA Situational Awareness / IA C2
  - Defend Systems and Networks
- Enforcement of Target Architecture and Leveraging of Enterprise IT Initiatives
  - SOA
  - Open Architectures
  - MCEITS
  - NCES
  - NMCP/DKO
- Universal Access and Adoption of Emerging Technologies
- Enterprise Licensing
- Acquisition Strategies and Financing Methodologies
- Legacy Network Environments
  - USMC NGEN Legacy Networks MCEN Strategy
  - USN Legacy Network Environment Strategy
- Telecom
  - Enterprise Managed Services
  - Visibility of Procured Assets and Services
  - Telecom Architecture
- Enterprise Content Management
- Privacy
- Data Strategy
- IT Services Frameworks
- Application, System, and Services Portfolio Management
- IT Governance
- Performance Management

Each of the Strategy Focus Areas that are under investigation is described in more detail, below.

4.3.1 Enabler of Warfighting Missions and Functions

4.3.1.1 Exercise Command Leadership. NNE~2016 will provide the information infrastructure that will enable commanders to exercise leadership and control over assigned forces.

Commanders must be able to exercise authority and direction over assigned and attached forces in the accomplishment of a mission. Commanders must be able to exercise effective leadership of an interdependent Joint force in rapidly changing scenarios involving complex distributed, simultaneous, or sequential operations, often with other agencies and nations. Commanders must be able to:

- Promulgate rules of engagement
- Issue necessary guidance for the employment and support of provided forces
- Establish and cultivate relations with mission partners
- Employ all assets available including instruments of national power, in a synchronized and integrated fashion, to achieve theater, national, and/or multinational objectives

4.3.1.2 Leverage Mission Partners. NNE~2016 will provide the information infrastructure that will enable commanders to interact with mission partners during an operation.

The ability for commanders to achieve/maintain unity of effort and to leverage the capabilities of mission partners not under his command. This is accomplished through coordination, collaboration, influence, persuasion, negotiation, and diplomacy, as appropriate. Mission partners may include other DoD units, non-DoD agencies, and coalition and international organizations. Commanders must be able to:

- Communicate mission objectives and support needs via, depending on the mission partner, available and applicable means of communication
- Establish structures and processes for collaboration with interagency and multinational partners

4.3.1.3 Monitor and Adapt. NNE~2016 will provide the information infrastructure that will enable commanders to monitor, assess, and adapt to operational developments on the battlefield.

Commanders must have visibility over friendly unit decisions and capabilities and the ability to monitor and react to changes in adversary status. Planners must be able to predict desirable and undesirable attack consequences and how effects may propagate throughout an adversary's system. The ability to respond rapidly and effectively to changing circumstances will enable commanders to maintain the initiative. Commanders must be able to:

- Track, shift, reconfigure (i.e. control) forces, equipment, sustainment, and support, even en-route
- Collaboratively assess achievement of planned effects
- Collaboratively identify and assess implications of unintended effects
- Use appropriate existing commanders, staffs, and associated support tools to collaboratively update and adjust plans to meet changing operational priorities
- Collaboratively integrate commanders' feedback, staff and organization inputs, and overall operational knowledge to determine the appropriate action when desired objectives are reached

4.3.1.4 Operational Planning. NNE~2016 will provide the information infrastructure that supports operational planning.

Operational planning, drawing on global resources and considering global consequences, directly ties offensive actions to campaign objectives. Planners must be able to focus on exploiting critical adversary vulnerabilities and must consider friendly critical capabilities and potential collateral damage. Parallel, distributed, collaborative planning capabilities and improved assessment tools are needed to compress process timelines. Commanders must be able to:

- Collaboratively develop, analyze, and select the COAs, branches, and sequels
- Collaboratively develop Joint and mission partner campaign plans, including the synchronization matrix and cooperation with the Maritime Domain Awareness (MDA) efforts
- Collaboratively develop operational plans across the Joint capability area domains
- Collaboratively assess effectiveness of plans and prepare for execution

4.3.1.5 Synchronization. NNE~2016 will provide the information infrastructure that supports the synchronization of the actions of operational forces.

The commander must be able to synchronize the actions of their assigned forces. This can be done through centralized direction, as in the past, or in a decentralized manner through self-synchronization of subordinate forces. The commander must have the ability to employ whichever method of synchronization is appropriate to the situation. Self-synchronization requires subordinates to have a clear understanding of the commander's intent, shared situational awareness (SA) and operational trust, good communications, and the ability to act without detailed direction from above. Commanders must be able to:

- Collaboratively synchronize operations among staff and subordinate commanders
- Establish appropriate operational, personal, liaison, electronic, and network linkages with mission partners to ensure coordination of operations
- Establish communications contact and ensure synchronization of activities and that procedures exist to support the effective transition of phases
- Validate targets prior to attack

4.3.1.6 Commanders' Intent. NNE~2016 will provide the information infrastructure that will enable commanders to communicate their intent to assigned and supporting forces.

Commanders' Intent is the ability for a commander to concisely express the operational purpose and desired end state. As the impetus for the planning process, it may also include the commander's assessment of the adversary commander's intent and an assessment of acceptable operational risk. In the net-centric collaborative environment, the commander's intent must be shared early and often to enable parallel planning and self-synchronized execution. Commanders must be able to:

- Collaboratively conduct mission analysis to develop commander's intent, warning order, deployment order, etc.
- Promulgate commander's intent and guidance
- Direct action through mission-type orders to subordinate echelons with minimal delay and confusion

4.3.1.7 Command Structures. NNE~2016 will provide the information infrastructure that will enable commanders to adapt their C2 structures and processes to support emerging operational needs.

Commanders need to quickly establish or adapt command structures across the force, with all mission partners and within the staff tailored to the mission, and to create the processes that will enable horizontal and vertical collaboration. It is essential that the infrastructure be in place to enable rapid reaction to new crises. Commanders must be able to:

- Exercise the core functions of command from austere as well as robust fixed sites, mobile sites (i.e., "on the move"), and in transition between sites
- Develop organizations and links between organizations to provide the agility to allow units to create self-synchronizing joint forces
- Establish/refine collaboration structures and processes across the force, including standing and ad hoc functional cells and communities of interest
- Establish collaboration mechanisms with mission partners

4.3.2 IT Workforce

4.3.2.1 User Training and Learning Management. To ensure that each user is fully capable of utilizing the NNE~2016 applications, capabilities, and services required by their job, a single, reliable, and efficient Learning Management System (LMS) must be implemented.

Information technology is one of the primary tools that DON personnel use in all aspects of their work – from personnel and pay specialists to command and control operations. Networks, computing services, and applications provide the means of accomplishing tasks in today's environment. In order to ensure that the capabilities and services provided through NNE~2016 are fully utilized, the users of those capabilities must be fully trained and the means must exist to continually train new users while providing for training on new applications and services. This training must encompass the needs of deployed and in-garrison personnel – training that is stove-piped in today's environment. The lack of manning and training of shipboard network administrators must be addressed. Shipboard network administrators must be multi-talented due to the lack of contractor specialist support that is required, but not available at sea. Once trained, at-sea forces must be able to quickly shift to shore-based assignments with minimal retraining, and vice versa. In order to ensure that future training meets the needs of the DON, the Government must be the responsible and authoritative source for requirements, review and approval of training content, determination of method of training delivery, and determination of training effectiveness. To fully coordinate training across afloat and ashore networks requires a single point of review and approval, which cannot be outsourced.

The LMS will be used to track NNE~2016 user learning and qualifications/certifications, provide access to NNE~2016 user training materials that are either government-developed or commercially available, and provide status reporting to stakeholders; i.e., initial and annual government-developed information assurance training. The Government will oversee and manage the development of training requirements and implementation of training plans approved and managed by DON military and government civilian personnel.

4.3.2.2 IT Workforce. As part of NNE~2016, establish a DON enterprise workforce able to easily function in the IM, IT, information assurance (IA) and information operations (IO) domains.

To ensure DON oversight, systems integration, engineering and design visibility and approval, operational control, configuration control, and asset management of afloat and ashore networks and associated computing services in a net-centric capable Naval networking environment, a new set of roles, responsibilities, and associated competencies will be developed and implemented across the DON IM and IT workforce. This includes those actions necessary to ensure that the workforce will:

- Provide secure and reliable networks
- Manage security in a distributed environment
- Conduct network, operating systems, and support services assessment and management
- Manage DON network and network-related IT assets
- Review and approve required architectures
- Oversee management and operations of NNE networks
- Provide telecommunications support (to include spectrum management)
- Acquire and incorporate new technologies into existing structures
- Provide network program management
- Be versed in the Information Technology Services Management approach
- Conduct data management

4.3.3 Level of Design Control. The Government will assume the Technical Design Authority (TDA) leadership role across all DON enclaves in order to achieve the objectives of NNE~2016.

The NNE~2016 Design Control strategy is based on the premises that the NNE~2016 environment will be a mix of government owned/government operated, government owned/contractor operated and contractor owned/contractor operated networks. In order for the Government to properly achieve its intended infrastructure goals and meet the intent of CANES, NCOW, NETOPS, and NCES in this budgetary and technologically uncertain environment, it is essential that the Government assume the central design authority role, evaluating and authorizing both commercial and government network architectures and solutions.

The Government will manage design control via oversight and authorization of all government and contractor design recommendations for the capability implementation baselines recommended by the various programs that constitute the NNE. Security design will be strictly controlled through the development and approval of the DON Senior IA Official (DON CIO) and the network Designated Approval Authorities (DAAs). A rigorous systems engineering approach will be applied in the design elements of NGEN that will support the lifecycle of the capability and/or technology insertion. Final approval of changes will be accommodated through a joint Configuration Change board that includes all major stakeholders. A process for emergency changes (i.e. Information Assurance Vulnerability Alert/Information Assurance Vulnerability Management, patches, immediate operations needs) will be closely coordinated through the NETOPS chain (e.g. Naval Network Warfare Command and Marine Corps Network Operations and Security Command). The Government will manage all elements related to the NGEN design through an enterprise architecture, architecture-based modeling and simulation, integration with industry, and government approved standards.

4.3.4 Operational Control of the Network. The Government will assume operational control of all NNE~2016 enclaves in order to ensure that network commanders have the authorities, situational awareness, and C2 tools and processes necessary to execute effective operational control of networks and IT services that align with and directly support warfighting and warfighting-support operations.

In order to successfully support warfighting and warfighting-support operations under NNE~2016, it is essential to pursue a strategy that provides NETOPS Commanders effective operational control of networks and IT services. Increasing dependence on networks and services to provide timely accurate information as the "lifeblood" of all other operations and the need to defend the network environment against a similarly increasing threat, has propelled DoD towards viewing cyberspace as more than a set of IT services, but as a critical warfighting capability. Today the networks are considered a critical infrastructure and the cyberspace they inhabit, a battlespace to be defended under the NETOPS mission assigned by the Secretary of Defense in the Unified Command Plan to Commander, US Strategic Command (USSTRATCOM). The Joint Concept of Operations for Global Information Grid NETOPS provides Commander, USSTRATCOM the concepts and C2 framework for GIG NETOPS, describing how NETOPS provides direct support to warfighter, business, and intelligence operations.

4.3.5 Information Assurance

4.3.5.1 Protect Information. NNE~2016 users will safeguard data and information as it is created, used, modified, stored, moved, and destroyed at the client, within the enclave, at the enclave boundary, and within the computing environment to ensure that all information has a level of trust commensurate with mission, based on assessed risk and mandated policies that govern protection of specific categories of information.

The goal of the GIG is to enable information originating from anywhere on the network to be available when required throughout the network. Not only must the information be accessible, but it must be trusted. A risk-based assessment must be done to determine the appropriate levels of safeguards for each class of data considered. Mission needs, as well as the level of sensitivity or classification, will all contribute to the levels of protection required.

Commanders must be able to trust their information at all levels. Mission-critical information must be accurate, timely, and available when needed to enable warfighters to achieve success. Information protection is accomplished through a defense-in-depth security architecture that includes comprehensive security specifications for IA and IA-enabled products, systems, and networks that are built into the products, systems, and networks lifecycle; security operating policies and procedures; security control validation; and personnel security controls, including security awareness and training.

4.3.5.3 Situational Awareness. NNE~2016 will implement an IA Situational Awareness (SA)/IA C2 posture that will be integrated into a User-Defined Operational Picture (UDOP), synchronized with NETOPS and emerging Joint C2 Common Operating Picture (COP) programs.

The complex and interdependent nature of our information networks and the demands of net-centric warfare require shared awareness and understanding across the enterprise to enable effective C2. Commanders require sufficient visibility into their network operations and the IA capabilities applied to protect, defend, and respond to them. This will provide decision makers and network operators, at all command levels, the tools for conducting IA and Computer Network Defense (CND) operations in the net-centric environment.

4.3.5.4 Defend Systems and Networks. An evolving capability to proactively recognize, react, and defend against threats and vulnerabilities in systems and networks to ensure that no access is uncontrolled and all systems and networks are capable of self-defense based on a risk-based assessment will be an integral part of the design and implementation of NNE~2016.

DON systems are constantly under attack and must be continuously defended. To ensure success, defensive mechanisms must be an integral part of the design and implementation of systems and networks across the enterprise, including NGEN and the NNE. Capabilities must be deployed to recognize and react to threats and attacks. The principal points of focus are CND protection, detection and reaction mechanisms for DON systems and networks, and adaptive configuration management. Adaptive configuration management is a critical capability that includes both active and passive defenses necessary to "correctly" respond to legitimate but changing demands while simultaneously defending against adversary-induced threats. Controls, devices, and procedures to recognize, react, and respond to potential system and network compromises must be in place and provide control sufficient to protect the integrity, confidentiality, and availability of NNE~2016.

4.3.6 Enforcement of Target Architectures and Leveraging IT Initiatives

4.3.6.1 Service Oriented Architecture. To align the DON to the DoD goal for a net-centric interoperable environment, programs under NNE~2016 must support the transformation to an enterprise SOA approach throughout the DON.

The DON must transform to an enterprise SOA approach that accelerates the decision cycle process throughout the DON and aligns to the DoD goal for a net-centric interoperable environment. The SOA strategy for the DON consists of employing enterprise level services that provide reusable capabilities via fixed and shore-based networks, forward deployed afloat networks, and forward edge networks such as mobile ad hoc networks. It also allows for the seamless integration of new agile technology (e.g. web services) to facilitate the Department's transformation to a net-centric interoperable environment. NNE~2016 will leverage current and future DoD/DON IT initiatives (e.g. NCES, DKO, MCEITS, etc.) by implementing SOA within the DON Enterprise Architecture. The DON SOA strategy within NNE~2016 will improve the effectiveness of the Department in meeting mission requirements, be it warfighting or warfighting-support, from any domain environment, anywhere, anytime, by accessing authoritative data and services that accelerate the decision-making cycle process of the warfighter. SOA can provide the following key benefits:

- Improve cost effectiveness, productivity, agility, and speed
- Allow IT to deliver services faster and align closer to the warfighter requirements
- Allow the business processes to respond more quickly with optimized deliverables
- Improved collaboration due to interoperable information access and exchange

4.3.6.2 Open Architecture. NNE~2016 will adopt an OA based on open standards which will allow the DON to achieve an affordable future by enabling the Naval forces to rapidly adapt to new missions and new threats.

Capabilities implemented on an open architecture leveraging open standards will create an interoperable fleet that can connect seamlessly with all DoD agencies and our nation's allies and global partners. This approach significantly increases opportunities for innovation and competition, enables reuse of components, facilitates rapid technology insertion, and reduces maintenance constraints. The Navy and Marine Corps have adopted OA as a way to reduce the rising cost of Naval warfare systems and platforms and to increase the capabilities of our systems. More importantly, OA will contribute to greater competition among system developers through the use of open standards and standard, published interfaces. These OA business and technical principles will deliver increased capabilities in a shorter time at reduced cost.

4.3.6.3 NCES. NNE~2016 will utilize the enterprise services provided under DoD's NCES program, to the maximum extent practical.

DoD is transforming the way it conducts warfare, business operations, and enterprise management. NCES is the foundation and one of the catalysts for transforming the current environment to a dynamic, collaborative, information sharing environment. This strategy enables the warfighter to utilize these capabilities no matter where current operations exist. The specific performance achieved will be dependent on the specific constraints of the operating environment. The NCES program will provide the capabilities and technical integration for secure and globally connected services that support the situational awareness, machine-to-machine (M2M) messaging, discovery, collaboration, security, availability, and user pull of needed information at the strategic, operational, and tactical levels throughout the full range of military, business, intelligence, and homeland defense operations. The DON will leverage these capabilities to the maximum extent practicable, while ensuring that any necessary capabilities not provided by the NCES program, will be provided by internal DON initiatives, such as MCEITS and CANES.

4.3.6.4 MCEITS. As part of the NNE~2016, the Department will use the Marine Corps Enterprise Information Technology Services (MCEITS) core capabilities to support and augment the DoD NCES initiatives.

MCEITS is a core capability within the Marine Air-Ground Task Force (MAGTF) C2 Framework and System of Systems (SoS). MCEITS contributes to the MAGTF C2 Framework end-to-end capability by enabling access to enterprise information and providing the ability to collaborate and share information across the business and warfighter domains. MCEITS accomplishes this by implementing an IT infrastructure with application, service, and data environments. MCEITS will deliver an IT infrastructure that can quickly and easily adapt to the evolving software, hardware, data, services, and management requirements while providing an enhanced enterprise visibility that facilitates greater reuse of IT assets. These capabilities provide responsive support for a secure, collaborative, interoperable data sharing environment while enabling the integration of products, services, and users via a SOA framework. With NCES compliance at the heart of the effort, MCEITS will provide the Marine Corps a common SOA framework for integration. This is expected to include the material solution portion of NNE~2016, particularly since the services provided from within the NNE~2016 solution should be NCES compliant. Additionally, and as part of the identified MCEITS capability set, it will provide enterprise-class data storage and application hosting capabilities. The Marine Corps will ensure integration of the MCEITS framework into the NNE~2016 material solution, such that MCEITS provides seamless information sharing.

4.3.6.5 Portal Strategy. NNE~2016 will provide a Navy Marine Corps Portal (NMCP) technology gateway that leverages common DoD/DON architectures and core net-centric capabilities (e.g. NCES, DKO).

The majority of Navy and Marine Corps portal initiatives are currently at the individual command level with no enterprise alignment strategy for seamless information and capability sharing. The DON will decrease cost and improve warfighting agility and business process effectiveness by consolidating its current portal investments into a single infrastructure (i.e., the NMCP Gateway). The NMCP Gateway, leveraging a consolidated DON portal infrastructure and DKO, is a vital piece of the strategy for providing interoperable information sharing across the NNE~2016.

4.3.7 Universal Access and Adoption of Emerging Technologies. The NNE~2016 must make the best possible use of current technologies and be flexible enough to adopt emerging technologies and rapidly satisfy operational needs.

The Department's desire to monitor, influence, and rapidly adopt emerging technologies to meet critical mission needs is somewhat hampered by current business practices. Current DON IT management and business practices are not optimized to ensure rapid development, testing, and implementation of new information technologies. The processes for identifying and prioritizing a new technology driven requirement; budgeting for the requirement; contracting for the capability; and developing, testing, and fielding the capability (including its non-material solution parts) are currently lengthy and not fully responsive to critical mission needs.

Many new technology requirements are generated reactively as the result of general progress on capabilities in the private sector or by others in DoD. In other cases, the requirement stems from a new threat to security and/or has been mandated for adoption by US Strategic Command (USSTRATCOM) or Joint Task Force-Global Network Operations (JTF-GNO). In each case, these technologies may or may not meet unique DON needs, since they were initially developed by and for use by the private sector or other government agencies. They often require further testing, prototyping, and small scale deployment before they become considered for full operation deployment within the Navy and Marine Corps environments. NNE~2016 will address these issues, including the long-term life cycle support to deployed capabilities.

With the rising importance of wireless connectivity for an increasingly mobile workforce, and the improvement and miniaturization of personal communication devices, the network design for NNE~2016 should provide for fully encrypted wireless connectivity for official communications. Authorization to access the network will be identical as in the case of land-based connections.

Accommodations will also have to be made for the "unanticipated" or occasionally connected users. The new "mobile workforce" has become more accustomed to effortless connectivity as part of their generational imperative. The NNE~2016 areas of particular areas of focus must be:

- "Access anywhere" such that warfighting and business users will have the ability to access the network anywhere in the world through a single sign-on.
- "Ubiquitous access" to all their files, information, data, and services from anywhere in the NNE~2016 environment
- "Single" e-mail address across the NNE~2016 while in the service of the Department.

4.3.8 Enterprise Licensing. NNE~2016 will adopt and enforce use of the DoD/DON Enterprise Software Initiative (ESI) program/concepts.

The DON's network infrastructure has been acquired and managed using multiple methods, i.e. government owned/government operated, government owned/contractor operated, contractor owned/ contractor operated, etc. The DON's diverse investment strategies must be better aligned with each other in order to increase value to the entire Enterprise by promoting efficient and reliable purchases. Effective use of multiple acquisition strategies, including enterprise licensing and procurement will provide for more cost effective purchasing and for a common software environment for NNE~2016. The use of Enterprise licenses and procurements are key to implementing an Information Technology Asset Management (ITAM) program, which encompasses all NNE~2016 assets regardless of service provider and ownership of the assets, reduced cost through economies of scale, greater security by ensuring the

most current patches have been installed, and increased interoperability by ensuring all DON users are on the same version are paramount. The end state is a portfolio of application licenses that have significant usage across the DON. Licenses will be pre-negotiated with the vendor to determine the most cost effective purchase method while providing exceptional service and value to the NNE~2016 customers. In addition to licenses, funding for license management and application delivery and testing will be put in place as well as determining current and end state requirements.

4.3.9 Acquisition Strategies and Financing Methodologies. NNE~2016 will be accomplished using a variety of acquisition and funding process methodologies that are consistent with defined policy, oversight, guidance, and accepted business practices that enable movement toward a net-centric enterprise environment that directly supports the warfighter.

4.3.10 Legacy Network Environments. NNE~2016 will rely on the Marine Corps' LNC effort, the Navy's CARS process, and CANES to reduce the Department's legacy networks, systems, and applications.

4.3.10.1 Marine Corps Strategy. The Marine Corps' Legacy Network Consolidation (LNC) effort is designed to substantially reduce the current network infrastructure footprint by consolidating the current Point-of-Presence (POPs) infrastructure. This transformation will enable the Marine Corps regionalization efforts, the NETOPS concept, and positions the Marine Corps to field enterprise IT services (e.g., MCEITS). The LNC initiative is a concept that mitigates current gaps in the Marine Corps enterprise computing environment. The infrastructure solutions and management strategies contained in this initiative will be incorporated into two MAGTF C2 Programs of Record, MCEITS, and the Network Services program.

4.3.10.2 Navy Strategy. Through the execution of the Cyber Asset Reduction and Security (CARS) processes, all secret and below legacy IT assets, in CONUS and OCONUS will be identified and analyzed to make a determination whether those assets will be transitioned into NNE~2016 and NGEN, approved to be excepted from the enterprise environment, or terminated. CANES will be used as the afloat strategy for reducing server footprints and migrating existing shipboard hardware into a centralized, managed process. CARS forces the engagement of all stakeholders (CNO N6, echelon II and subordinate commands, Navy Functional Area Managers, Navy Command Authority (CA) and Designated Approval Authority (DAA), program managers for NMCI/ONE-NET, and Electronic Data Systems (EDS)) in the process to determine the appropriate solution for the Navy's legacy IT assets. It also merges multiple initiatives (Legacy Network Shutdown, IT Asset Reduction, and Cyber Condition Zebra) into one coherent effort to solve the Navy's IT asset management and security issues. Finally, CARS interfaces with other enterprise programs and initiatives such as Navy ERP and Sea Warrior to ensure there is coordination across these programs.

4.3.11 TELCOM

4.3.11.1 Enterprise Managed Service. Develop an Enterprise Managed Services implementation model for NNE~2016.

Portions of the NNE~2016 will be based on a managed services model. As an enterprise system, it is critical that the NNE~2016 be operated and maintained in a consistent and coordinated manner via enterprise managed services. This allows the greatest optimization of Department resources in personnel expertise, information sharing, and funding. Further, in an enterprise managed service environment, the base principle is that a suitable service is available when needed to the requesting office, enabling the

effective and efficient use of limited IT assets. Moreover, by managing services at the enterprise level, the administrative duties are centralized. As a result, duplicative administrative and technical resources are eliminated from commands and activities allowing for expenditures on additional mission-critical activities. DON organizations could then concentrate on their core mission; using information services instead of working on how to deliver information. This strategy is in accordance with recent DoD guidance to review and implement Joint enterprise services where possible and appropriate. Further, DoD has mandated the Department of the Navy utilize the Defense Information Systems Agency (DISA) for basic services, such as long distance telephone service and advanced connectivity needs which will be the underpinning to the NNE~2016 infrastructure. An enterprise managed services model will allow the DON to seamlessly integrate into Joint enterprise services, leveraging the capabilities of all the military departments and DoD.

4.3.11.2 Asset Visibility. NNE~2016 will provide integrated asset and service visibility into all networking domains.

The DON requires a substantially increased level of accuracy, comprehensiveness, and overall visibility into its asset and service inventories in order to effectively manage the enterprise. A high level of visibility and active monitoring ensures the right services are available when and where needed, costs are properly accounted, and duplicative acquisitions are reduced. Additionally, asset visibility is an essential step towards gaining and maintaining an Approval to Operate (ATO) of the particular NNE program. As the Department's primary service delivery vehicle, NNE~2016 will either contain or touch a significant portion of the DON's IM/IT assets, and provide an excellent opportunity to deliver increased asset and service visibility and continually update and communicate the benefits derived. It is therefore critical to design an NNE~2016 end-state with this IM/IT management capability in mind. The introduction of advanced automated tools, such as an automated IT asset discovery tool, to support DON-wide asset management will enhance the Department's capabilities and ensure telecommunications requirements and capabilities are acquired appropriately within the developed architecture.

4.3.11.3 Telecommunications. NNE~2016 will deliver a service oriented telecommunications architecture.

The NNE~2016 will deliver a diverse suite of services throughout the Enterprise. These services will be SOA-compliant and will include services such as voice, converged wireless, and video conferencing. The effective and efficient delivery of these services is wholly dependent on the underlying telecommunications infrastructure. That infrastructure will also be broad in scope and highly complex in order to deliver the benefits of NNE~2016 as well as respond to ongoing technical advances and convergence. The NNE~2016 telecommunications architecture is a strategic, critical asset. In order to be effective and protected, it must be documented in detail. Ideally, the NNE~2016 Telecommunications Architecture would be a logical extension of the existing DON Enterprise Architecture and a primary deliverer of the capabilities in the Operational View (as well as a prime repository of the Systems and Technical Standards Views).

4.3.12 Enterprise Content Management. NNE~2016 will provide web-based Enterprise Content Management (ECM) capabilities and infrastructure that will fulfill the statutory and regulatory requirements for records management[1].

[1] DoD 5015.2-STD "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007

ECM will be required to enable all DON users and mission partners to capture, manage, store, preserve, and deliver (share) the information they need, when they need it, in a form that is understood and can be acted upon, and is protected from those that should not have it. ECM includes functions normally associated with knowledge management, document management, correspondence management, records management, and workflow. NNE~2016 ECM tools and strategies will allow the management of unstructured information, wherever that information exists. The DON and its mission partners are comprised of many geographically dispersed commands that, to operate optimally, must often share content/information across their domains. Sharing enterprise content will facilitate better decision-making, increase situational awareness, increase the efficiency of task accomplishment, and improve mission effectiveness.

ECM includes, on a departmental level:

- Development of enterprise information security solutions
- Shared information through secure domains
- Statutorily compliant management of content that meets the criteria of being a Federal record
- "Push" and/or "pull" information sharing processes
- Low bandwidth replication for occasionally connected users
- Process notifications that pace, prompt, and apprise designated workflow participants through the workflow/document/information life-cycle
- Automated processes that create, maintain, and refresh critical information and knowledge
- Increased efficiency of task accomplishment to enable effective and agile mission support and decision-making
- Unified information and work flows into a single, secure organization-wide portal
- Flexible "push" and "pull" reporting for leadership
- Robust search and business intelligence capabilities
- User training and implementation support throughout the NNE~2016 domains

4.3.13 Privacy. NNE~2016 will protect all data , in both client and server environments, to protect/safeguard privacy and sensitive information. Protection must begin with system development and be carried through the entire system lifecycle.

This must be done to meet requirements as set forth in the Privacy Act of 1974 and to minimize the number and volume of compromised or potentially compromised Personally Identifiable Information (PII) data losses and thus decrease the likelihood of identity theft and other nefarious acts.

4.3.14 Data Strategy. NNE~2016 users will have the capability to discover, access, understand, and trust the information that they need to make decisions, increase adaptability of forces, improve situational awareness, and achieve greater precision in mission planning and execution.

In a net-centric environment, enterprise-level Authoritative Data Sources (ADS) must be visible, accessible, understandable, trusted, and interoperable, in compliance with Federal legislation, DoD, and DON policy and guidance. Under NNE~2016, DON, Navy, and Marine Corps personnel will have access to the authoritative information they need to accomplish their mission, at the right time, from the right sources, and in the right form. They will be able to exchange information between Services and agencies, and with all levels of US Government, international coalition partners, and the private sector, in support of national strategy on information sharing.

4.3.15 IT Services Management Framework NNE~2016 will implement an Information Technology Service Management (ITSM) framework to measure and report on all aspects of the NNE's "end-to-end" IT service delivery framework of people, processes, and products.

Information Technology is what drives the DON today. The fact is that the efficiency and effectiveness of the DON mission is critically dependent on the high availability, dependability, security, and performance of IT services. The ITSM framework is composed of a highly structured, tightly integrated and interdependent set of Service Support (e.g. Service Desk, Configuration, Release, Change, Incident, and Problem) and Service Delivery (e.g. Capacity, Availability, Service Continuity, Service Level, and Financial Management Processes), with the Service Catalog in the front office and a Configuration Management Database (CMDB) in the back office, each playing a vital role supporting each other and, most importantly, providing a service life-cycle sustaining check and balance on each other. To ensure the warranty of meeting and exceeding the statutory and regulatory requirements for information management, NNE~2016 will build and operate within an ITSM framework to bring about the consistency, reliability, and dependability of all IT process interfaces that lead to a federated CMDB – a metabase that links the Government with all Service Sources' Configuration Items, Documentation, and Change History.

The ITSM framework will support the development and implementation of effective and efficient processes, which are capable of adaptation to the ever changing IT environment, where business-driven metrics, critical success factors, quality of service, and key performance indicators are put in place to measure continuous service improvement and process maturity.

4.3.16 Applications and Portfolio Management. As part of NNE~2016, the Department will implement a mandatory Portfolio Management (PfM) process to deliver additional Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities (DOTMLPF) and operational capabilities to the Fleet and meet its net-centric goals.

Historically, typical IT systems and/or capabilities have been acquired and managed at local levels without regard for enterprise value or impact. This allowed duplicative investment in systems or platforms that deliver the same or similar capabilities, limiting the ability to share information or fully incorporate the DOTMLPF factors. Implementing a mandatory Portfolio Management process ensures that decision-makers compare competing investments objectively based on (1) their military, business and functional value; (2) that they are balanced in terms of a set of pre-established selection criteria that supports mission requirements, strategic direction, and compliance with Departmental policies and procedures; (3) and are effectively managed throughout the investment's life-cycle. This PfM process will apply to all Navy and Marine Corps systems and applications. The overall objective of a structured IT portfolio process is to deliver substantial benefits and operational capabilities to the DON warfighter, as well as, ensuring compliance with approved security policies and procedures, and standard architectures (i.e., business and technical).

4.3.17 Governance. NNE~2016 will adopt a formally structured governance organization and processes to provide the leadership, direction, and oversight required to ensure an integrated and effective approach to development and operation of the DON Information Technology Enterprise.

The DON IM/IT governance process will provide the logical structure for the direction, decision-making, execution and control of the funding, acquisition, and sustainment of the NNE~2016. A robust and effective governance process will ensure organizational and technological change can be effectively managed by leadership while ensuring compliance with law, regulation, and policy. Additionally, a well-

aligned and supported enterprise governance process will provide the flexibility to incorporate government and contract support roles and responsibilities based upon prescribed requirements and capabilities. Although the DON has several IM/IT governance processes in place to meet legal requirements, a federated approach that aligns the various domains that will be served by the NNE is currently not in place. To ensure a seamless transition from NMCI to NGEN and the NNE, it is imperative that the proper DON governance processes incorporating the best network, development, and management services and processes are engaged across the Enterprise. A federated NGEN governance organization and process, including stakeholders and decision makers from across the NNE, will ensure that requirements from lower commands and organizations are given visibility and deliberated under the umbrella of the overarching guidance covering all DON IM/IT investments. In this manner, the resultant end state will be best positioned to support accomplishment of the Department's warfighting and warfighting- support missions.

4.3.18 Performance Measurement. As the NNE will be a mix of contractor owned/contractor operated, government owned/contractor operated, and government owned/government operated networks and network services, the NNE~2016 Performance Measurement Strategy will be developed based on active monitoring and reporting of Service Level Agreements within the Information Technology Services Management framework.

Maintaining the end-to-end performance of NNE is critical to the success of the Department's warfighting and warfighting-support missions. The NNE~2016 operational commanders will actively monitor the Service Level Agreements (SLAs) developed for NGEN and develop complementary SLA measurement factors for networks that will monitor:

- Availability Management: to optimize infrastructure capability and its supporting organizations, ensure that promised services meet or exceed their availability targets, and measure configuration data related to each IT service.
- Release Management: provide a repeatable process for rolling out releases, implement high quality releases, implement releases efficiently and effectively.
- Incident Management: quickly resolve incidents, maintain IT service quality, improve IT and business productivity, maintain user satisfaction.
- Problem Management: minimize the impact of problems (reduce incident frequency/duration), improve quality of services being delivered, resolve problems and errors efficiently and effectively.
- Service Desk Management: resolve customer issues and problems at first call, maintain customer productivity, provide a positive customer call experience, provide effective support for customer calls.
- Service Level Management: deliver IT services as agreed to by customers and the business, manage the business/user interface, provide services at acceptable cost, manage quality of IT services in line with business requirements.
- IT Service Continuity Management: recover services from major disruptions within business timeframes, ensure all required services can be recovered from major disruptions, maintain viability of IT service continuity plans, provide service continuity at acceptable costs.
- Capacity Management: provide accurate capacity forecasts, provide services with appropriate capacity to match business need, protect services from capacity related incidents, demonstrate cost-effectiveness through accurate capacity planning.

4.4 Bottom Up Review

At the start of the development of NNE~2016 and the NGEN Requirements Combined Task Force efforts, the Center for Naval Analysis was contracted to interview a wide variety of Navy and Marine Corps users throughout the global Naval establishment. Many statements were collected from these interviews, after which they were analyzed, and compared with existing joint net-centric requirements documentation to form a basis of the 12 NGEN functions that coincidentally aligned, in general, with the focus areas previously discussed. The combination of these elements was used as the initial description of how NNE~2016 and NGEN should operate.

The distribution of statements across the NGEN key functions is shown below:

- Adaptability5
- System Interoperability
- Collaboration
- Information Access
- Security
- Information Exchange
- System Responsiveness
- Cross-Domain Security
- Information Service Visibility
- Workforce and Training
- Policy and Governance
- Information Service Management

The comments received were often applicable to one or more functions, highlighting the complexity and coordination required to operate in a net-centric environment. Other comments, however, were exclusive to one function. Common themes and trends of the interview results are highlighted:

- **Adaptability.** Of the adaptability function statements received during the interviews, several described a need for greater compliance with the GIG and DoD standards to facilitate interoperability during migration and integration of systems.

- **Collaboration.** The need to operate near real-time throughout the enterprise and be adaptable to various operating conditions. Collaboration tools would be at the desktop and would operate in conjunction with the Information Exchange function. Given today's globally connected millennium generation, online collaboration is the way of the future and is what many Sailors and Marines of the 21st century have grown up with. The Naval service must accommodate this way of life in its NNE~2016 plans. Additionally, current combat situations have shown the need for near real time open collaboration between the Navy and Marine Corps and our Joint, Coalition, federal and non-government organization partners.

- **Cross-Domain Security.** The need to support and comply with security requirements for each community of interest (COI) while also adhering to DoD architecture standards.

- **Information Access.** Comments relayed a need for remote access, the need to sometimes access blocked Internet Protocol (IP) addresses while also being attentive to the exchange of sensitive information. Again, given the millennium Sailors and Marines' environment, the Naval service

must accommodate wide access to public Internet based services, collaboration, and information sources.

- **Information Exchange.** Comments addressed the need for an ability to share data. Although comments were similar to those cited in the collaboration theme, they focused more on the interchange of the files between servers rather than desktop tools. (The main focus of information exchange is exchanging information across multiple language and cultural environments.)

- **Information Service Management.** There were general indications from many of the respondents that conformance with the ITSM standards was necessary. Also of concern is the availability and timely response of the help desk center to respond to and track users' needs.

- **Information Service Visibility**. Interview responses described a need for the reporting of network status and available services enterprise-wide. Visibility should include an ability to drill down to the user level.

- **Policy and Governance.** During the interviews, policy, process, and security were cited as inhibitors to the migration of and access to information. Comments discussed the need for a process for the approval, testing, and certification of hardware and software.

- **Security.** Interview results for the security function varied from the need to control access, to the identification of and recovery from threats to compliance with DoD security requirements.

- **System Interoperability.** Comments from these interviews described a need to support accessibility between security boundaries and user groups; policy, processes, and security requirements were cited as barriers to system interoperability.

- **System Responsiveness.** Comments indicated a need for Quality of Service, class of service, and prioritization. Interviews described possible factors affecting responsiveness (e.g., network capacity, file size).

- **Workforce and Training.** Comments focused on user training for new and existing tools and policies. Training should be tailored to support the roles and responsibilities of the end user.

The results of the bottom up reviews and the individual focus area are being aligned and combined, where appropriate, to hone the development of both select strategies for NNE~2016 and NGEN, as well as the functional needs of NGEN.

5.0 Effect on the Near Term (NGEN)

As previously mentioned, concurrent with the development of the long-term vision for NNE~2016, the Department is also faced with the near-term challenge of beginning to lay the groundwork for the replacement of the NMCI contract. In transitioning from the Department's existing IT user capabilities, the initial block of the follow-on to NMCI must be in place in time to ensure the continuity of the Department's basic shore-based IT services after the NMCI contract ends in September 2010.

NMCI was a revolutionary approach for obtaining voice, video, and data communications and computing capabilities within DoD, acquiring IT capabilities via a fixed price, multi-year, performance-based services contract. While many of the NMCI objectives were achieved, since 9/11 the Department's priorities have shifted and several key lessons-learned and upgrade plans will be factored into the NGEN, as follows:

- Expanded use of DoD infrastructure and increased use/control of network management tools
- Improved security and certification requirements that balance the need to protect assets with the users' need for access to achieve the mission
- Operators and users need:
    - An adaptable infrastructure and underlying architecture that can be changed to meet operational necessity without intrusive administrative procedures, delays, and penalties
    - More responsive contractual terms and conditions
    - Improved interoperability, collaboration, and service mobility
- Users want:
    - Predictable technical refresh
    - Rapid deployment of network services
    - The ability to accommodate unplanned, rapid reconfiguration or experimentation to address the coalition or Joint warfighting requirements that develop within the Fleet forces
    - A more intuitive knowledge management and information sharing capability
    - Rapid upgrade paths to state-of-the-shelf technologies or software that would enhance mission accomplishment
    - Single sign-on authentication
    - Broader use of secure wireless capability
    - Integration of voice over IP

As currently envisioned, NGEN must minimize the transition risk to the Department's user community. It will incorporate the NMCI lessons learned and customer identified needs, address performance deficiencies, and focus on improved reliability and security. NGEN will provide services to the full range of Navy and Marine Corps end points that include data, voice, and video users, a mix of end-user accounts and interfaces to other DON and DoD communications environments. In addition, NGEN will provide support to non-DON end points that are identified as users of those services under the current data, voice, and/or video networks/systems. Additional capabilities will be added in future block upgrades.

6. References

1. DoD Net-Centric Environment Joint Functional Concept of 4/7/05
2. GIG Capstone Requirements Document (GIG CRD)
3. GIG ES Initial Capability Document (GIG ES ICD)
4. DoD Joint Operations Concepts (JOpsC)
5. NCES CONOPS of 3/1/05
6. Naval Concept of Operations 2006
7. Draft CANES CDD, v1.4
8. Draft CANES Implementation Plan
9. ISNS CPD of 4/17/07
10. MHQ w MOC CONOPS Approval brief of 12/13/06
11. BLII/ONE-NET backgrounder of 5/16/06
12. ONE-NET ESM Update v2 of 4/27/07
13. PEO EIS ONE-NET brief of 4/5/06
14. USMC C4 Campaign Plan of 5/3/04
15. USMC ICS Executive Overview
16. USMC ICS v0.5
17. ICS Enterprise IT CONOPS (Appendix A to ICS)
18. ICS Network Strategies (Appendix B to ICS)

7. Glossary

Item	Definition
AAUSN	Administrative Assistant to the Under Secretary of the Navy
ACAT	Acquisition Category
ACMC	Assistant Commandant of the Marine Corps
ADNS	Automated Digital Network System
ASD NII	Assistant Secretary of Defense for Network Infrastructure and Information
ATO	Authority to Operate
BAN	Base Area Network
BLII	Base Level Information Infrastructure
BTA	Business Transformation Agency
C2	Command And Control
C4	Command, Control, Communications, and Computers
CA	Command Authority
CANES	Consolidated Afloat Networks and Enterprise Services
CARS	Cyber Asset Reduction and Security
CCA	Clinger-Cohen Act
CENTRIXS	Combined Enterprise Regional Information Exchange System Maritime
CIO	Chief Information Officer
CMDB	Configuration Management Database
CND	Computer Network Defense
CNO	Chief of Naval Operations
COCOM	Combatant Commander
COI	Community of Interest
CONOPS	Concept Of Operations
CONUS	Continental United States
COOP	Continuity Of Operations
COP	Common Operating Picture
COTS	Commercial Off The Shelf
CND	Computer Network Defense
CRM	Customer Resource Management
DAA	Designated Approval Authority
DCTS	Defense Collaboration Tool Suite
D/DCIO(N)	Deputy DONCIO (Navy)
DII COE	Defense Information Infrastructure Common Operating Environment
Dir C4	USMC HQ Director, C4
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DKO	Defense Knowledge Online

Item	Definition
DoD	Department Of Defense
DoD CIO	Department Of Defense Chief Information Officer
DON	Department Of Navy
DON CIO	Department Of Navy Chief Information Officer
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership,
EA	Enterprise Architecture
ECM	Enterprise Content Management
EDS	Electronic Data Systems
ERP	Enterprise Resource Planning
ESDE	Enterprise Shared Data Environment
ESI	Enterprise Software Initiative
FAA	Functional Area Analysis
FAM	Functional Area Manager
FMB	Financial Management and Budget
FNA	Functional Needs Analysis
FSA	Functional Solutions Analysis
GCCS-M	Global Command and Control System – Maritime
GCSS	Global Combat Support System
GCMP	GIG Convergence Master Plan
GES	Gig Enterprise Services
GIG	Global Information Grid
GIG-BE	Global Information Grid – Bandwidth Expansion
HQMC C4	Headquarters Marine Corps
IA	Information Assurance
IEC	Information Executive Committee
IM	Instant Messaging
IM/IT	Information Management / Information Technology
IO	Information Operations
ISNS	Integrated Shipboard Network System
IT-21	Information Technology for the 21st Century
ITAM	Information Technology Asset Management
ITIL	Information Technology Infrastructure Library
JFMCC	Joint Force Maritime Combatant Commander
JTF-GNO	Joint Task Force Global Network Operations
KM	Knowledge Management
LAN	Local Area Network
LNC	Legacy Network Consolidation
LMS	Learning Management System
M2M	Machine to machine
MAGTF	Marine Air-Ground Task Force
MCEITS	Marine Corps Enterprise Information Technology Services

Item	Definition
MCNOSC	Marine Corps Network Operations Support Center
MCEN	Marine Corps Enterprise Network
MDA	Maritime Domain Awareness
MEB	Marine Expeditionary Brigades
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
MHQ	Maritime Headquarters
MOC	Maritime Operations Center
NCES	Net-Centric Enterprise Services
NCOE	Network Centric Operations Environment
NCOW	Network Centric Operations And Warfare
NCW	Network Centric Warfare
NETOPS	Network Operations
NETWARCOM	Network Warfare Command
NGEN	Next Generation Enterprise Network
NIPRNet	Non Classified Internet Protocol Router Network
NKO	Navy Knowledge Online
NMCI	Navy Marine Corps Intranet
NMCP	Navy Marine Corps Portal
NNE	Naval Networking Environment
NNWC	Navy Network Warfare Command
OA	Open Architecture
OCONUS	Outside of the Continental United States
ONE-NET	OCONUS Navy Enterprise Network
OSD	Office Of The Secretary Of Defense
P&G	Policy & Governance
PACFLT	Pacific Fleet
PEO C4I	Program Executive Office Command, Control, Communications,
PEO EIS	Program Executive Office Enterprise Information Systems
PfM	Portfolio Management
PII	Personal Identifiable Information
PM NMCI	Program Manager Navy Marine Corps Intranet
POP	Point of Presence
RFP	Request for Proposals
RNOSC	Regional Network Operations Security Center
SA	Situational Awareness
SECNAV	Secretary Of The Navy
SHF	Super High Frequency
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SOA	Service Oriented Architecture

Item	Definition
SoS	System of Systems
SPAWAR	Space and Warfare Systems Command
UDOP	User Defined Operational Picture
UHF	Ultra High Frequency
USN	United States Navy
USSTRATCOM	United States Strategic Command
VHF	Very High Frequency
WAN	Wide Area Network
XML	Extensible Markup Language