

**Marine Corps Appendix  
to the DSP  
v 1.0**



# Table of Contents

1. INTRODUCTION.....	1
1.1. Purpose .....	1
1.2. Scope.....	1
1.3. Process Overview .....	1
2. MARINE CORPS DEPLOYABLE SUPPORT SERVICES .....	4
2.1. Marine Corps Enterprise Network (MCEN) Support Services .....	4
2.2. Marine Corps Tactical Data Network (MCTDN) Support Services .....	4
2.3. Tactical Training Portal Support Services .....	5
2.4. NMCI Support Services .....	6
2.4.1. Reachback.....	6
2.4.2. Help Desk .....	7
2.4.3. Logistics.....	7
2.4.4. Maintenance .....	7
2.4.5. Training in the Deployment Process .....	7
2.4.6. Data Migration .....	7
2.4.7. Email Forwarding and Redirection .....	7
2.4.8. Directory Services.....	8
2.5. Customer Technical Representative (CTR) Support and Responsibilities .....	8
3. METHODS OF EMPLOYMENT .....	9
3.1. Garrison .....	9
3.2. Leave, TAD, and Liberty .....	9
3.2.1. NMCI Email Redirection.....	9
3.2.2. Client E-mail forwarding.....	10
3.2.3. Server E-mail forwarding .....	10
3.2.4. RAS/VPN Connectivity.....	10
3.3. Exercise/Operational Deployment.....	11
3.3.1. Peripheral Devices.....	11
3.3.2. Data Migration .....	12
3.3.3. RAS/VPN.....	12
3.3.4. Email Redirection.....	12
3.3.5. Email Forwarding .....	13
3.3.6. NMCI Seat Deployment .....	13
3.3.7. Loading PKI Certificates for RAS/VPN .....	13
3.3.8. Joining a Deployed Domain .....	14
3.3.9. Installing PKI Certificates for OWA Access.....	14
3.3.10. Dial In Access .....	14
3.3.11. OWA from a Deployed Network .....	15
3.3.12. NMCI Seat Rebuild.....	15
3.3.13. Reconfiguring Internet Explorer during RAS (After joining a non-NMCI domain) .....	15
3.3.14. Termination of Email Redirection .....	16
3.3.15. Termination of Email Forwarding .....	16
3.3.16. Data Migration (Post Deployment) .....	16
3.3.17. NMCI Seat Return .....	17

3.3.18.	Trouble Shooting the Return Process .....	17
3.3.19.	Garrison Operations in Support of Tactical Training .....	17
3.3.20.	Domain Transitions .....	17
4.	PROCEDURAL INSTRUCTIONS NOT INCLUDED AS ATTACHMENTS ..	18
4.1.	High Speed VPN.....	18
4.1.1.	Client to Peer .....	18
4.1.2.	Peer to Peer.....	18
4.2.	Email Forwarding .....	18
4.2.1.	Client Email Forwarding.....	18
4.2.2.	Server Email Forwarding .....	18
4.3.	Data Migrations.....	18

## **Attachments**

1. NMCI Engineering Operations Procedure – Govt. Aide To Deploy
2. NMCI Engineering Migration Operations Procedure – Pack Up Kit Standard Operating Procedure Deployables
3. NMCI Garrison Training Support Plan Deployed Support Working Group
4. NMCI Deployable Seat – Configuring Internet Explorer with PKI CERT
5. Outlook Web Access User’s Guide
6. NMCI Deployable Seat – Redirecting NMCI E-Mail Procedure
7. NMCI Deployable Seat – Remote Access Server (RAS) Procedures Document
8. NMCI Deployable Seat – TimeStep (PERMIT/Client) VPN Procedures Document
9. Remote Access Server Getting Started Guide
10. Remote Access Server User’s Guide
11. NMCI Deployable Seat – Data Migration Procedure
12. NMCI Deployable Seat – Administrator’s Aide to Configuring Network Settings for Joining a Deployed Network Domain
13. NMCI Deployable Seat – Configuring Internet Explorer for Usage on the NMCI Network
14. NMCI Deployable Seat – Deployable Application (Deploy) Procedure
15. NMCI Deployable Seat – Deployable Application (Return) Procedure
16. Outlook E-Mail Forwarding Procedures

# **1. INTRODUCTION**

## **1.1. Purpose**

This appendix describes the USMC unique procedures for processing user seats into and out of the NMCI environment. The Marine Corps Information Technology (IT) environment will change under NMCI. Since NMCI is an Indefinite Delivery Indefinite Quantity (IDIQ) contract, much of the service is centrally ordered and funded. Overall program costs are based on the number of seats purchased by the USMC. It is therefore important to define the required type of seats and inherent services necessary to support a unit's mission. Deploying units must decide if they will remain connected to NMCI via "portable" seats or transition the seat via the Deployable Process Architecture (DPA\*) to "deployed" status and access NMCI from external connectivity. The difference in these methods will become apparent to the reader of this appendix. IT Marines must be aware of their unit IT mission requirements, rely on their past experience, and possess a thorough understanding of the NMCI options, to efficiently and successfully support the deploying unit. This appendix will serve as a guideline for ensuring the IT Marines have viable options for best supporting their unit.

\* Details of the DPA are contained in the NMCI Engineering Operations Procedure – *GOVT Aide to Deploy, Version 2.3 dated 10/16/02 (Attachment 1)*.

## **1.2. Scope**

This document defines the USMC procedures required to transition an NMCI seat/user from the NMCI environment into other user environments, and back into the NMCI.

## **1.3. Process Overview**

To fully understand the scenarios for deploying NMCI seats, it is necessary to first understand the basic mechanics of seat and account deployment under NMCI.

The intention of the deployable process is to provide the operational unit the ability to achieve and sustain self-sufficiency in all facets while in a deployed status.

To achieve and sustain self-sufficiency, it is highly recommended and encouraged for the Commanding officer of the deploying unit and the designated Unit IT representative to ensure that all configuration management and configuration control processes and precautions are taken and followed. Documenting and noting all configuration changes made to each NMCI deployable seat for integration into the deployed location's network will facilitate a quick and seamless reintegration into the NMCI environment upon return from the deployment.

Deploying an NMCI seat from the NMCI environment to an external network requires the following instructional documents:

- Submission of an Embarkable Move/Add/Change (MAC) request (Request to Deploy) to move the seat from the NMCI to the deployed environment.
- Migration of User/Organization data.
- Suppression of the NMCI Enterprise Management System (EMS) functionality on the deployable seat.
- Transfer of system administrative rights to the individual NMCI deployable seat.
- Redirection and/or Forwarding of Email.

The reintegration process is essentially the deployment process reverse order, with the addition of a scan for network configuration and Information Assurance (IA) compliance that is made by the NMCI EMS prior to restoring the seat to full NMCI functionality.

The configuration for IP addressing, Domain Name Service (DNS), and IP routing must be modified in order to return a deployed seat to the NMCI network. The deploying unit's Information Technology (IT) representative must reconfigure the seat prior to its reentry into NMCI, in order to accept a Dynamic Host Configuration Protocol (DHCP) network address from the NMCI network.

NMCI Machine and User Accounts – In the Windows 2000 client and server environment used within NMCI, NMCI machine accounts and user accounts are two separate entities (similar to Windows NT client and server environment). Either one may be put in a “deployed” status independently of the other.

In fact, a user may be deployed with someone else's machine.

Disconnecting an NMCI Machine Account

Disconnecting an NMCI User Account

Deployed NMCI Machine Account – The seat is under the full control of the unit IT. It may be reconfigured as required, including loading additional software, changing user profile or hardware settings, etc. Any applications added while in a deployed status must be removed prior to reconnecting to the NMCI environment. Data files resulting from such applications are not required to be removed; however, data requiring preservation should be migrated to alternate storage; NMCI reconfiguration/IA scripts target executable files of various types during the reconnection process. Currently, in addition to these administrative actions, deploying seats triggers the provisioning of spares kits, a critical necessity for the deploying unit. The specific components provided and percentages of each are provided in the Pack Up Kit (PUK) SOP (Attachment 2).

Deployed NMCI User Account – For a user account, being in the “deployed” status simply enables email redirection to occur, although this does not happen automatically; it must be selected during the “request to deploy” process. Unit policy will determine which users, if any, are allowed to have mail redirected to a deployed account. Options for email forwarding and redirection and the impacts of each are explained in Section 3.

Reconnect NMCI Machine Account

Reconnected NMCI User Account

## **2. MARINE CORPS DEPLOYABLE SUPPORT SERVICES**

### **2.1. Marine Corps Enterprise Network (MCEN) Support Services**

The MITNOC provides network technical advice and assistance during the planning phase of a deployment or exercise and coordinate swift solutions to networking problems during the execution phase.

### **2.2. Marine Corps Tactical Data Network (MCTDN) Support Services**

Wide-Area Network (WAN) - A WAN is comprised of multiple router connections interconnecting Local Area Networks across large geographical areas. Standardized Tactical Entry Point or STEP sites provide MCTDN WAN Point of Presence connectivity into the Defense Information Switched Network or DISN. DISN provides Internet Access Backbone (IAB) gateways for Non-Secure Internet Protocol Router Network (NIPRNET) and Secure Internet Protocol Router Network (SIPRNET) connections. The MCTDN is required to connect all NIPRNET and SIPRNET connections across DISN provided IAB gateways.

Internet Packet Routing (IPR) – IPR is the process of assembling and disassembling data for transmission to and from remote systems. IPR requires a systemic process of creating user data (application layer), formatting and representation of the data (presentation layer), establishing and terminating application sessions (session layer), transport fault detection, recovery, and dividing data into fragments (transport layer), encapsulating the data into a packets (routing layer), framing and translating data into bits (data link layer), and finally transmitting the electrons (physical layer) to remote systems.

External Network Access (ENA) – ENA is any request for, or transmission of data that extends beyond one physical/logical segment to another. ENA services traditionally traverse a router with a point of origin (local) and termination points (remote).

Remote Access Service (RAS) – RAS is a connection between two computers via a Private Automatic Branch Exchange (PBX) – telephone network. RAS connections extend IP connectivity to mobile users and are primarily used to gain access to protected “intranet” and the public “internet” environments.

Information Assurance (IA) – IA is defined in Joint Pub 3-13 “Joint Doctrine for Information Operations” (9 October 1998), as: “Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”

Public Key Infrastructure (PKI) – Enables users of a basically unsecured public network such as the Internet to securely and privately exchange data through the use of

a public and a private cryptographic key pair. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

Local Area Network (LAN) – A communications system that links computers into a network, usually via a wiring-based cabling scheme. LANs connect PCs, workstations and servers together to allow users to communicate and share resources like hard disk storage and printers. The MCTDN extends NIPRNET and SIPRNET services to users via separate physical LAN devices.

Internet Packet Routing – See WAN IPR above.

Network Management – The process and techniques of remotely or locally monitoring and configuring networks. Network management takes account of five key areas: configuration management, fault management, performance management, accounting management, and security management.

Directory Services (DS) – A dynamic means to browse the network for users and resources. Examples of DS are, Global Address List (GAL) recipients and network neighborhood computer resources.

File Sharing – A container (folder), partition or machine available to multiple users for sharing data. Typically, file sharing occurs in client/server relationships. Servers maintain data in containers that reside on physical disk partitions, and users access, modify, and delete data as necessary. The owner of the container or data controls user access to files in shared containers.

Network Storage – A repository of organizational and user data, stored on devices (file server, CDROM tower, Network Attached Storage (NAS), etc.) within a LAN. These devices archive data on a regular basis. Network Storage is apportioned, maintained, and supported for access, historical, and disaster recovery purposes.

Terminal Emulation – Software (i.e., IBM Host on Demand, Reflection for IBM, etc.) that allows a computer to mimic the attributes of a dumb terminal normally attached to a mainframe or mini-computer, providing a user with access to function keys and control sequences. The most commonly emulated terminal is IBM's 3270.

### **2.3. Tactical Training Portal Support Services**

The Marine Corps requires an NMCI capability similar to the Navy's Pier-side Connectivity, for the purpose of providing connection points on Bases and Stations that will allow for tactical network training to continue. All Marine Communications elements currently use garrison networks to prepare for deployment and for training, and these NMCI connection points, referred to as "Garrison Network Portals," will continue this capability. Units must be able to continue to build tactical architectures, while in garrison, in order to provide tactical training prior to deployment, test and configure equipment prior to going into a combat zone, avoid the logistics costs associated with fully deployed tactical training exercises, and eliminate equipment and software

problems prior entering the austere environments which are typical of the Marine deployment. The Garrison Network Portal, or simply Portal, provides auto-sensing Ethernet and Fast Ethernet Local Area Network (LAN) connections, with accompanying Wide Area Network (WAN) connectivity, to an exercising unit, which can range from one laptop to over a thousand network-attached deployable devices, using the full spectrum of network services. All currently available network services must be present at the Portal for the exercising unit, whether these services are provided by the Information Strike Force or by the servicing base G6. A goal of the portal concept is to maximize the benefit of “backyard exercise” training, while reducing or eliminating architectural changes to the NMCI networks which support the base. The Portal replaces an existing capability at each base and station, where the exercising unit currently enters the garrison networks through any Ethernet wall plug, in coordination with the Base G6. There will be basically two types of Portals: the *Building Portal*, and the *Weatherized External Portal*. It is currently envisioned that 100 – 500 portals will be necessary in order to replace the current connectivity aboard the bases and stations. Additionally, there will need to be a nodal cell, referred to as the Deployed Support Cell, in a central location aboard the base, which will be operated by the Base/Station G6 to support units who conduct training through the Portals spread throughout the base. A detailed description of this proposed service is contained in Attachment 3.

## **2.4. NMCI Support Services**

### **2.4.1. Reachback**

#### **High-Speed Virtual Private Network (HSVPN)**

HSVPN extends all NMCI Services to the User by using tunneling methods across existing networks. These networks can be tactical or commercial. HSVPN allows Users with an NMCI Seat and User account to attach to external networks and extending the NMCI environment out to their desktop at speeds of the external network. Both Pier to Pier and Client to Pier is supported.

#### **Outlook Web Access (OWA)**

OWA is a commercial Application that allows an NMCI USERS access to his/her NMCI Email Account from external networks. The User will require a computer running at a minimum Internet Explorer 5.0, his/her PKI Certificate and his/her NMCI User Name and NMCI Password.

#### **Remote Access Service (RAS)**

RAS Reachback would be used when an USER with an NMCI Seat is located where NMCI network services are not locally available. RAS services use a Commercial Phone Line or Commercial like services are provided (e.g. TCC-42 with Commercial Access, DSN). RAS connectivity requires that a user connect via dialup to UUNET and connect to the NMCI network with VPN software (PERMIT/client). This service will be used during both Leave/TAD and Exercise/Operations. RAS Access will extend all NMCI services to the user at modem speeds.

### **2.4.2. Help Desk**

NMCI Helpdesk is provided via both commercial and DSN telephone. The user will need to know both the asset tag number and the Machine Name that they are experiencing issues with before contacting the Help Desk. The Help Desk will assign a trouble ticket number and assign a priority to the ticket and start working the issue.

### **2.4.3. Logistics**

#### **Pack-Up Kit (PUK)**

PUK's will be issued depending on the Units needs. Working directly with your CTR will help the unit IT determine the extent of the PUK that is needed for your operation. A PUK will normally contain additional hardware. Gold Disk's (Machine Rebuild Software) will be included with the PUK that will allow unit IT's to rebuild / restore a NMCI seat back to a static state.

### **2.4.4. Maintenance**

Unit IT's will be trained on the 1<sup>st</sup> and 2<sup>nd</sup> echelon maintenance of the Deployable machine. This training will include, Hard Drive Replacements, systems rebuild, proper cleaning and care for the deployable equipment.

### **2.4.5. Training in the Deployment Process**

ISF is responsible for training System Administrators/Users in those skills, which are required due to the differences between the NMCI environment and the generic skills required to be an effective system administrator in a tactical network environment. Standard training for system administrators/ users will be provided through existing Marine Corps formal schools and other training courses.

### **2.4.6. Data Migration**

NMCI User Data can be stored on NMCI Shared Drives or on the NMCI Seat in the Users My Documents folder. This data must be migrated/backed up in order to ensure that the data is available after the NMCI Seat is joined to a non-NMCI Domain.

### **2.4.7. Email Forwarding and Redirection**

Email Forwarding and Email Redirection are two different processes. Email Forwarding will maintain a copy of the users Email messages in the users assigned mail store.

Email Redirection happens at the users Mail Exchange Server. A message that is received by the exchanger will be automatically redirected to another assigned exchanger. Care must be used to ensure that a valid account exist on the

accepting exchanger to insure that an existing account exists. If an account is not available the message will be lost.

Redirection is accomplished by one of 3 means:

- Calling the NMCI HelpDesk and requesting that E-Mail Redirection be started.
- Contact the Unit CTR for batch user Redirection.
- Accessing a secure NMCI website by logging into the server.

There are 2 types of Email Forwarding.

- Client side forwarding which requires the user's Machine is be on line in the NMCI Environment.
- Server side forwarding, which will occur at the NMCI Mail exchanger.

#### **2.4.8. Directory Services**

### **2.5. Customer Technical Representative (CTR) Support and Responsibilities**

Customer Technical Representatives are the primary unit interface to the ISF and NMCI services. CTR roles and responsibilities before, during, and after deployments are contained in the NMCI Engineering Operations Procedures – Gov't Aid to Deploy (Attachment 1).

### 3. METHODS OF EMPLOYMENT

In the Windows 2000 client and server environment used within NMCI, NMCI machine accounts and user accounts are two separate entities(similar to Windows NT client and server environment.) Either one may be put in a “deployable” status independently of the other. The Marine Corps will employ the NMCI network to conduct repeatable processes, which can be divided into the following four (4) areas:

#### 3.1. Garrison

In the garrison environment, all data processing, help desk, and administrative services will be provided by ISF. The user or Marine System Administrators can take no administrative actions in the garrison environment. No system administrator privileges will be available for USMC personnel while in garrison.

#### 3.2. Leave, TAD, and Liberty

An NMCI user in a leave, liberty or TAD status will still have NMCI services available with or without an NMCI seat. An NMCI user with a portable or deployable seat may disconnect that machine from its physical connection to NMCI, and use a RAS or VPN connection to access NMCI services. The user may also utilize Outlook Web Access (OWA) from a non-NMCI computer to access limited NMCI services.

Outlook Web Access is available from any non-NMCI provided computer with IP connectivity (internet access.) In order to use this capability, users should be aware that PKI certifications must be installed on the computer they are utilizing. User may access NMCI Outlook services such as email, calendar and public folders via OWA. Table 3.1 lists the instructional documents to be followed in order to access this service.

Document	Paragraph	Attachment
Configuring Internet Explorer with PKI Cert	Entire document	4
NMCI ISF Outlook Web Access Users Guide, IE 5 edition unclas version 1.1	Entire document	5

Table 3.1

##### 3.2.1. NMCI Email Redirection

User may redirect email to another .mil or .gov address. Table 3.2 lists the instructional documents to be followed in order to access this service.

Document	Paragraph	Attachment
Redirecting NMCI email procedures	Entire document	6
NMCI Engineering Operations Procedure – Gov't Aid to Deploy, v2.3	2.2.2	1
Table 3.2		

### 3.2.2. Client E-mail forwarding

Users may forward email to another .mil or .gov address. Table 3.3 lists the instructional documents to be followed in order to access this service.

Document	Paragraph	Attachment
Outlook Email Forwarding	Entire Document	16
Table 3.3		

### 3.2.3. Server E-mail forwarding

Users may forward email to another .mil or .gov address. Table 3.4 lists the instructional documents to be followed in order to access this service.

Document	Paragraph	Attachment
Exchange Email Forwarding		In development
Table 3.4		

### 3.2.4. RAS/VPN Connectivity

Via RAS/VPN connection, the portable or deployable NMCI seat receives all NMCI services as though the user was physically connected to the NMCI. When accessing NMCI services under the conditions in this paragraph, the user has no administrative machine privileges. Table 3.5 lists the instructional documents to be followed in order to access this service.

Document	Paragraph	Attachment
Remote Access Service (RAS Dialin) Procedures Document	Entire Document	7
TimeStep (Permit/Client) VPN Procedures Document	Entire Document	8
NMCI ISF Remote Access Service Getting Started Guide	Entire Document	9
NMCI ISF Remote Access Service Users Guide	Entire Document	10
Table 3.5		

### 3.3. Exercise/Operational Deployment

An exercise deployment is defined as the conduct of training supporting the development of processes and procedures improving overall combat efficiency, sustainability and survivability of operational forces. An operational deployment is defined as the conduct of operations in a non-training environment. It can be a wartime deployment, afloat, humanitarian operation, or any other deployment that is not intended as a training evolution. An NMCI user can “deploy” locally or to another geographical area for a training exercise. A User or Unit IT must execute the Deployable Application version 2.1, so the Unit IT will receive XDEPLOYADMIN privileges/password. This is required to allow the NMCI deployable seat to join a non-NMCI domain. Administrator privileges are provided under the XDEPLOYADMIN user account. The password for the XDEPLOYADMIN account is provided by the Information Strike Force (ISF) helpdesk at the request of the unit IT. This entire process is detailed in the Government Aid to Deploy, version 2.3, dated 16 Oct 2002 (Attachment 1).

#### 3.3.1. Peripheral Devices

Peripheral devices, either government furnished equipment (GFE) or NMCI provided (CLIN 23) are authorized for use during deployments.

##### 3.3.1.1. Government Furnished Equipment (GFE)

If the unit owns deployable IT assets, these assets may continue to be deployed along with NMCI deployable equipment. Currently owned tactical printers may be used. Printers not directly attached to the NMCI garrison network, may also be taken on deployments, if authorized by local command policy. An example is a stand-alone workstation printer. If the capability exists for the unit to independently purchase additional peripheral equipment for deployment through external sources, the unit may exercise this option in accordance with local command procedures.

##### 3.3.1.2. CLIN 23 Items

Another option for units to purchase peripherals with local funds is through NMCI CLIN 23. All CLIN 23 items have been “deemed” deployable by EDS. Operational requirements may drive the use of creating equipment “pools”. This method may be driven by mission requirements, optempo, and local command policy. If a unit requires additional CLIN 23 items not currently on the NMCI contract, the unit must contact MCSC for a CLIN 23 modification.

**NOTE:** CLIN 23 items may be purchased via the contract for limited duration usage. Thus, if a unit required deployed peripheral support for 6 weeks at a CAX, they could order CLIN 23 peripherals for the 6-week period.

### 3.3.2. Data Migration

If data migration is required from the NMCI to a deployed environment, deploying NMCI users may follow the instructional documents listed in table 3.6 to migrate any necessary data.

Document	Paragraph	Attachment
Data Migration Procedures	Entire Document	11
Outlook Backup & Restore		In development
NMCI Engineering operations Procedure – Gov't Aid to Deploy, v2.3	2.3.5	1

Table 3.6

### 3.3.3. RAS/VPN

While an NMCI seat is in a deployed status, the capability to RAS/VPN back into NMCI exists. Table 3.7 lists the instructional documents to be followed in order to access this service.

Document	Paragraph	Attachment
NMCI/ISF Remote Access Service Getting Started Guide v1.3	Entire document	9
NMCI ISF Remote Access Service Users' Guide, v 1.6	Entire document	10
Remote Access Service (RAS Dial In) Procedures Document	Entire document	7
TimeStep (Permit client) VPN Procedures Document	Entire document	8

Table 3.7

### 3.3.4. Email Redirection

NMCI deploying users may use the instructional documents outlined in table 3.8 to redirect their NMCI email to their deployed account. It may not be possible to complete this step prior to the deployment. If that is the case, table 3.8 also outlines the instructional documents to accomplish email redirection after deploying.

Document	Paragraph	Attachment
Redirecting NMCI Email Procedures	Entire document	6
NMCI Engineering operations Procedure – Gov’t Aid to Deploy, v2.3	2.2.2	1
Table 3.8		

### 3.3.5. Email Forwarding

NMCI deploying users may use the instructional documents outlined in table 3.9 to forward their NMCI email to their deployed account. It may not be possible to complete this step prior to the deployment if the new email address is unknown. If that is the case, table 3.9 outlines the instructional documents to accomplish email forwarding after deploying. Note that there is a difference between email redirection (para 3.3.4) and email forwarding (para 3.3.5). Email redirected from NMCI will not leave a copy of the message in the deployer’s NMCI mailbox. Email forwarded from NMCI will leave a copy of the email in the users NMCI mailbox as well as sending a copy to the deployed account.

Document	Paragraph	Attachment
Outlook Email Forwarding	Entire Document	16
Table 3.9		

### 3.3.6. NMCI Seat Deployment

The steps taken in preparation to disconnect from the NMCI environment and join a non-NMCI environment, achieve administrative privileges, and stop all EMS services are outlined within the documents in Table 3.10.

These events are initiated by the execution of the Deployable Application 2.1 and require a connection to the NMCI (Network LAN or RAS/VPN). This event may occur before or after physically relocating from the garrison NMCI environment.

Document	Paragraph	Attachment
NMCI Engineering operations Procedure – Gov’t Aid to Deploy, v2.3	2.2	1
Deployable Application (Deploy) Procedure (DA 2.1)	Entire Document	14
Table 3.10		

### 3.3.7. Loading PKI Certificates for RAS/VPN

Table 3.11 indicates the instructional documents required to load PKI certificates onto the TIMESTEP/PERMIT application, which allows a deployed or TAD NMCI user to RAS/VPN to NMCI.

Document	Paragraph	Attachment
NMCI/ISF Remote Access Service Getting Started Guide v1.3	Entire document	9
NMCI ISF Remote Access Service Users' Guide, v 1.6	Entire document	10
Remote Access Service (RAS Dial In) Procedures Document	Entire document	7
TimeStep (Permit client) VPN Procedures Document	Entire document	8
Table 3.11		

### 3.3.8. Joining a Deployed Domain

Table 3.12 outlines the instructional documents required to join a deployed NMCI seat to a tactical non-NMCI domain.

Document	Paragraph	Attachment
Administrator's Aid to Configuring Network Settings for Joining a Deployed Network Domain	Entire document	12
Table 3.12		

### 3.3.9. Installing PKI Certificates for OWA Access

Instructions for installing a PKI ID certificate for access to OWA are contained in table 3.13.

Document	Paragraph	Attachment
Configuring Internet Explorer with PKI CERT	Entire document	13
NMCI ISF Outlook Web Access Users Guide, IE 5 edition unclass version 1.1	Entire document	5
Table 3.13		

### 3.3.10. Dial In Access

Dial in access procedures are reflected in the instructional documents outlined in table 3.14.

Document	Paragraph	Attachment
Remote Access Service (RAS Dialin) Procedures Document	Entire document	7
NMCI/ISF Remote Access Service Getting Started Guide	Entire document	9
NMCI/ISF Remote Access Service User's Guide	Entire Document	10
TimeStep (Permit client) VPN Procedures Document	Entire document	8
Table 3.14		

### 3.3.11. OWA from a Deployed Network

A deployed user may utilize OWA to access limited NMCI service while connected to a deployed network. The procedures for this service are outlined in Table 3.15.

Document	Paragraph	Attachment
Configuring Internet Explorer with PKI Cert	Entire document	13
NMCI ISF Outlook Web Access Users Guide, IE 5 edition unclass version 1.1	Entire document	10
Table 3.15		

### 3.3.12. NMCI Seat Rebuild

Table 3.16 lists the instructional documents required to rebuild a deployed NMCI seat.

Document	Paragraph	Attachment
Gold Disk Rebuild Procedures		In development
NMCI Engineering operations Procedure – Gov't Aid to Deploy, v2.3	2.3.3	1
Table 3.16		

### 3.3.13. Reconfiguring Internet Explorer during RAS (After joining a non-NMCI domain)

This is a unique scenario. After joining a non-NMCI domain, cached Internet Explorer settings are lost and must be reconfigured to enable IE during a RAS session back to NMCI. Table 3.17 reflects the instructional documents required to reconfigure Internet Explorer proxy settings.

**NOTE (Security Concern):** Users MAY NOT maintain deployed LAN connectivity, while connecting to NMCI via a RAS connection.

Document	Paragraph	Attachment
Configuring Internet Explorer for Usage on the NMCI Network	Entire document	13
Remote Access Service (RAS Dialin) Procedures Document	Entire document	7
NMCI/ISF Remote Access Service Getting Started Guide	Entire document	9
NMCI/ISF Remote Access Service User's Guide	Entire Document	10
Table 3.17		

### 3.3.14. Termination of Email Redirection

Instructional documents to terminate email redirection are listed in table 3.18.

Document	Paragraph	Attachment
Redirecting NMCI Email Procedures	Entire document	6
NMCI Engineering operations Procedure – Gov't Aid to Deploy, v2.3	2.2.2	1
Table 3.18		

### 3.3.15. Termination of Email Forwarding

Instructions for terminating email forwarding are covered in table 3.19.

Document	Paragraph	Attachment
Outlook Email Forwarding	Entire Document	16
Table 3.19		

### 3.3.16. Data Migration (Post Deployment)

Instructional documents to migrate data developed during the deployment, back into the NMCI are listed in table 3.20.

Document	Paragraph	Attachment
Data Migration Procedures	Entire Document	11
Outlook Backup & Restore		In development
NMCI Engineering operations Procedure – Gov't Aid to Deploy, v2.3	2.3.5	1
Table 3.20		

### 3.3.17. NMCI Seat Return

The steps taken in preparation to disconnect from the non-NMCI environment and join the NMCI environment, relinquish administrative privileges, and start all EMS services are outlined within the documents in Table 3.21.

These events are initiated by the execution of the Deployable Application 2.1 and require a connection to the NMCI (Network LAN or RAS/VPN). This event may occur before or after physically relocating from the non-NMCI environment.

Document	Paragraph	Attachment
NMCI Engineering operations Procedure – Gov’t Aid to Deploy, v2.3	2.2	1
Deployable Application (Return) Procedure (DA 2.1)	Entire Document	15

Table 3.21

### 3.3.18. Trouble Shooting the Return Process

Refer to the Deployables Support Plan (DSP) Appendix D: NMCI Seat and User Account Reintegration Checklist and the Deployable Error Code Document for an explanation of error message and suggested resolutions.

If the Unit IT is unable to resolve issues, they should contact the ISF Help Desk at (866) 843-6624 (THE-NMCI)

### 3.3.19. Garrison Operations in Support of Tactical Training

Garrison training portals are under negotiation with ISF and instructions for their use will be published after negotiations are complete. A detailed description of the proposed service is contained in Attachment 3.

### 3.3.20. Domain Transitions

When engaging in an Operational Deployment, the requirement exists to create unique domains for deployed forces. MITNOC is the USMC POC for creation of deployed domains. The process for this will be determined through future negotiations and promulgated by HQMC (C4) when complete. Those procedures will be included as a portion of this document.

## **4. PROCEDURAL INSTRUCTIONS NOT INCLUDED AS ATTACHMENTS**

Procedural instructions contained in this section are intended to cover procedures and processes that are not specifically covered by the detailed instructions provided as attachments to this document.

### **4.1. High Speed VPN**

#### **4.1.1. Client to Peer**

#### **4.1.2. Peer to Peer**

### **4.2. Email Forwarding**

#### **4.2.1. Client Email Forwarding**

#### **4.2.2. Server Email Forwarding**

### **4.3. Data Migrations**

Data migration is defined as the process of deploying user data with the deploying force. Currently, existing data is available to accompany deployed forces. There are several methods used to transport the data. These methods include, but are not limited to, Network Access Storage (NAS) devices, servers, user workstations and additional storage media, such as hard drive, tape, or CD ROM.

Command requirements will dictate the type of media to be utilized based on the content limitations of the respective media types. Media types currently available under the NMCI contract can be found at the following URL:

<http://www.nmci-isf.com/>