

COMMANDER

NAVAL NETWORK AND SPACE OPERATIONS COMMAND



CONCEPT OF OPERATIONS PLAN (CONOPS)

FOR

NAVY MARINE CORPS INTRANET

(NMCI)

November 2003

Document Approval

Approved By:

Rear Admiral J. Cryer

Date

23 Dec 03

Table of Contents

Executive Summary.....	Page
1.0 Mission and Purpose.....	Page 1
1.1 Overview.....	Page 1
1.2 NNSOC Mission.....	Page 1
1.3 OPS Plan Purpose.....	Page 1
1.4 Assumptions.....	Page 1
2.0 Roles and Relationships.....	Page 2
2.1 Introduction.....	Page 2
2.2 Operational Authority and Responsibilities.....	Page 3
2.2.1 Directive Authority.....	Page 3
2.3 Responsibilities.....	Page 3
2.3.1 Chief of Naval Operations.....	Page 3
2.3.2 Marine Corps Network Operations and Security Command..... (MCNOSC)	Page 4
2.3.3 Unified Combatant Commander, Fleet Commands and Major..... Claimants	Page 4
2.3.4 Director NMCI.....	Page 4
2.3.5 Commander, Naval Network Warfare Command (NNWC).....	Page 4
2.3.6 Space and Naval Warfare Systems Command (SPAWAR).....	Page 4
2.3.7 Naval Component Incident Response Team (NAVCIRT..... (NCTF-CND))	Page 5
2.3.8 Fleet Information Warfare Center (FIWC) Red Team.....	Page 5
2.3.9 Program Management Officer (PMO).....	Page 6
2.3.10 Integrated Support Center (ISC).....	Page 6
2.3.11 Commander Naval Network and Space Operations Command..... (CNNSOC) NMCI Operations Organization	Page 7
2.3.12 Green Team.....	Page 8
2.3.13 Operations Enterprise Action Group (OPS EAG).....	Page 8
2.3.14 Global Network Operations Center (GNOC) Detachment.....	Page 8
2.3.15 EDS GNOC.....	Page 11
2.3.16 NNSOC GNOC – EDS GNOC Coordination.....	Page 12
2.3.17 NNSOC GNOC – ISC Coordination.....	Page 13
3.0 NMCI Operational Guidance.....	Page 14
3.1 Background.....	Page 14
3.2 Purpose.....	Page 14
3.3 Governance Bodies.....	Page 14
3.3.1 Operations Advisory Board.....	Page 14
3.3.2 Stakeholder Council (SHC).....	Page 15
3.3.3 Enterprise Action Groups.....	Page 15
3.3.4 Programmatic Enterprise Action Group (PEAG).....	Page 16
3.3.6 Operations Enterprise Action Group (OPS EAG).....	Page 16

3.4 Organizations and Administrative Support.....	Page 16
3.5 NMCI Governance Issue Resolution Process.....	Page 17
4.0 Network Operations.....	Page 19
4.1 Introduction.....	Page 19
4.2 Reports.....	Page 19
4.2.1 EDS Provided Reports.....	Page 19
4.2.2 NNSOC Provided Reports.....	Page 20
4.2.3 Reporting of Essential Services.....	Page 20
4.2.4 Additional Reporting Requirements.....	Page 20
4.3 Service Restoration Policy.....	Page 22
4.4 SOPs and PPRs.....	Page 23
4.5 INFOCON Procedures.....	Page 23
4.5.1 Background.....	Page 23
4.5.2 INFOCON MOA.....	Page 23
4.6 Network Attacks and Information Assurance Incidents.....	Page 24
4.6.1 Coordinating Responsibilities.....	Page 24
4.6.2 Global Information System Security Administrator (GLISSM).....	Page 24
4.6.3 Pre-Planned Responses (PPRs).....	Page 24
4.7 NIA – NIB.....	Page 25
5.0 Operational Interfaces.....	Page 26
5.1 Scheduled Maintenance and Notification Procedures.....	Page 26
5.2 Securing Unclassified Desktop Computers.....	Page 27
6.0 NMCI Operational Communication plans.....	Page 28
6.1 NNSOC Communication.....	Page 28
6.2 EDS Communication.....	Page 28
6.3 Printed Collateral.....	Page 29
7.0 Cutover and Operational Readiness Review (Under Development).....	Page 31

Appendices

Appendix A – SOP and PPR Listing..... Page 32
Appendix B – Network Restoration Priorities..... Page 34
Appendix C – EDS Generated Reports.....Page 36

List of Figures

Figure 1 – Operational Direction and Status..... Page 2
Figure 2 – NMCI Organization Chart..... Page 9
Figure 3 – EDS Organization Chart..... Page 12
Figure 4 – NMCI Governance Structure Page 16
Figure 5 – NMCI Governance Issue Resolution ProcessPage 18

Commander
Naval Network and Space Operations Command
Navy and Marine Corps (NMCI)
Concept of Operations Plan

Reference:

- (a) INFOCON Memorandum of Agreement (MOA)
- (b) NAVNETWARCOMINST 5239 CNNWCINST 5239.1 dated 25 October 2002
- (c) Department of Defense instruction 8500.2, dtd. 06FEB2003
- (d) CJCS 05Apr1999 THE DON CIO ((VERSION 99-1, 5 APRIL 1999 153)) Information Technology Standards Guidance (ITSG) initiative version
- (e) CJCSM 6510.01, DoN CIO 25 Mar 2003 Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND) Manual
- (f) IA Pub 5239-October 2003
- (g) COMNAVNETWARCOM Memorandum 3100, dated Mar 2003 (Revised NMCI governance structure).
- (h) NWP 6-01, Basic Operational Communications Doctrine page 2-2 paragraph 2.4.1
- (i) OPNAVINST 2201.2 Navy and Marine Corps Computer Network Incident Response
- (j) OPNAVINST 5239.1 Navy Information Assurance Program
- (k) DoD Directive 8530.1 Computer Network Defense
- (l) DoDI 8520 CND Service Providers
- (m) NMCI CONOPS dtd 13 May 2002
- (n) NMCI Operations Enterprise Action Group Charter
- (o) ISC CONOPS (in draft)

Cancellation: This cancels the NMCI CONOPS signed 13 May 2002.

Executive Summary

The Navy-Marine Corps Intranet (NMCI) is a service contract that employs Service Level Agreements to meet Naval Information Technology (IT) service requirements. NMCI Network Operations is the responsibility of the NMCI contract team, referred to as the Electronic Data Systems (EDS). The Naval Network and Space Operations Command (NNSOC) is the Navy single point of contact to provide operational direction to the NMCI contractor for network operations and to evaluate requirements and coordinate all decisions involving service priorities, restoration priorities and other enterprise-wide operational issues. NNSOC was formed in July 2002 by the merger of elements of Naval Space Command (NSC) and Naval Network Operations Command (NNOC). The Command operates and maintains the Navy's space and global telecommunications systems and services, directly supports war fighting operations and command and control of naval forces, and promotes innovative technological solutions to war fighting requirements.

Operational direction as it applies to NMCI includes four basic functions:

- Setting NMCI service priorities
- Prioritizing network and service restorations
- Re-configuring the network to support emerging Unified and Fleet Combatant Commander (CC) requirements
- Implementing network defense measures

NNSOC, in coordination with the Marine Corps Network Operations and Security Command (MCNOSC), is responsible for the day-to-day operation of the Department of the Navy (DoN) IT networks. NNSOC and MCNOSC will oversee overall performance of these networks to ensure availability, reliability and security of critical information. MCNOSC is the central point of contact for the USMC. NNSOC and MCNOSC are responsible for implementing and monitoring network priorities and policies as directed by the NMCI governance organization.

COMNAVNETWARCOM (CNNWC) is the Designated Approving Authority (DAA) for the Navy portion of NMCI and approves Certification and Accreditation (C&A) of the network to operate at an acceptable level of security risk in close cooperation with the Major Claimants/Activity DAAs. The Major Claimants/Activity DAAs retain responsibility for all other systems. The DAA for the USMC portion of the network is the Director of the C4 Department, Headquarters, U.S. Marine Corps.

This Network Operations Plan will require periodic review. During the course of real world operations and experiences, it is expected that improvements will be identified, which will need to be captured and applied within this document. These changes will be transmitted to all NMCI users via record message in the form of NMCI Information Bulletins (NIB) and NMCI Information Advisories (NIA). Updates to this instruction will incorporate all applicable outstanding NIB's and NIA's.

1.0 Mission and Purpose

1.1 Overview

This chapter discusses NNSOC's mission and the purpose of the NMCI OPS PLAN.

1.2 NNSOC Mission

“Operate and maintain the Navy's space and global telecommunications, information and space systems and services to directly support operations, training and education, and to promote innovative solutions to the warfighter”. NNSOC enables naval forces to use information and space technologies and expertise to achieve and maintain knowledge superiority essential for dominating the battle space.

1.3 NMCI OPS PLAN Purpose

The purpose is to promulgate the procedures and processes that detail the operational direction and support responsibilities of NNSOC and to establish the framework of cooperation and understanding of the overarching enterprise with regards to implementing NMCI.

1.4 Assumptions

- The USMC will retain control of the Marine Corps Enterprise Network (MCEN). The MCEN is comprised in totality of the USMC NMCI Community of Interest (COI) and the USMC Non-NMCI Legacy COI. The MCNOSC will provide operational direction for global information technology systems and services for the Marine Corps MCEN.
- DAA responsibilities for the MCEN NMCI COI will be coordinated using a Memorandum of Agreement (MOA) between NAVNETWARCOM and HQMC C4.
- This document will discuss Navy specific roles and responsibilities pertaining to NMCI.

2.0 Roles and Relationships

2.1 Introduction

Operational direction of NMCI will be based on Department of Defense (DoD) and DoN policies, directives, guidance and requirements provided by the Unified and Fleet CCs. The NMCI supports Network Operations enabling dynamic execution of warfare operations and naval processes (tactical and non-tactical applications -- e.g. automate maintenance activities, training, personnel and administration). The current Fleet and Unified CC component relationships are illustrated in Figure 1.

NMCI Operational Relationships

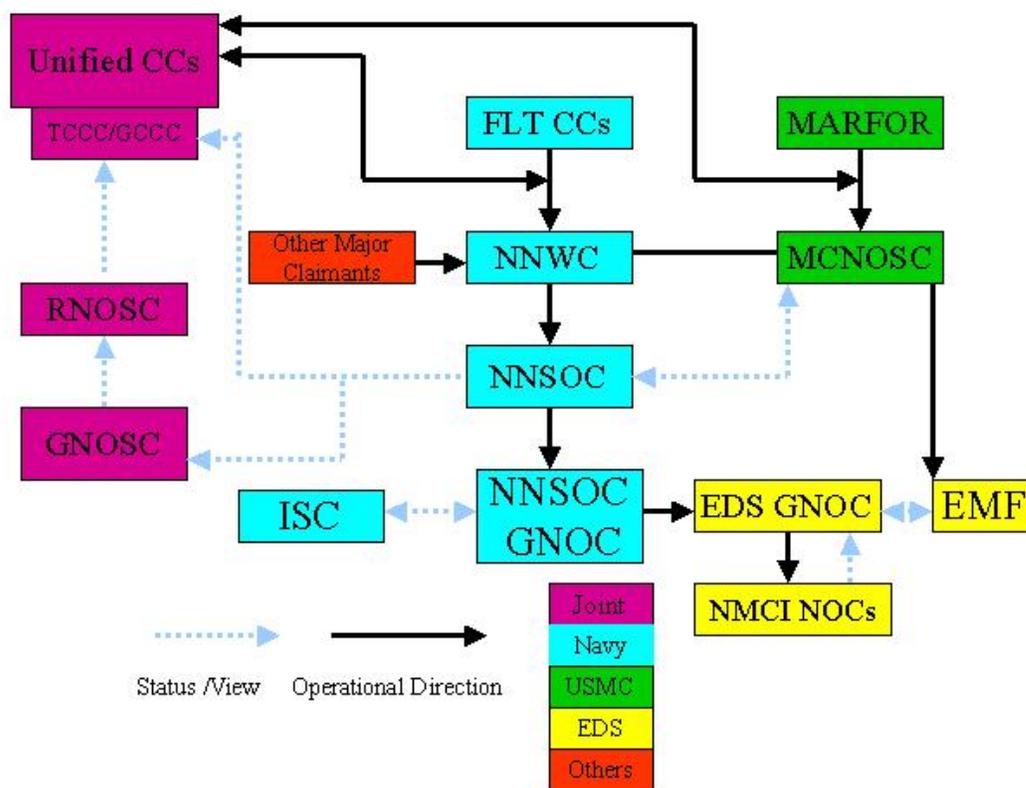


Figure 1 - Operational Direction and Status

NNSOC's Global Network Operations Center (GNOC) Detachment supports NNSOC's operational mission as stated in paragraph 1.2 by monitoring network performance, security and

policy implementation. The NMCI GNOC detachment will work through the vendor's (EDS's) GNOC using tools sanctioned by the Government and provided by the contractor.

NNSOC and MCNOSC currently coordinate with each other on IT matters pertaining to their respective services. The current Marine Corps Enterprise Network (MCEN) remains under the complete control of the MCNOSC. At such time that the USMC NMCI COI is established within the NMCI enclave, NNSOC and the MCNOSC will coordinate closely on NMCI day-to-day operations, policy implementation and network security.

Defense Information System Agency (DISA) operates through the Global Network Operations and Security Center (GNOSC). DISA manages the provisioning, implementation, and operational control of long-haul communications networks, circuits, services, and equipment. Specific responsibilities to NMCI have been delineated in the 17 August 2000 Memorandum of Agreement (MOA) with ASD (C3I), DoD CIO and DoN. The source document that defines the roles and responsibilities for provisioning long-haul telecommunications services that support NMCI is the NMCI Wide Area Network Provisioning Process Document. More specifically, a separate MOA exists among DISA, SPAWAR PMO, and NMCI EDS detailing interim management procedures in support of NMCI (information on control of DISN is found in NWP 6-01, Basic Operational Communications Doctrine pg 1-2 para 1.4).

2.2 Operational Authority and Responsibilities

2.2.1 Directive Authority

NNSOC will remain completely responsive to all requirements generated from Unified and Fleet Combatant Commanders (CCs) and Major Claimants. NNSOC will provide operational direction to the Navy portion of NMCI in accordance with an operational direction Memorandum of Agreement (MOA) signed by United States Pacific Command (USPACOM), United States Joint Forces Command (USJFCOM), Commander Pacific Fleet (CPF) and Commander United States Fleet Forces Command (FFC). The MOA will detail the processes necessary to gain consensus for a single course of action for the NMCI enterprise. NNSOC will then direct EDS as appropriate to carry out the Combatant Commanders' requirements. NNSOC will coordinate as necessary with MCNOSC.

2.3 Responsibilities

2.3.1 Chief of Naval Operations

The role of the CNO is defined in reference (h).

2.3.2 MCNOSC

The NNSOC and the MCNOSC will provide mutual support on NMCI operations, security, and policy implementation. Specific coordination instructions will be codified in a Memorandum of Agreement to be developed.

2.3.3 Unified CCs, Fleet CCs and Major Claimants

Unified and Fleet CCs and Major Claimants provide operational requirements to NNSOC via NETWARCOM. Unified and Fleet CCs coordinate among themselves and approve operational direction actions. NNSOC ensures EDS operates NMCI to meet these requirements. All actions taken will be coordinated with Unified and Fleet CCs, Major Claimants and NETWARCOM and the Director NMCI as appropriate.

2.3.4 Director NMCI

The Director, NMCI in the Assistant Secretary of the Navy's (Research, Development and Acquisition) (ASN RD&A), organization is the centralized point of authority and accountability for NMCI contract performance and execution to include conducting operational test and evaluation. The ASN RD&A, the Program Executive Office for Information Technology (PEO-IT) and the Director, NMCI will manage the acquisition. Director, NMCI is vested with the authority, accountability and resources necessary to manage the NMCI program plans and budgets for the development, production, Fleet introduction and life cycle support of assigned systems, equipment, and other infrastructure for NMCI.

2.3.5 Commander, Naval Network Warfare Command

Acts as the Navy's central operational authority for space, information technology requirements, network and information operations in support of naval forces afloat and ashore; to operate a secure and interoperable naval network that will enable effects-based operations and innovation; to coordinate and assess the Navy operational requirements for and use of network/command and control/information technology/information operations and space; to serve as the operational forces' advocate in the development and fielding of information technology, information operations and space and to perform such other functions and tasks as may be directed by higher authority.

NETWARCOM is the Designated Approval Authority (DAA) for the Navy portion of NMCI.

2.3.6 Space and Naval Warfare Systems Command (SPAWAR)

SPAWAR will do purchasing for commands and the testing and evaluation of the implementation for the Navy, and Marine Corps Systems Command will do the same for the Marine Corps. SPAWAR, as the certification authority, will support NETWARCOM in the network security certification and accreditation process. The contractor (EDS) develops the NMCI security architecture and submits an initial input/draft of the System Security Authorization Agreement (SSAA) to SPAWAR. If the draft SSAA is approved, SPAWAR develops the Security Test and Evaluation (ST&E) plan and coordinates the plan with the Red and Green Teams. SPAWAR, in concert with the Director, NMCI, makes an accreditation recommendation to the operational DAA, who makes the decision to grant final accreditation. SPAWAR is assigned additional duties to NETWARCOM to provide technical support to NNSOC on Navy systems and equipment that is NMCI related.

2.3.7 Naval Component Incident Response Team (NAVCIRT)

As of 16 Jun 03, The Naval Computer Incident Response Team (NAVCIRT) and Navy Component Task Force - Computer Network Defense (NCTF-CND) merged operations.

NAVCIRT, operated by the Navy Component Task Force, provides computer security incident support to DoIN activities. As designated by ref (i), NAVCIRT serves as the DON focal point for the DoD exchange on computer vulnerabilities, viruses, and "hacker" incidents. NAVCIRT is also a member of the Forum of Incident Response and Security Teams (FIRST), which is comprised of international government agencies and commercial firms. NAVCIRT has assumed all NCTF-CND responsibilities, and is responsible for the coordination and direction of the defense of Navy computer systems and networks. In accordance with refs (j), (k) and (e), Computer Network Defense (CND) is defined as actions taken pursuant to legal authority to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks. Consistent with guidance set forth in ref (l), NAVCIRT will provide a CND Service (CNDS) for all information systems and computer in order to maintain CND situational awareness; implement CND protection measures; monitor and analyze in order to detect unauthorized activity; and implement CND operational direction. For additional responsibilities see ref (m).

NAVCIRT and Marine Forces Integrated Network Operations (MARFOR-INO), in concert with NNSOC, will perform security oversight of the enterprise wide network.

2.3.8 Fleet Information Warfare Center (FIWC) Red Team

- The FIWC Red Team is a team of IT professionals designed to raise Navy computer and network awareness and provide training.
- The Red Team focuses on NIPRNET, SIPRNET, and JWICS systems. Prior to Red Team operations, the officer conducting the exercise may place specific networks and systems off-limits.
- Operations include mapping, probing, intrusion, and placing marker files.
- FIWC will implement a Red Team operation to conduct the following activities for NMCI:
 - Monitor security related Service Level Agreement (SLA) compliance, monitor Information Assurance Vulnerability Alert, (IAVA), Bulletin and Technical Advisory compliance and verify the effectiveness of software patches.
 - Electronically probe for undiscovered network vulnerabilities, randomly or as directed.
 - Monitor the Secret Internet Protocol Network (SIPRNET) and Non-classified Internet Protocol Network (NIPRNET) gateways at all NMCI Network Operation Centers. This activity will be an integral component of the NMCI security architecture and operations.
- Red Teams will not:

- Damage, delete, or alter data files
- Shut down computer or network systems
- Tamper with system parameters
- Copy data
- Violate personal privacy

2.3.9 Program Management Office

Program management for NMCI is the responsibility of the Navy and Marine Corps Program Management Offices (PMO). SPAWAR PMW-164 staffs the Navy PMO. The PMO directly supports the NMCI Director's Office by managing overall transition and steady state efforts. This includes collection and execution of Claimant and Command requirements, facilitation of legacy system transition, assessments of technology, and implementation of DoN and DoD plans and policies as well as the following specific responsibilities:

- Verify execution of annual NMCI requirements plan
- Oversee contract execution
- Implement DoN and DoD plans and policies
- Collaborate with NETWARCOM to develop and implement policies and best business practices
- Coordinate transition and implementation efforts
- Facilitate transition of legacy systems
- Conduct technology assessments
- Manage Government Furnished Equipment (GFE)
- Coordinate Government Furnished Facilities (GFF)
- Provide engineering, technical, and financial assistance
- Conduct business process management
- Provide customer liaison

The PMO structure provides maximum NMCI customer support through a matrix concept that covers technical and T&E requirements, information assurance (IA), legacy applications (LA), business and financial management support, programatics, contract management, site deployment coordination, and customer advocacy.

2.3.10 SPAWAR Integrated Support Center (ISC)

The ISC provides a central, single-point-of-contact support during system transition, and steady-state operation of NMCI. This approach will deliver a consistent customer experience, resolve conflicts, and deliver targeted solutions.

The ISC has no operational authority. Ultimate operational authority resides with CNNSOC. The ISC will, however, retain administrative authority to address program issues and to refer Governance or Operational issues to the appropriate organization for resolution. Additionally, the ISC maintains the chain of command for site management through regional coordinators and facilitates day-to-day business through its rapid response team.

2.3.10.1 Integrated Support Center will:

- Resolve/elevate program issues at the Enterprise level.
- Centralize support for completion of NMCI transition and sustained life-cycle operations
- Maintain disciplined procedures - week-day “watch standing”
- Act as central point for incoming/outgoing NMCI communications
- Track issues immediately (real-time) into synergistic resolution process
- Administrative authority to address program and refer governance/operational issues

Watch Standers are to be knowledgeable in the areas of expertise assigned and to be able to respond to questions in these areas or to refer the questioner to the appropriate individual who can answer their question.

2.3.11 NNSOC NMCI Operations Organization

NNSOC N3 Department is the focal point for decisions involving network service priorities, restoration priorities, and any other enterprise-wide operational issues. Specific functions include:

- Work with Director NMCI, Navy PMO, and NMCI prime contractor (EDS) to identify and resolve day-to-day problems affecting the operation of the network.
- Be aware of emerging operational requirements.
- Direct NMCI prime contractor (EDS) implementation of required information assurance actions as directed by higher authority.
- Work with Director NMCI, Navy PMO, and NMCI prime contractor (EDS), to resolve intranet OPTEMPO changes necessary because of operational, exercise, and/or test requirements.
- Provide global network visibility to DoD agencies (DISA GNOSC).
- Act as Navy Point of Contact (POC) for all DoD inquiries about NMCI operational status.
- Act as the Navy POC for the MCNOSC for all operational issues.
- Participate in annual review of NMCI requirements, to include service changes, new technology insertions, and required contract modifications.
- Ensure the EDS is informed of and responding to increased levels of service required in response to or in anticipation of changes in Navy OPTEMPO.
- Provide NMCI information assurance vulnerabilities (IAV) Alerts, Bulletins, and Technical Advisories compliance in the daily status report and through Online Compliance Reporting System (OCRS).
- Identify and notify the Fleet of significant network service interruptions and restorations affecting NMCI services via the OPREP reporting system, Fleet advisories, and the NNSOC C4 status page, as appropriate.
- Advise and coordinate with NETWARCOM on appropriate measures and options for security certification and accreditation of the network.
- Represent the interests of Major Claimants in enterprise issues and liaison between the Navy, NMCI Navy PMO, and the NMCI prime contractor for operational issues that cannot be resolved at command or claimant levels.

- Coordinate with Unified and Fleet Commanders to determine operational priorities.
- Operate NMCI network in compliance with DoD, Unified Commanders, and DoN policies as they apply to operational direction of NMCI.

2.3.12 Green Team

The SPAWAR PMW 161 Green Team will focus on monitoring EDS compliance to Service Level Agreements (SLA) and interface with the local commands to check security policy compliance at the tenant command and base level. The majority of Green Team internal assessments will be completed on site. The Green Team assessment tools are to be non-invasive and use administrative permissions. All Green Team assessment activities will be conducted under the cognizance of the local commander.

2.3.13 Operations Enterprise Action Group (OPS EAG)

As indicated in ref (m), NNSOC co-chairs the Operations EAG with the MCNOSC. The Stake Holders Council (SHC) established the Operations EAG in May 2001 with the vision that it would remain in place for the life of the NMCI contract. The OPS EAG core team is composed of representatives from NNSOC, MCNOSC, EDS, FFC, COMPACFLT, USPACOM and USJFCOM. Their collective goal is to develop and implement procedures and processes for enterprise oversight of NMCI network operations.

2.3.14 GNOC DET Organization - Government Oversight of NMCI

The Government has established a presence at the Contractor's Global Network Operations Center (GNOC) in order to monitor overall NMCI operations and to exercise operational direction to include setting of priorities for contracted services, setting priorities for resolution of problems/deficiencies, and to direct changes in network security posture over critical segments of the NMCI infrastructure, in support of DoN statutory and war-fighting responsibilities.

The NMCI EDS GNOC is the enterprise organization responsible for direct liaison with the NNSOC's GNOC Detachment (DET) who is the government's on-site representative. The GNOC DET provides day-to-day operational oversight, performs liaison and coordination, and receives reports from the EDS on network health, outages, security events and general incidents concerning the enterprise network. The NMCI organizational chart is illustrated in Figure 2.

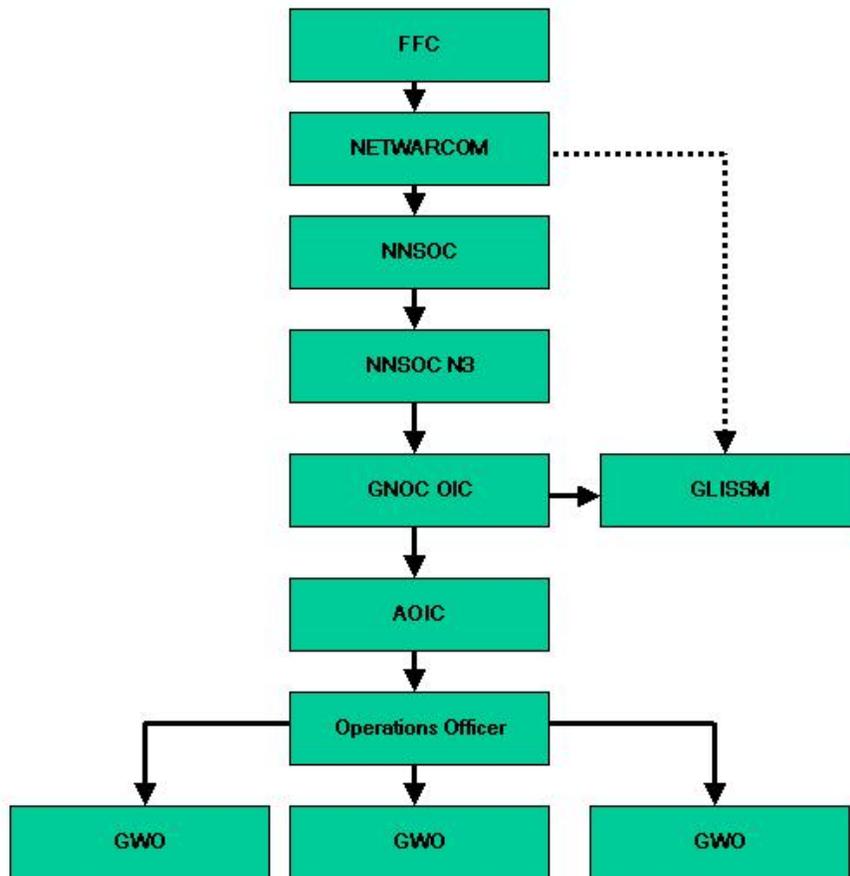


Figure 2 - NMCI Organization Chart

GNOC OIC Responsibilities

- Primary operational liaison between GNOC/NNSOC and NMCI on operational and security issues that affect operations.

GNOC A-OIC Responsibilities

- Serves as Officer in Charge in the OIC's absence.

GNOC DET Operations Officer

- Responsible for analyzing, reporting and recording all real-time conditions that affect network health.
- Coordinate with the Fleet and Unified Combatant Commanders to expedite operational impact assessment on war-fighting commands.

- Ensures EDS is informed of restoration priorities for services based upon operational tempo and fleet requirements.
- Identifies and notifies N36 of network service interruptions and restorations affecting NMCI services as addressed in a MOA.
- Initiates actions as required in GNOC SOPs/PPRs, MOAs during major outage or crisis. Responsible for keeping CNNSOC informed of any such instances. POC for the GNOC during time of crisis. Coordinates outage notifications during critical mission outages.

Global Information Systems Security Manager (GLISSM)

- Carries out duties as described in COMNAVNETWARCOMINST 5239.1 (Reference b)
- Responsible for directing changes in network security posture based upon DoN, DoD and NNSOC and NETWARCOM policies and guidance as detailed in MOAs and MOUs.
- Responsible for monitoring compliance of all required security reporting through regularly recurring reports, direct liaison and the Online Compliance Reporting System. Serves as quality assurance for the compliance and proper reporting for all regional NOCs.
- Ensures Commander, NAVNETWARCOM and NNSOC network security officers are kept apprised of all significant information relating to NMCI.
- Tracks and reports proper responses by NMCI to virus incidents, intrusion attempts and other vulnerabilities to network security.

GNOC Command Duty Officer Responsibilities:

- Responsible to the GNOC Director for daily operations of the GNOC during his/her watch and for ensuring all CNNSOC/GNOC policies and procedures are implemented in accordance with specific guidance provided from the GNOC Director.
- Primary point of contact between Navy, Major Claimants and contractor.
- Provides timely updates and status reports to the OIC, AOIC, Operations Officer or ISSM of on-going events.
- Primary point of contact for GNOC Watch Officer (GNOCWO) after normal working hours.
- Liaison for major circuit outages.

GNOC Watch Officer (GNOCWO) responsibilities:

- Is a qualified Petty Officer, having completed JQR for the GNOCWO
- Responsible to the CDO for daily operations of the GNOC during his/her watch and for ensuring all NNSOC/GNOC policies and procedures are implemented in accordance with specific guidance provided from the GNOC Director.
- Coordinates with EDS to monitor and report NMCI network health and security posture using real-time and near-real-time methods.
- Performs duty as the CNNSOC Point-of-contact for all issues that may require special attention after normal duty hours. Responsible for notifying the GNOC CDO of any such issues, to include emergency personnel, operations, or facilities related issues.
- Coordinates with Regional NOC reporting stations in monitoring the global unclassified and classified networks and systems by use of real-time and near-real-time methods.
- Directs EDS to set Information Operations Conditions (INFOCON) for NMCI as detailed in the INFOCON MOA.
- Directs INFOCON exercises for the watch team when necessary.

Watch Stander Responsibilities:

- Responsible to the GNOCWO for daily operations during his/her watch and for ensuring all CNNOC/GNOC policies and procedures are implemented in accordance with specific guidance provided from the GNOC Director.

2.3.15 EDS GNOC Organization

The EDS GNOC is co-located with GNOC DET Norfolk. EDS Organization chart is displayed in Figure 3.

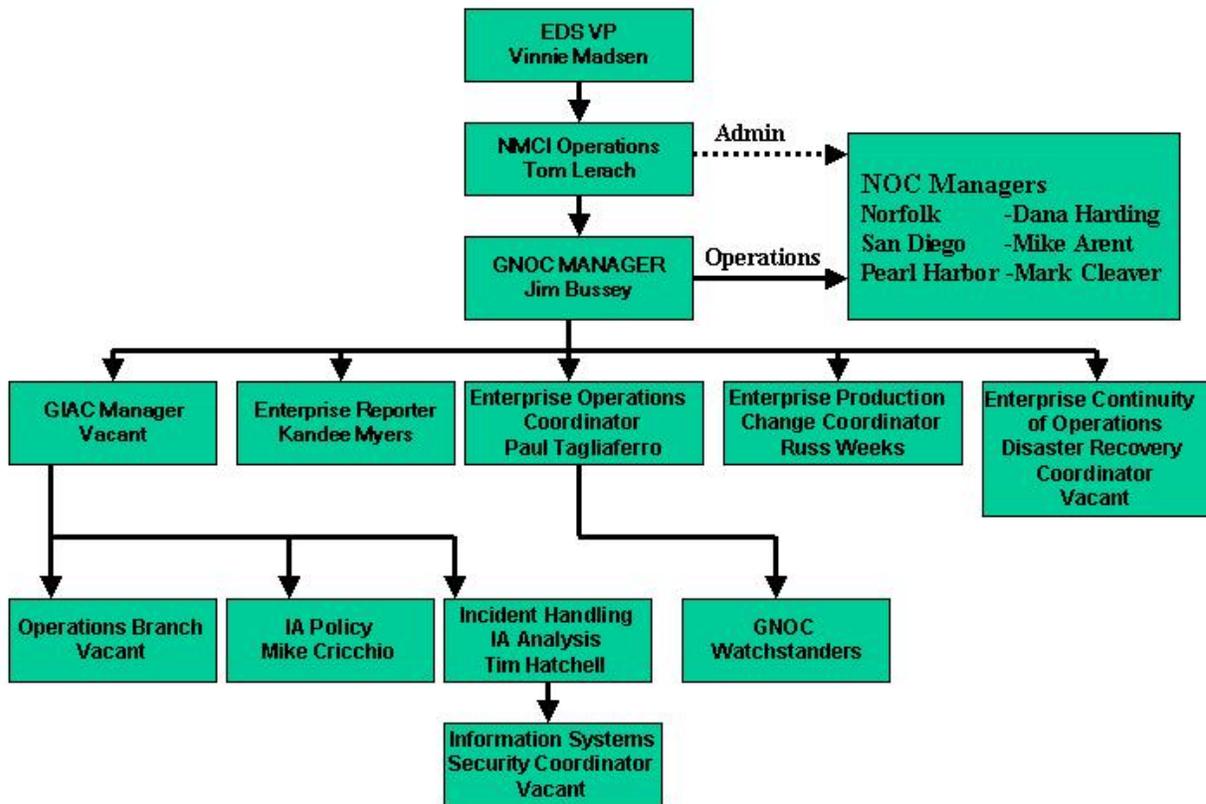


Figure 3 - EDS Organization Chart

2.3.16 NNSOC GNOC and EDS GNOC coordination

The key to effective oversight is good communications channels and a structured, methodical approach to interaction at all operational levels. Ad-hoc activities and interchanges will consistently occur but they will exist within a formal, well-defined government and contractor operational structure.

The following communications frequency is expected at minimum:

- Daily contact will be scheduled to discuss status, urgent topics, operational issues and to provide feedback between government and contractor counterparts.
- Weekly meetings will be scheduled on a regular basis between counterparts.
- Periodic formal meetings will be scheduled to review current workload, progress and status. EDS is responsible for coordinating the agenda 48 hours in advance of the meeting.

- Bi-monthly informal meetings will be scheduled out of the work environment either on a recurring basis or on an ad-hoc basis as needed. Purpose of these meetings will be to discuss current priorities, progress, requirements, and philosophical direction. Neither formal agenda nor minutes are required for these meetings.

2.3.17 NNSOC GNOC / Integrated Support Center (ISC) Coordination

NNSOC GNOC will liaison with ISC as required to properly resolve immediate Enterprise issues that require Program Manager assistance. Ref (o), presently being drafted, will contain detailed operating procedures for the ISC.

3.0 NMCI Operational Governance

3.1 Background

IAW reference (g), the NMCI governance structure will be a permanent structure for the life of the NMCI contract. The charter will be reviewed annually or at the direction of the Operations Advisory Board (OAB), Director NMCI, Navy IO, CNO (N6N7), HQMC or COMNAVNETWARCOM. The NMCI governance structure scope encompasses all enterprise strategic direction, requirements validation, resource and policy matters relating to the NMCI. The scope does not include contract management or network operations. The ASN (RDA) NMCI Executive Steering Committee will provide oversight and guidance specific to the administration of the NMCI contract.

3.2 Purpose

The NMCI governance structure has four primary purposes:

- Establish a working level forum for DoN Claimants and major commands to provide senior level user input to the NMCI enterprise.
- Provide enterprise level review and approval of NMCI requirements and resource priorities.
- Review and recommend enterprise NMCI policy, standards and architectures.
- Review and recommend amendments to the annual NMCI planning process.

3.3 Governance Bodies

3.3.1 Operations Advisory Board (OAB).

The Operations Advisory Board is co-chaired by Deputy DoN CIO Navy and Deputy DoN CIO Marine Corps. Members include HQMC C4, CFFC, COMPACFLT, NETWARCOM, Director NMCI, EDS, NAVAIR, CNET, SPAWAR and NAVSEA. Advisory representation is provided as requested by OAB members.

3.3.1.1 Responsibilities

- Approve policies for operation of NMCI IT policy
- Approve NMCI strategic direction
- Render decisions on issues forwarded by the Stakeholders' Council
- When required, approve the formation/designation of Enterprise Action Groups, and issues to be worked by the groups

3.3.2 Stakeholders' Council (SHC)

The Stakeholders' Council is the primary forum for NMCI requirements and implementation issues. Membership is drawn primarily from Navy Echelon I and II commands, their subordinate Echelon IIIs (as they may indicate), Marine Corps Major Commands and Headquarters Departments, and Unified Combatant Commanders who are customers of NMCI.

Members will be the N6/G6/CIOs' from the entities responsible for IT issues within their respective organizations. Appropriate level representatives from ASD (C3I) and the Joint Staff are included as observers. EDS is included in an advisory capacity when as appropriate. The Stakeholders' Council is co-chaired by the NETWARCOM N6 and HQMC C4. NETWARCOM N6 and HQMC C4 (CP) are co-executive secretaries for the council. Director NMCI will provide technical and advisory support to the SHC.

3.3.2.1 Responsibilities

- Review and validate evolving needs for the NMCI enterprise as a whole
- Review and endorse the results of the NMCI annual planning process
- Review and endorse enterprise resource priorities
- Review and approve enterprise applications review and approve enterprise applications (Gold Disk)
- Recommend enterprise application to Operations Advisory Board and Functional Area Managers (FAMs)/Program Executive Office for Information Technology (PEO-IT)
- Review policies required for the operation of NMCI. Recommend new policies to the Operations Advisory Board
- Review and approve DoN Claimant/Major Command membership on Enterprise Action Groups and issues to be worked to including reasonable timelines for resolution based on the specific issue. Forward recommendations to the Operations Advisory Board
- Provide recommendations on strategic direction for the NMCI enterprise to the Operations Advisory Board
- Forward issues for which consensus cannot be reached or has which have not been resolved within allotted timeline to the Operations Advisory Board

3.3.3 Enterprise Action Groups (EAGs)

EAGs are working groups of DoN and vendor technical personnel modeled on NMCI DoN Action Coordination Teams, and the DoN CIO-led group that established DoN Architecture and Standards. Some will be standing groups, such as the Security (SEAG) and Technical (TEAG) groups, and the Operations Enterprise Action Group (OPS EAG). Some will be issue-specific, and to be formed on an as-needed basis. Each group will be assigned a lead organization designated by the Stakeholders' Council, or the Operations Advisory Board Committee when required, which will provide sponsorship for the group.

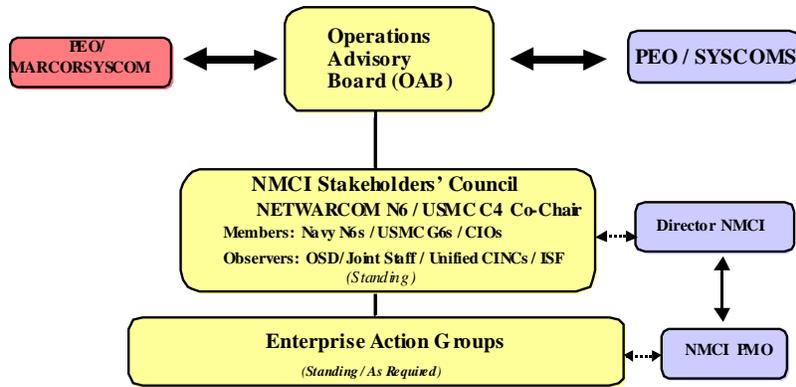


Figure 4. NMCI Governance Structure

Each group will be assigned a lead organization designated by the Stakeholders' Council, or the Information Executive Committee when required, which will provide sponsorship for the group.

- Work NMCI issues identified by Stakeholders' Council
- Provide deliverables and recommendations to Stakeholders' Council

3.3.4 Programatics Enterprise Action Group (PEAG)

The PEAG is an O-6 level oversight body that provides an overall collaborative perspective to a number of acquisition issues that cross the boundaries of the multiple governance bodies. In the overarching context of NMCI Governance (general strategy, policy, requirements definition and major funding issues) the NMCI PEAG's scope of responsibility encompasses all programatics issues regarding the long-term sustainment of the NMCI, including but not limited to: governance; performance measurement and customer support; risk analysis; gap identification and mitigation; identification and mitigation of funding shortfalls; processes and procedures for sustainment of NMCI readiness. It is anticipated that some questions forwarded to the ISC will need to be referred to the PEAG for collaborative direction.

3.3.5 Operations Enterprise Action Group (OPS EAG)

The OPS EAG is a permanently standing enterprise action group chaired by the MCNOSC and NNSOC N36. Its scope is Enterprise operations, defense information systems, shipboard and deployed networks. Its purpose is to develop and implement procedures and processes for enterprise oversight and network operations.

3.4 Organizations and Administrative Support.

3.4.1 The NMCI governance structure ensures that issues are resolved at the appropriate levels and that the entire DoN community is involved in developing/approving an integrated, synchronized NMCI strategy and that the ultimate oversight of the NMCI enterprise rests with the DoN and Service CIOs.

3.4.2 NETWARCOM N6 and HQMC C4 (CP) will serve as co-executive secretaries of the Stakeholders' Council and, will be responsible for:

- Administrative support in the preparing, staffing, and coordinating resolution of proposed issues, agendas and the publication of minutes of the Stakeholders' Council
- Additionally, will establishing timelines for issue resolution, (based on the nature of the issue and on recommendations of Operations Advisory Board), to expedite solutions or
- Forwarding if unresolved issues to appropriate Flag level the OAB for resolution

3.5 NMCI Governance Issue Resolution Process.

3.5.1 Any member of the Council may submit issues for consideration by the Stakeholders' Council. Issues will be submitted to the co-chairs of the Council, the NETWARCOM N6 and HQMC C4.

3.5.2 The co-chairs of the Council will determine, in conjunction with the PMO/PCO/Vendor, if the issue can be resolved within the NMCI contract. If not, the co-chairs will include the issue in the Stakeholders' Council agenda.

3.5.3 Agenda items will be staffed to the Stakeholders' Council and discussed virtually, by VTC, or at a Council meeting. A bi-weekly VTC will be used as a forum to discuss/resolve Stakeholders' Council agenda items. The items will be posted in advance on the NMCI eRoom web site and an email notification sent to the Stakeholders' Council POCs.

3.5.4 If consensus is reached in the Stakeholders' Council, the decision will be forwarded to the PEO-IT Director NMCI, PMO, N6N7/USMC and NETWARCOM for implementation. If consensus is not reached, the issue will be forwarded to the Operations Advisory Board for a decision.

3.5.6 Issues requiring study will be forwarded to a standing Enterprise Action Group, a new group formed to address the specific issue, or a designated organization. The Stakeholders' Council or Operations Advisory Board, as required, will approves the standup of new groups and designates a lead organization for the group. The Stakeholders' Council co-secretaries will track the progress of the issues for the Stakeholders' Council. The group working the issue will report back to the Stakeholders' Council with a recommendation for resolution of the issue.

NMCI Governance Issue Resolution Process

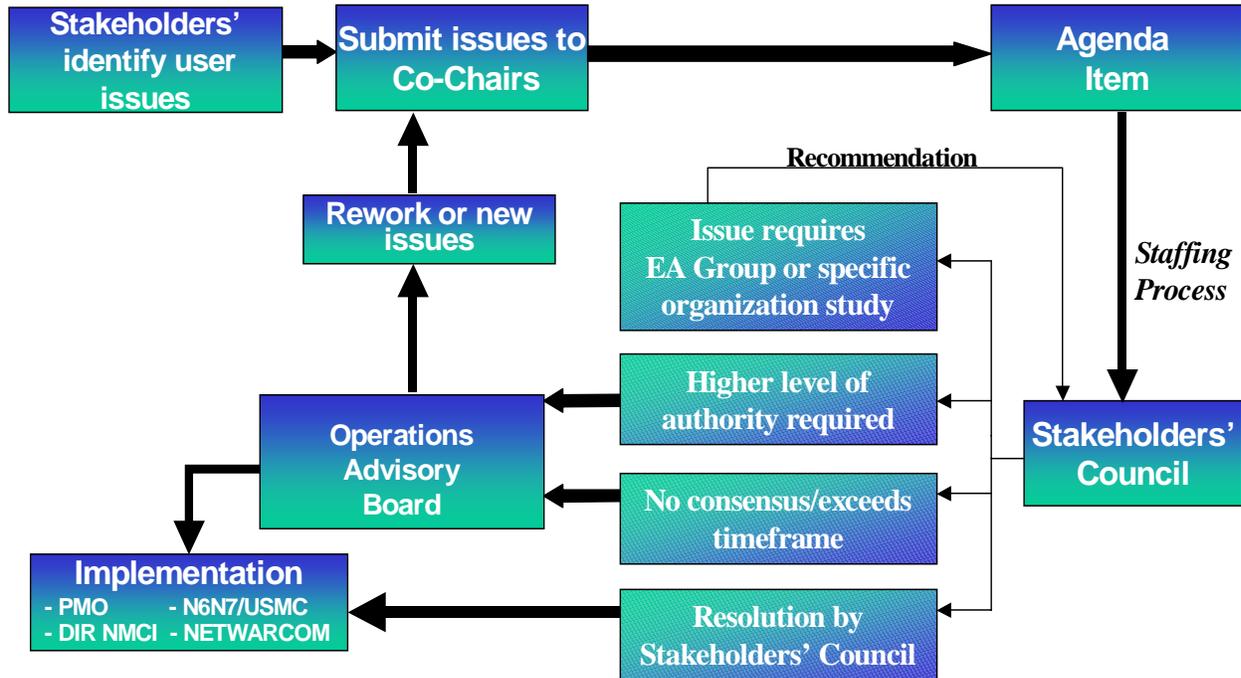


Figure 5 NMCI Governance Issue Resolution Process

4.0 Network Operations

4.1 Introduction

The NMCI contract, section 5.4 under governance states the following:

“NMCI network management policies, procedures, and tools shall enable the Government to exercise operational direction over critical segments of the NMCI infrastructure in support of DoN statutory and war-fighting responsibilities. Operational direction includes the ability to set priorities for contracted services, and to set priorities for resolution of problems/ deficiencies, and to direct changes in network security posture. This capability is required by the Navy and Marine Corps (and Air Force and Army if supported under NMCI) and by theater (CINCPAC and CINCLANT).”

NETWARCOM is responsible for security and accreditation administration, setting policy and acts as the operational DAA for NMCI, excluding that portion which comprises the Marine Corps COI. NNSOC is the agency for exercising operational direction of NMCI. The Government has established a presence at the Contractor’s Global Network Operations Center (GNOC) in order to monitor overall NMCI operations and to exercise operational direction. This includes setting of priorities for contracted services, setting priorities for resolution of problems/deficiencies, and implementing changes in network security posture over critical segments of the NMCI infrastructure, in support of DoN statutory and war-fighting responsibilities. This government oversight is the responsibility of the NNSOC Global Network Operations Center, Norfolk. The GNOC reports operationally to the NNSOC N3 Department. The operational direction process includes:

- Directing emergent network reconfigurations that respond to scheduled and unscheduled force deployments, command relocations, and contingency operations
- Restoring and recovering from network threats and CNA.
- Directing changes in INFOCON as detailed in the INFOCON/Operational Direction MOA.
- Keeping the Major Claimants informed of the status of NMCI and reporting significant network events as they occur.

4.2 Reports

NNSOC and EDS will generate network situational awareness. EDS provides a network picture to NNSOC with the use of various reports on network status, services, incidents and outages. Each of these reports and others described in this section are intended to provide authoritative information that will be used to communicate a “course of action” that the network operations chain of command has agreed upon. Appendix C contains a list of all EDS generated reports. NNSOC reports NMCI status to users via NNSOC SIPRNET webpage. This information is found in the Global C4 Status Board at <http://205.9.251.246/global>.

4.2.1 EDS Provided Reports

EDS has generated documents that detail NMCI operational reporting ranging from daily events to monthly planned considerations (outages and advisories). A complete list is found in

Appendix C. Restoration priorities are detailed in a separate document also produced by EDS and are available in Appendix B. Roles and responsibilities have been developed to describe a number of the processes that are detailed in the PPRs. A complete list found in Appendix C.

4.2.2 NNSOC Provided Reports

The SIPRNET Global C4 Status Board (<http://205.9.251.246/global>), provides the latest up to date telecommunications status from NCTAMS PAC, NCTAMS LANT, NCTAMS EURCENT and NCTS Bahrain as well as NMCI service status. This information is updated every four hours or as information becomes available. The GNOC Watch Officer (GNOCWO) updates the C4 status page as NMCI status changes. In addition, the page provides links to the most recent information pertaining to NIPR and SIPR loading, force disposition and movement, Daily Summary Report (DSRs), EDS's daily status and GNOC Det daily status.

4.2.3 Reporting of Essential Services

There are eight essential services that have been identified by EDS as being critical to customer support and enterprise operation that require immediate notification through a Response to Operational Problems (RtOPs). An RtOPs is defined as a severity level one-problem resolution process designed to notify EDS senior management and customer senior management. Reports of RtOPs will be made to the GNOCWO in the same manner and under the same conditions RtOPs notification is made to EDS and customer senior management. RtOPs are used to report unclassified (NIPRNET) outages and incidents only. Classified (SIPRNET) outages or incidents are reported verbally to the GNOCWO.

Information reported will include at a minimum the month/day/year/time, when the notification is initiated, the principle point of contact related to the incident, the principle point of contact's phone number, the RtOPs case number, the production environment impacted, the essential service affected, the number of users impacted, number of mission critical seats, the impacted sites, when the problem was discovered month/day/year/time, the root cause/reason for outage or incident once issue resolved, and the plan of action for rectifying incident. Follow up messages will be provided at a maximum of 90 minutes after initial discovery of incident. Updates will detail actions taken and planned. Classified reports will not be reported using unclassified means.

The eight essential services are:

- File Services
- Print Services
- Mail Services
- Web Services
- Legacy Access/Reach-back
- Online Web Access (OWA) Services
- Blackberry
- Remote Access Services (RAS)

4.2.4 Additional Reporting Requirements

Other reporting instances to the GNOCWO that do not fall into the "essential services" category as defined above are necessary to provide the government the most available situational

awareness to support operational direction. The same information as provided for RtOPs will be used in these instances with the only difference being that these items will be reported to the GNOCWO immediately upon identification of the incident or occurrence.

Other operational scenarios that require GNOCWO notification include:

- Outages affecting a Flag/General Officer or Senior Executive Office (SES) level customer.
- Any SIPRNET outage, whether believed to be the responsibility of the EDS or not.
- Any virus, worm or malicious code for which an out-of-cycle patch is being recommended by the vendor or which has garnered national media attention.

Outages caused by failed facilities support, weather, various other emergencies or changes in readiness conditions affecting NMCI must also be reported to the GNOCWO as identified in the following paragraphs. Classified reports will not be reported using unclassified means.

Outages caused by weather or other acts of nature are reported to the GNOCWO. Additionally, reports are made to the GNOCWO if anticipated weather, or other acts of nature, have the potential to threaten NMCI. Reports will be updated every six hours or as information becomes available.

Emergency. Report via SITREP to the GNOCWO bomb (threat or action), fire, or terrorist (threat or action). Report initially, then update once an hour at a minimum.

Facility Outages. Report via RtOPs to the GNOCWO any facilities outages to include:

- Air Conditioning
- Power (Commercial or Public Works)
- Generator Power
- Commercial Telephones
- DSN Telephones
- UPS
- Fire Drills requiring evacuation from a NOC facility should be reported via telephone.

Readiness Conditions. Report to the GNOCWO the attainment of INFOCON measures. Report updates upon increase of condition.

Some additional situations requiring reporting include:

- HAZCON – Loss of Redundancy
- Any IA Security Event
- Any Red Team Event
- Site and/or Command Isolation

- Intermittent Service Outage
- COINS connectivity unavailable, VBNS+ Primary Path connectivity unavailable.
- Change to an approved Production Environment Schedule Change (planned maintenance/upgrades)
- Any requests for changes to the Production Environment that are outside established Change/Maintenance windows
- B1/B2/B3 Architecture Change
- Any emergency Break-Fix Change to Production environment
- ECCB Unapproved Break-Fix Change
- Emergent Suppression Change
- Emergent Suppression Completion
- Software Distribution Solution Failure where a site is completely unable to receive software via any architected means
- Significant Operational Change
- Network Support System Outage
- Network management System (NMS) Outage

The GNOCWO reports these situations to the NNSOC NWO as they occur.

4.3 Service Restoration Priority

NNSOC will consult with the Fleet and Unified Combatant Commanders to validate different restoration priority/concerns for the process. This will ensure that all Major Claimants' operational requirements will be met. NNSOC will provide service restoration priorities to EDS. During NMCI outages or degradation, services will be maintained to the highest extent possible. Restoration will occur in a manner approved by the Unified Combatant Commanders, monitored by NNSOC, while ensuring enterprise information assurance and network management is maintained.

A design for graceful degradation of NMCI will ensure that maximum service is provided to each user in accordance with the priorities set for NMCI components and the processes and services supported. The NMCI enterprise is driven by SLA accomplishment. Factoring in Major Claimants' operational requirements, NMCI will operate to meet SLAs no matter the status of the network (it doesn't matter if the network is degraded due to hardware or software limitations or malicious activity/attacks etc.). Although NMCI is driven by SLA accomplishment, the operational requirements of the customer have priority. Considering the priority of restoration, mission critical seats will be considered first to regain their operational capability. EDS/NNSOC has generated a priority list of the restoration of hardware, software and services located in Appendix B.

After mission critical seats are restored, NNSOC will further direct the restoration of services following these guidelines:

- Emergent Contingencies
- On-going operations
- Exercises and training events
- Testing events

NNSOC will consult with the Fleet and Unified Combatant Commanders to validate different restoration priority/concerns for the process. This will ensure that all Major Claimants' operational requirements will be met. The goal being that during any degradation suffered by NMCI, services will be maintained to the highest extent possible and restoration will occur in a manner approved by the Operational Commanders', monitored by NNSOC and conducive to enterprise information assurance and network management.

4.4 SOP and PPRs

NNSOC, in coordination with EDS have established a set of Standard Operating Procedures (SOPs), and Pre-planned Responses (PPRs). Specific SOPs that deal with NMCI are listed in Appendix A. The NMCI Global Information Assurance Center (GIAC), collocated with the GNOC, maintains PPRs for IA events.

4.5 INFOCON Procedures

4.5.1 Background:

The INFOCON system is established by the Secretary of Defense (SECDEF), and executed through the operational authority of the Commander, U.S. Strategic Command (USSTRATCOM) as part of USSTRATCOM's overall responsibility for Computer Network Defense (CND) for the DOD. The Joint Task Force-Computer Network Operations (JTF-CNO) is the USSTRATCOM's operational component for Computer Network Operations. FIWC takes direction from JTF-CNO and coordinates the direction of defense of Navy computer systems and networks. Commanders (Navy has provided authority down to the CSG/ESG level) can impose more *restrictive* measures from a higher level of INFOCON as a situation may warrant, although they cannot take action or adopt a posture less restrictive than that set for the enterprise. In today's network-centric environment, Major Claimants should understand that any risk on NMCI would affect all NMCI users equally. A global network approach necessitates a common understanding of the threat, INFOCON level, and defensive measures implemented with the declared INFOCON. NNSOC has developed a process, vetted through the Fleet and UNIFIED Combatant Commanders, which describes how INFOCONs will be set on NMCI. This approved process is detailed in ref (a).

4.5.2 INFOCON MOA

NMCI INFOCON procedures have been generated from those procedures currently followed by JFCOM and PACOM. These procedures will be rescinded and replaced with the USSTRATCOM procedures when the procedures have been approved by the JCS. The exact process has been detailed in the Coordinating Instructions for Setting US Navy Information Condition (INFOCONs) on the Navy Marine Corps Intranet MOA ref (a).

The INFOCON system must support the commander's ability to perform assigned mission critical responsibilities without major operational mission degradation. The reliance on information systems for critical operational and support functions, such as command and control, intelligence and logistics means that it can not be afforded to disconnect the Navy from these critical resources or other units/agencies. Nor can an adversary be allowed to drive a self-imposed denial of service through the adoption of an overly restrictive security measure. The key tenet is that the Navy should strive to stay connected if at all possible while minimizing all non-essential connections. Each site will have different requirements based on its particular architecture (i.e. legacy applications, etc.). These requirements should be detailed in such documents as the SSAA and any processes or considerations governing those differences should be noted in the appropriate Memorandums of Agreement (MOAs).

4.5.2.1 NNSOC will notify NETWARCOM of the need to convene the Operational Direction Action Team (ODAT). NETWARCOM will announce a meeting of the ODAT for Fleet and Combatant Commanders. As a result of changing the INFOCON level under NMCI, there is a possibility that setting a specific measure across the enterprise will jeopardize operations in a specific commander's Area of Responsibility (AOR). Therefore, prior to directing a change in INFOCON, an ODAT will be convened. The ODAT will be co chaired by PACOM and JFCOM. Voting members include: PACOM, JFCOM, COMLANTFLT, COMPACFLT, MCNOSC and NAVNETWARCOM. EDS will be invited to attend the ODAT as a technical advisor, as required. The ODAT will promulgate all agreed courses of actions, directing the modification of INFOCON through the GNOC. Any areas that cannot be agreed to will be sidebar for further discussion between the ODAT members.

4.6 Network Attacks and IA incidents

4.6.1 Coordinating Responsibilities

NNSOC will be the coordinating command in responding to any network attack or IA incident affecting NMCI, reporting to NETWARCOM. NNSOC will direct EDS in reacting to, and recovering from, any IA event through the NNSOC GNOC. NNSOC GNOC, will develop in coordination with the EDS GNOC enterprise level Standard Operating Procedures (SOPs) and Pre-Planned Responses (PPRs) to meet emerging threats.

4.6.2 Global Information System Security Administrator (GLISSM)

The GLISSM is located at the NNSOC GNOC and is part of the GNOC detachment. The GLISSM duties and responsibilities are contained in reference (b), and in paragraph 4.2.4 below. The GLISSM is NNSOC's representative for the daily administration of Information Assurance (IA) measures and procedures on NMCI.

4.6.3 Pre-Planned Responses (PPRs)

There are numerous PPRs dealing with appropriate responses to specific attacks. The procedures all follow the same basic process as described below:

- Identify the threat.

- Report the incident to the appropriate organizations.
- Correct the situation or isolate the affect of the degradation.
- Restore the rest of the network to the highest extent possible.

The details of the process will are covered in associated NNSOC and EDS SOPS, and will be included in the NMCI CND CONOPS when completed.

4.7 NMCI Information Advisory (NIA) and NMCI Information Bulletin (NIB)

With the growing number of NMCI users and in keeping with NMCI policies, NIBs and NIAs will be used to keep all users informed of policy and procedural changes within the scope of NMCI. NIB/NIAs are serialized regular Navy messages. NNWC is the releasing authority for all NIBs and NIAs. NIBs will provide NMCI policy and procedural guidance. NIAs will be used for informational topics and to provide interim guidance until policy is validated and put in place. NIBs will be incorporated into future revisions.

5.0 Operational Interfaces

5.1 Scheduled Maintenance and Notification Procedures

5.1.1 Guidance and procedures for the conduct of scheduled and emergent maintenance on NMCI and AOR networks.

5.1.1.1 Scheduled outages and maintenance actions

a. Routine maintenance that is not expected to have an operational impact is scheduled IAW the following timeline (all times local to where the maintenance is taking place):

- (1) MON - THU: 2200-0400
- (2) FRI: 2200-1100 (Saturday)
- (3) SAT: 2200-0400
- (4) SUN: Not normally scheduled

b. NMCI GNOC Det will make notification via RMG/EMAIL/USER notifications for maintenance that has a potential for operational impact and for temporary changes to the above maintenance schedule.

c. Concurrence/non-concurrence is gained through coordination between EDS GNOC, EDS regional managers, EDS site managers, site CTRs and the commands affected by the maintenance. Site non-concurrence results in a postponement of the maintenance until a mutually agreed upon time is reached.

d. Notification will be sent announcing the significant maintenance event with an anticipated operational impact NLT 24 hrs prior to event start.

5.1.1.2 Demand maintenance is a specific category that is required IOT correct urgent problems or support transition efforts. This category does not permit more than 24 hrs to prepare and requires user notification only usually via email.

5.1.1.3 Unscheduled outages

A. RtOPs report these outages to the designated POCs at each major Command IAW GNOC Det SOPS, PPRs and instructions.

C. Phone notification and NMCI Fleet advisories messages will be sent based on the severity of the outage and services or infrastructure affected. For example, if an outage affecting all NMCI services at NAS Patuxent River Maryland would occur, it would be of the severity for

phone notification and/or NMCI Fleet Advisory. The latest status of NMCI is available on the NNSOC SIPRNET C4I Status website (205.9.251.246/NMCI).

5.1.1.4 Testing: Entities with requirements for testing shall have a DAA approved test plan. Notification to users and action officers will be in accordance with section 5.3.1.1 above.

5.2 Securing unclassified desk top computers

5.2.1 NMCI is an enterprise service provided through a centralized management process. As part of this service, EDS updates operating systems and applications installed on NMCI seats to keep them current. Upgrades, replacements and patches for the seat software are installed by automatically pushing the changes to seats from the NMCI network operations centers. To receive pushes, it is necessary for the seat to be powered up and connected directly to the network.

5.2.1.2 Unless special conditions exist that would necessitate powering down the unclassified seat, the NMCI standard practice for unclassified end users is to log off, but not power off the computer, when securing from daily activities. Software upgrades cannot be pushed to seats that are secured at the time of the push or are receiving NMCI services via the Remote Access Service (RAS). In these instances, the push automatically occurs as soon as the seat is directly connected and powered up.

5.2.1.3 Locking the seat also differs from logging off. When a seat is locked, automatic pushes to that seat are not permitted. Users should never lock their seat as a means of securing the NMCI seat outside normal working hours.

5.2.1.4 Software upgrades cannot be pushed to seats that are receiving NMCI services via the Remote Access Service (RAS). In this instance, the push automatically occurs as soon as the seat is directly connected.

6.0 NMCI Operational Communication Plan

6.1 NNSOC Communication:

NNSOC has developed and uses various vehicles for communicating with NMCI Commands and users. The objective of the NNSOC NMCI communications process is to ensure timely and accurate dissemination of information during NMCI operations.

6.1.2 C4 Status Page

The C4 status page will be the **primary means** by which the NNSOC GNOC will communicate the status of NMCI to all users. The C4 Status page is available on the SIPRNET <http://205.9.251.246/global>.

6.1.3 User Communiqués

User Communiqués is a NNSOC GNOC/ EDS GNOC coordinated email by which NNSOC GNOC transmits NMCI user information to all, or selective groups of NMCI users. The NNSOC GNOC will collect and maintain group email addresses as required to properly respond to real world situations and exercise environments.

6.1.4 NMCI Advisories

NMCI advisories are regular Navy messages transmitted by the NNSOC GNOC and/or the Network Watch Officer transmitted to inform Navy Commands of critical NMCI events, such as power outages, service interruption, and exercise events.

6.2 EDS Communication

EDS executes NMCI enterprise-wide user communications using several types of media. These advisories and notification are distributed via email and posted within the NMCI internal and external websites. These media types are described below.

6.2.1 Email

Email will be used to distribute or “push” key information to users. NMCI User Alerts and the *Inside NMCI* newsletter will be distributed to users through email. All-Hands, site specific and server farm specific distribution lists will be implemented to facilitate this form of email communication.

6.2.2 NMCI User Alerts

NMCI User Alerts will be used for time sensitive and high priority communications. NMCI User Alerts will be placed in a standard NMCI User Alert template (Exhibit B) indicating user action when required. NMCI User Alerts will be used to communicate planned/unplanned network outages, NMCI operating environment changes, virus alerts, and any change or update requiring user action. The process for creating and distributing user alerts is cited in Section 6.3.

6.2.3 Inside NMCI newsletter

The *Inside NMCI* newsletter will also be distributed to all NMCI users via email. The newsletter will contain low to medium priority announcements distributed to users on a periodic basis. Newsletter content examples include announcements of new or updated postings to the NMCI

User Information websites, upcoming changes to the NMCI environment, and general NMCI news. Links to additional information on included topics will be provided when appropriate. The process for developing and distributing the *Inside NMCI* newsletter is cited in Section 6.2.

6.2.4 NMCI Web Sites

Users can access or “pull” information from both the internal and external NMCI User Information web sites. The web sites serve as a central repository for NMCI user collateral and provide users with an NMCI ‘Tip of the Week’ and other NMCI reference materials. The NMCI User Information section of the eds.com/NMCI and NMCI portal web sites will serve as a central repository for user collateral.

6.2.5 NMCI Tip of the Week

The web sites will be routinely updated with an NMCI ‘Tip of the Week’ to educate users on NMCI and application functionality. These tips will provide operational guidance on specific issues based on Help Desk tickets, customer satisfaction survey results, or general user feedback. The process for posting ‘Tip of the Week’ material to the NMCI User Information web sites is cited in Section 6.4.2.

6.2.6 NMCI Reference Materials

User collateral and NMCI reference materials will be available on the internal and external NMCI User Information web sites. Users will be informed of new or updated documents through announcements in the *Inside NMCI* newsletter. Users can access information from the NMCI User Information websites by downloading or printing documents. The process for posting new or updated documents to the NMCI User Information web sites is cited in Section 6.4.1.

6.3 Printed Collateral

NMCI Getting Started Guides (GSG) are distributed with each new NMCI workstation at the time of transition. The NMCI Getting Started Guide consists of several user reference materials providing instruction on key elements of the NMCI operating environment. Each document included in the GSG is available on the NMCI User Information websites. Processes for the production and distribution of GSG’s are cited in Section 6.5.1.

COMMUNICATION	FREQUENCY	DISTRIBUTION METHOD
Alerts	As needed	Email to Users
Alerts (Software Pushes)	As needed	Email to Users; Posted to the User Information web page
User Collateral	As needed	Posted to the User Information web page
Tip of the Week	Routine	Posted to User Information web page
Inside NMCI	Routine	Email to Users and post to User Awareness web page

Getting Started Guide	As needed	Distributed with each new NMCI workstation
-----------------------	-----------	--

7.0 Cutover and Operational Readiness Review (Under development)

The purpose of the Cutover and Operational Readiness review is to ensure that a site in the final stages of AOR is ready to cutover to and operate within the NMCI enterprise network. A secondary purpose is to establish a baseline level of knowledge of NMCI operating idiosyncrasies for the site NMCI users. The development of this process is a collaborative effort between NNSOC and PMO and the Director, NMCI. It is envisioned that an Assist Team will be formed, using NNSOC, GLISM, EDS and PMO personnel. The team will additionally be used as a tool during steady-state operations, to assist Commands that experience a sudden drop in corporate NMCI knowledge.

APPENDIX A

SOPs / PPRs available on the Global C4 Status Board on the NNSOC SIPRNET website:

<http://205.9.251.246/global>

100 Administration

- 100 Standard Operating Procedures
- 101 Key Personnel Recall Procedures
- 102 NNSOC Organizational/Collateral Duties
- 103 GNOC Director Responsibilities
- 104 GNOC Watch Officer (GWO) Responsibilities
- 105 GNOC LCPO, LPO & TPO Responsibilities
- 106 GNOC Watch stander Responsibilities
- 107 GNOC Watch Turnover Responsibilities
- 108 GNOC Shift Change Responsibilities
- 109 GNOC Command Log
- 110 Telephone Communications Procedures
- 111 Security Procedures
- 112 CTF EDS Norfolk Regional NOC Director Support Procedures
- 113 Computer Security Procedures
- 114 GNOC Command Center Tour Guide
- 115 Gate Guard User's Guide
- 116 Message Dissemination Subsystem
- 117 NNSOC Remedy User's Guide (currently being revised)
- 118 AMCROSS Emergency Leave Procedures for Military Personnel
- 119 GNOC Daily Status Report
- 120 Handling Procedures for Unclassified Messages
- 121 Handling Procedures for Classified Messages

200 Emergency Pre Planned Responses

- 200 Pre-Planned Response
- 201 GNOC Fire Evacuation
- 202 Bomb Threat Procedures
- 203 Fuel Spill or Gas Leak
- 204 Inclement Weather
- 205 Outages
- 206 Status Report
- 207 Unsecure Space or Safe
- 208 Medical Emergencies
- 209 Relocation to Alternate GNOC (San Diego)
- 210 GNOC OPREP-3/Unit SITREP Handling Procedures

300 Security/IA Procedures

- 301 Root Access

- 302 Access
- 303 Attempted Access
- 304 Denial of Service (DOS)
- 305 Probes
- 306 Malicious Logic
- 307 Poor Security
- 308 Navy Information Operations Condition (INFOCON) Implementation
- 309 Information Assurance Vulnerability (IAV) Alert-Bulletin-Technical Advisory
- 310 Internet Protocol (IP) Addressee-Port Blocking Messages

400 Sample Messages

- 401 Sample Fleet Advisory NMCI Power Outage
- 402 Sample Fleet Advisory NMCI Service interruption
- 403 Sample Fleet Advisory NMCI Loss of NIPRNET Connectivity
- 404 Sample Fleet Advisory NMCI NIPRNET WEB BROWSING (U)
- 405 Sample Fleet Advisory NMCI SIPRNET WEB BROWSING (S)
- 406 Sample Fleet Advisory NMCI NIPRNET SIPRNET NETWORK DEGRADATION
- 407 Sample UNIT SITREP Message
- 408 Sample OPREP Message
- 409 Sample INFOCON Message

500 References

- 500 Web Site Index
- 501 Points of Contacts
- 502 Duty NOC Manager Numbers
- 503 Security Terms & Abbreviations

APPENDIX B
Network Restoration Priorities

Note: No one command has priority over another. Outages are treated enterprise-wide using the following restoration priority:

Infrastructure From the Highest to the Lowest

NOC

Very Large Server Farm

Large Server Farm

Medium Server Farm

Small Server Farm

BAN

Pier-Side Connectivity

Remote Site

LAN (building)

Workgroup (wiring closet/switch)

Desktop

Classified Service

SIPRNET Access

Domain Name Services

Organizational Messaging

Desktop Access to Legacy Apps

Directory Services

Remote Access

Proxy & Cache Services

E-Mail Services

Fixed/Moveable VTC

File Services

Web Services

Print Services

NMCI Web Portal

Software Distribution

Unclassified Service Restoration Priorities

Intranet Access

NIPRNET Access

Domain Name Services

Organizational Messaging

Desktop Access to Government Apps

Directory Services

E-Mail Services

Fixed/Moveable VTC

File Services
Print Services
Proxy/Cache Services
NMCI Web Portal
Web Services
Internet Access
Software Distribution
Remote Access

**APPENDIX C
EDS REPORTING REQUIREMENTS**

Type	Title	Contents	Frequency
Service Levels	SLA Data Report	Data showing service levels provided for period	Monthly
Financial	Small Business Report	Data showing small business cumulatively and at 1 st and at 2 nd and 3 rd tier use for period	Every six months
Financial	Small Business Report	Data showing small business who had previously supported DON workload and are integrated into NMCI	Every six months
Financial	Small Business Report	Data showing small business revenue down to a site specific level (i.e., the base zip code or phone area code region)	Every six months
	Order Status Report	Data shall include ordering office, order number, order date, order status, back order date, ordered amount due, date order created, order created by I.D., date order last modified, number of ordered products, ordered product, product number, quantity, order product status and unfilled orders status, quantity shipped, date shipped, quantity installed, and order price.	Monthly
	Asset and Credit Report and Asset Management Database	Data shall include description of asset, location of asset, quantity of asset, assessment line item number, date of assessment, plant property value, age, life cycle duration and cost, proposed/actual credit amount, delivery order number, deductive delivery order amount, line of accounting, funding document number, funding document description, delivery order description, commitment amount, obligation amount, and expenditure amount. See Attachment 9.	Monthly (maintained continuously)
	Incentive Report	Data shall include order or modification number, date and amount, description of incentive, date of audit, and date of incentive payment.	Monthly
Security	Incident Report	Data shall include any configuration changes, computer incidents, network incidents, INFOCON status, and intrusion detection reaction alert status.	Within 24 hours of incident

	C&A Documentation	Data shall include the following: <ul style="list-style-type: none"> • System Security Authorization Agreement (SSAA) • Risk Assessments • Vulnerability Assessments • Risk Mitigation Plans 	SSAA: Initial draft 30 days after placement of first order, second delivery 90 days after placement of first order, third delivery 180 days placement of first order, with revisions at IOC and FOC and if there are any significant architecture changes at any other time. All other requirements due annually, at a minimum.
	DISN Connection Approval Documentation	Data shall include documentation required for NIPRNET and SIPRNET connection approval as specified in DISN connection approval policy	30 days following placement of first order
	Security CONOPS (Including Disaster Recovery Plan)	Detail security procedures for operations on NMCI	Within 45 days placement of first order and updates semi-annually thereafter.
	Security Critical Product Selection	Data shall include a listing of all IA mechanisms, to include but not be limited to the following: firewalls, intrusion detection systems, virtual private networks, security management tools, operating system for server and user workstations, smart card reader, etc.	15 days after placement of first order and within 10 working days of changes
	Security Status Report	Real time data feed supporting government oversight of security functions.	Continuous
	Security Procedures	Data shall include security procedures describing how IA mechanisms will be operated to provide the security services	Delivery with initial seats, updates with changes
	GFE Type 1 Crypto Requirements	Data shall include a detailed listing of required GFE Type 1 crypto devices. Data shall include the following at a minimum: quantity of Type 1 crypto required, classified key material required, dates required for both crypto and classified key material:	15 days placement of first order, updates with changes
Architecture	Diagram Reports	The documentation will provide a systems architecture view of the NMCI in contractor's standard format. The documentation will include a full description of all external interface points, to include DoD compliant technologies, protocols, and peering arrangements for external connectivity. It will include	NLT IOC, and within 5 working days of changes

		physical and logical connectivity, and how interoperability is achieved at the interfaces. The architecture will detail NMCI hosting of legacy systems. Data shall include graphic architecture designs and cabling diagrams, at least to the building level	
	Network Connectivity Plan	Data shall include network topology showing WAN/MAN/BAN/LAN connectivity. All external interface connection points (DISN, Internet, etc.) shall be clearly annotated.	15 days placement of first order and within 10 working days of architecture changes
	Security Architecture	Data shall include architecture diagrams that depict how information is transferred through defense in depth boundaries 1 through 4 (e.g., from MAN/WAN connections at boundary 1 to interior destinations, down to hosts on LAN at boundary 4). Diagrams should include the proposed employment of all major network components (at a minimum in-line network encryptors, firewalls, intrusion detection systems, servers, routers, switches, load-balancers, and data path) that play a significant role in network operation, management, and security. Diagrams shall also indicate location of alternate paths and backup equipment. This includes information sources, supporting paths and capacities, any unique manipulation of data in transit, points of termination and placement of all proposed security components. The diagrams shall be in contractor format. Diagrams shall address both unclassified and classified architectures, and also any unique architectural differences associated with different types of locations (NOC, large base, small base, etc.).	15 days placement of first order, and within 10 working days of architecture changes.

Type	Title	Contents	Frequency
Personnel	Personnel Skill Maintenance Plan	Data shall include a plan for affected personnel assignments and training monthly.	Monthly
Voice	Voice Billing Statements	Separate billing statements at the seat/line/trunk level for tolls on FTS 2001 or commercial long distance	Monthly
Video	Configuration Management Report	Provide data sufficient to identify configuration management of video seats	Updated with each deployed unit
Interoperability Document	OCONUS interoperability	Interoperability technical information for OCONUS provider	As required
DISN Waiver	Request for Government Waiver	Waiver for commercial or alternative to DISA/WAN service	As required
Network Management System Service	Information Feeds for Government Oversight	Historical data summary and management reports detailing NMS functions	Continuous
Integrated Configuration Management	Logical Relationship Record	Logical relationship record of items and asset inventory	24 hours after change
Embarkables	Consumable and Electronic Test Equipment Report	Data should include a list of consumable items with sources and a list or electronic test equipment	Updated with each deployed unit