# 7th Signal Command
# Enterprise Email - Spiral 1

## Concept of Operations
## 2012

**March 3, 2010**

**Version 1.30**

**THIS DOCUMENT SUPERSEDES ALL PREVIOUS VERSIONS**

**DISTRIBUTION:**

This document is intended for use by US Government agencies and their Contractors doing business with the United States Army CIO/G6. This document is for information purposes only and is not to be construed as directive in Nature or official policy. This document is available by request from the 7th Signal Command (Theater) G3, ATTN: NETC-SFC, Fort Gordon, GA 30905-5832.

**DISTRUBUTION STATEMENT C:**

Distribution authorized to U.S. Government agencies and their contractors to protect technical information from automatic dissemination under the International Exchange Program or by other means. Other requests for this document shall be referred to 7th Signal Command (Theater) G3, ATTN: NETC-SFC, Fort Gordon, GA 30905-5832.

DISCLAIMER

The contents of this document are not to be construed as an official Department of the Army position unless so designated by other authorized documents. The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

Refer requests for all changes that affect this document to: G3 (Plans), 7th Signal Command, ATTN: NETC-SFC-O, Fort Gordon, GA 30905-5832.

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

Prepared by
Mr. Herman Wells
Enterprise Services Chief, 7th Signal Command

___________________ Date____________

Prepared by
Mr. Tom Duke
Engineering Services Chief, 7th Signal Command

___________________ Date____________

Reviewed by
Mr. Richard Breakiron
Deputy G3, Future Operations, 7th Signal Command

___________________ Date____________

Released by
xxxxx
xxxxx

___________________ Date____________

(U) This page intentionally left blank.

# CHANGE NOTICE

| Date of Change | Version Number | Description of Change |
|---|---|---|
| 1 Oct 2009 | 0.1 | Initial draft |
| 20-Nov 2009 | 0.2 | 2nd draft |
| 4 Dec 2009 | 0.3 | Review with CTNOSC and AGNOSC |
| 7 Dec 2009 | 0.4 | Additional clarification and removal of non-spiral 1 issues. |
| 14 Dec 2009 | 1.0 | Final questions resolved and document submitted for staffing and signature |
| 18 Feb 2010 | - | Original author: LTC Peter Barclay, CIO/G6 |
| 19 Feb 2010 | 1.05 | Changed from DA directed CONOPS to 7th Signal Command CONOPS |
| 22 Feb 2010 | 1.06 | Implemented changes from Tom Duke and Richard Breakiron |
| 23 Feb 2010 | 1.07 | Implemented changes from LTC Barclay |
| 24 Feb 2010 | 1.08 | Implemented changes from Roger Loeb, Steve Simpkins, and Herman Wells |
| 24 FEB 2010 | 1.09 | Implemented changes from meeting with Richard Breakiron, Tom Duke, Steve Simpkins, and Herman Wells |
| 25 FEB 2010 | 1.1 | Implemented changes from PHONECON with Roger Loeb, MAJ Moore, LTC Barclay, Keith Lowry, Mr. Boyle, LTC Watkins, and Herman Wells |
| 1 MAR 2010 | 1.15 | Incorporated comments from latest GO level IPR |
| 1 MAR 2010 | 1.20 | Roger Loeb, CTNOSC, PMO, LTC Barclay comments added |
| 2 MAR 2010 | 1.25 | Donald Greenlee and Joan Tracy comments added |
| 3 MAR 2010 | 1.30 | Ensured document was publicly releasable |

# (U) EXECUTIVE SUMMARY

## (U) BACKGROUND

The strategic environment has changed significantly since the end of the Cold War, and events since September 11, 2001 have dramatically demonstrated that we have entered a new era of conflict with difficult challenges to overcome. To meet these challenges, the Department of the Army requires enterprise services to create an information advantage by providing seamless collaboration and moving the power of information to the tactical edge. Implementing an Army Enterprise Email Service (EMCS) is a major step towards meeting these needs.

## (U) PROBLEM

Today’s joint force operations require extensive collaboration across organizational boundaries and rapid deployments to world-wide locations. To operate across organizational boundaries, our forces are hamstrung with excessive equipment (e.g., multiple user access devices), inefficient operations (e.g., multiple user email addresses), and suffer the consequences of reduced capabilities (e.g., unable to quickly find contact information for non-organizational personnel). Our current environment of disparate, loosely connected organizational email systems has inherent deficiencies that prevent net-centric operations and hinder cross-organizational collaboration.

## (U) WAY FORWARD (VISION STATEMENT)

The Army plans to eventually consolidate existing email systems into a single enterprise email service. The ultimate end state of the Army EMCS is to provide operational forces with the ability to access email from any terminal attached to a DoD network in any operational environment. Forces can easily discover the contact information for, and exchange messages with, anyone in the DoD enterprise. Virtual teams, spanning organizations and geographical locations, can create dynamic distribution lists and share calendars. Deploying forces can seamlessly disconnect from the home station and reconnect at forward locations without the need for intensive, manual administrative processes. Distributed nodes at the tactical edge can operate as an integrated part of the Amy EMCS when network connectivity is available or operate stand-alone, providing local user email services when disconnected from the enterprise network. Forces have stable identities allowing full collaboration to leverage the collective knowledge of U.S. forces to defeat any enemy. The current acquisition effort is the first step in that direction. This initial effort is a learning opportunity for the Army. Future acquisitions may or may not be built on this foundation.

## (U) BENEFITS

The Army EMCS will improve mission effectiveness; reduce vulnerabilities to cyber attacks posed by adversaries, and save millions of dollars. In summary, those who support the goals of our nation require robust global connectivity and email in a wide variety of environments.  The DoD must operate collaboratively across the collective enterprise to seamlessly facilitate information-enabled operations.  Army EMCS is the first step.

NOTE: The Executive Summary and throughout this document, the desired end-state of a consolidated email system is provided.  In this way, leaders working on Spiral 1 understand the Army’s vision for the future.  It in no way guarantees or is meant to imply this will be the final end-state.

# (U) TABLE OF CONTENTS

# TABLE OF CONTENTS

## (U) LIST OF FIGURES

## (U) LIST OF TABLES

**No table of figures entries found.**

.

# 1 (U) INTRODUCTION

## 1.1 (U) PURPOSE

This document, 7th Signal Command Enterprise Email Spiral 1 (EMCS) Concept of Operations (CONOPS), describes the concept of operations for initial managed service enterprise email capabilities, which will:

- Operate in a fully networked, global collaborative environment.
- Initially address the full spectrum of Army email mission requirements at the non-tactical level.
- Establish a baseline e-mail service in order to evaluate the EMCS on its ability to support Army organizations within CONUS.
- Set the stage for ongoing operations and maintenance of the system after full operational capability of Spiral 1 is complete.

## 1.2 (U) SCOPE

This CONOPS specifies the full operational capability (FOC) required to execute spiral 1 enterprise email operations across the Army enterprise and will set the stage for expanded email capability for future requirements. The CONOPS describes the end state for spiral 1 Army enterprise email service (EMCS) consistent with current joint warfighting and intelligence community operations. Spiral 1 only applies to the unclassified (NIPRNet) network within the Continental United States (CONUS) and will have the capability to support up to 230,000 users.

## 1.3 (U) OVERARCHING MISSION NEEDS

To keep pace with the ever changing strategic global landscape, the Department of Defense is pursuing the most comprehensive transformation since World War II. The Army transformation efforts underway in support of the DoD are both evolutionary and revolutionary in nature and intended to improve our national capabilities to meet the demanding requirements of a nation at war, as well as future, full spectrum national security requirements. National security transformation will attain a force capable of full spectrum operations in a joint/inter-agency, network-enabled, and global collaborative environment.

To meet national security challenges, the Army community requires enterprise capabilities that provide an information advantage through network-enabled, commander-centric operations and seamless collaboration across the entire enterprise, while moving the power of information to the tactical edge. These enterprise capabilities must be configured to achieve the appropriate balance between information sharing and information security.

The primary mission drivers for the Army EMCS are improved mission effectiveness by using common, standard enterprise services; unification (e.g., improved security, enterprise directory services, and identity management services), and significant cost savings. A user's email address should not change as the user moves between home station, mission rehearsal or exercise, en route, and deployment. This includes providing access to email from any location (using client software or a web-browser), a complete global address list, universal calendar functionality, and similar enterprise email capabilities. The objective is to improve U.S. Army operations by enhancing communication across the Army enterprise. Military, civilian, and contractor personnel supporting U.S. Army missions require the ability to:

- Access email capabilities from anywhere, at anytime, and from any place, whether stationary or mobile.
- Find and validate the identity of, and securely exchange information with, people within the Army enterprise and external entities (e.g., federal agencies, mission partners, and coalition partners) with whom they must interact to perform missions.
- Coordinate efforts by sharing individual, organizational, and resource calendars across the Army enterprise.
- Easily and effectively share information among virtual groups that are geographically dispersed and organizationally diverse.
- Continue critical mission operations at a local level when disconnected from the enterprise email network.

The Army community must:

- Improve the effectiveness of mission planning and execution by integrating and extending email capabilities.
- Reduce the vulnerability of email to the growing cyber security threats by eliminating unnecessary seams between the thousands of current heterogeneous local networks.
- Reduce the cost of email by eliminating unnecessary administration and inefficient network configurations to free up resources for other Army priorities.

The initial effort of implementing Army enterprise email as a managed service is the first step towards ultimately achieving the overarching needs. It fulfills some of the objectives completely, some of them partially, and some of them not at all, while allowing the Army to understand both the value and the complexity of implementing managed services.

## 1.4 (U) CURRENT ARMY EMAIL ENVIRONMENT

Army organizations have independently implemented and optimized email capabilities for effective use within their respective organizational boundaries. Consequently, the Army enterprise contains multiple, disparate stove-piped email systems and processes that prevent net-centric operations and hinder cross-organizational/mission collaboration. Further, the multiple organizational email systems employ user access devices that are uniquely configured to limit access to authorized users. In this current environment users are unable to:

- Easily find and exchange information with personnel across operational environments and across the DoD.
- View calendars and reserve shared resources external to respective local organization.
- Send signed and encrypted email to many DoD personnel.

Linking islands of organizational networks with dissimilar security capabilities and processes creates vulnerabilities. Unless corrected, these cross-organizational vulnerabilities provide opportunities for enemies to apply increasingly sophisticated cyber attacks. Collectively, sustaining the plethora of organization-specific email systems within the Army enterprise consumes significant resources with estimated annual operating costs in excess of $400 million. Dominant cost factors are the administrative and technical support staffs required to support each organizational email system at the post, camp, base, station and current APC.

The Army's Active Directory (AD) structure is based on multiple generating forces' forest implementations of Microsoft Active Directory 2003 or in some cases 2008 in both the Non-secure Internet Protocol Routing (NIPR) Network and the Secure Internet Protocol Routing (SIPR) Network. *Currently* the Army's NIPR AD environment consists of fifteen (15) approved forests supporting approximately 300 sites and 950,000 users around the world. The approved forests are: Space and Missile Defense Command (SMDC), Continental United States (CONUS), Inspector General Network (IGNET), the Army Reserves, Medical Command (MEDCOM), Military Entrance Processing Station Command (MEPCOM), Accessions Command, Military Academy (EDU), Intelligence and Security Command (INSCOM), National Guard, Corp of Engineers, Europe, Pacific, Korea, and Southwest Asia. The Army's SIPR AD is similar to the NIPRNet except at a much smaller scope due to smaller user population.

Of special note is the current reliance of email on Army Knowledge Online (AKO). All Army personnel are required to have an AKO email address, and this is the default (or universal) address that all personnel use. All email destined for Army mail servers external to the users enclave flows through AKO (see Figure 1 below). The figure demonstrates the flow of email from logical enclaves (CONUS, the Managed Service Provider (MSP), or Europe) to various users. It does not necessarily indicate which Active Directory (AD) forest someone logs into (despite the triangles), but rather which logical email enclave a user gets service from. Any use of Exchange within the Army must take this fact into consideration when implementing user accounts. In addition, local email user addresses are linked to a single email address registered with AKO. Though this allows individuals in the Army to maintain one email username, it does not provide transparency when existing users move from one location to another. Usernames must be decoupled from the existing installations Exchange server and paired with the receiving installation's Exchange server.

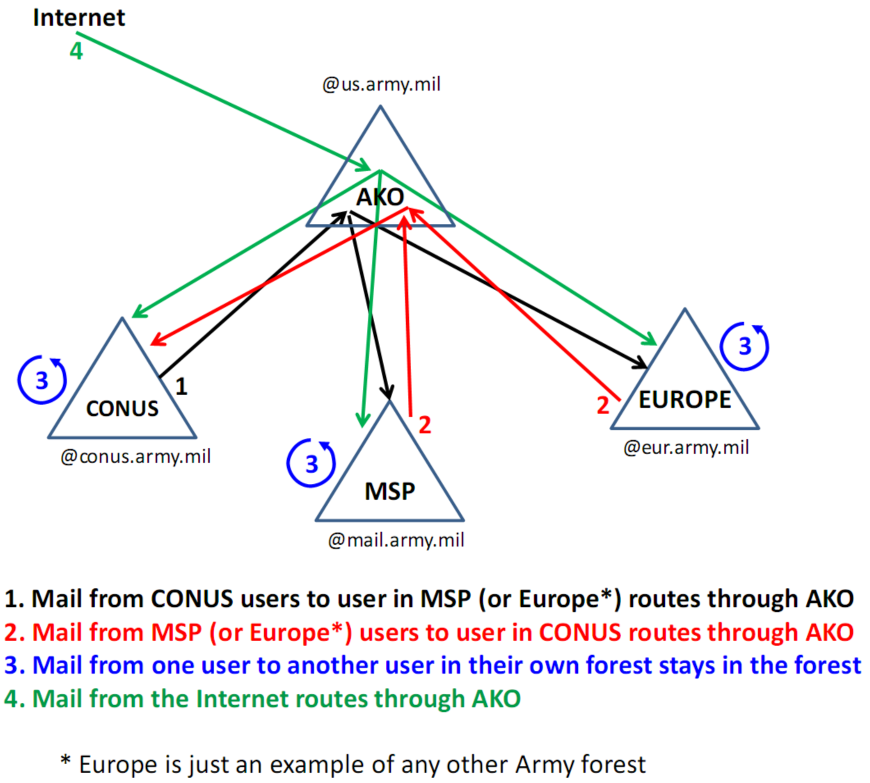
Internet
4
@us.army.mil
AKO
3
CONUS
1
@conus.army.mil
3
MSP
2
@mail.army.mil
3
2
EUROPE
@eur.army.mil
1. Mail from CONUS users to user in MSP (or Europe*) routes through AKO
2. Mail from MSP (or Europe*) users to user in CONUS routes through AKO
3. Mail from one user to another user in their own forest stays in the forest
4. Mail from the Internet routes through AKO
* Europe is just an example of any other Army forest

**Figure 1. (U) Depiction Email Routing Flow (LTC Peter C Barclay, 2010)**

Today's joint operations require extensive collaboration across organizational boundaries and rapid deployment to world-wide locations. Currently, email users who must operate across organizational boundaries are hamstrung with multiple user access devices and/or hindered by reduced capabilities when interacting with non-organizational Army and DoD personnel. Deployed forces must carry extensive support equipment to temporary operating locations or lose connectivity with supporting networks for extended periods of time.

The initial effort of implementing Army enterprise email as a managed service is not intended to address every issue raised in this description of the current Army email environment.

## 1.5 (U) SPIRAL 1 ARMY EMAIL ENTERPRISE SERVICES (EMCS)

Army personnel will not experience any reduction in capability or service level from the email service.  They will be able to access email and a fully-populated DoD global address list, and calendaring from any location (using client software or a web-browser). Military members without access to their own thick client or desktop will be able to manipulate email via a rich Exchange based web client with features such as drag-and-drop, drop down buttons, pop-up windows (with editing), and tool bars.  The email service will provide support for mobile/wireless platforms such as RIM Blackberry or Windows Mobile. The service will continue to support S/MIME for encrypting and signing messages.

(U/FOUO)  The EMCS will be operated by a managed service provider using Microsoft Exchange 2010.  They will provide a workable strategy and automated tools to lead in the migration of users and mail based data from the current installation to the EMCS location in an expedient and efficient manner with minimal direct touch labor assistance from the local Network Enterprise Center.  The MSP will comply with all relevant DoD and Army policies, including DIACAP and DoD policy (DoD STD 5015.2) for retention and archiving.  The managed service provider will have a 24x7 Tier II service desk that is electronically integrated with the Army’s Tier I Enterprise Service Desk (ESD).  Army personnel will contact the ESD, and the ESD will elevate relevant email problems to the Tier II service desk for resolution.  Metrics that provide a clear view of IT systems performance and customer quality of service will be provided that detail email availability and enable an enterprise strategy for service level agreements (SLAs).

## 1.6 (U) ACRONYMS, KEY TERMS, AND REFERENCES

(U//FOUO)Acronyms and key terms used in this document are contained in Appendices A and B.  Required and related publications and prescribed and referenced forms are listed in Appendix C.

# 2 (U) SPIRAL 1 ROLES AND RESPONSIBILITIES

## 2.1 (U) ARMY CHIEF INFORMATION OFFICER /G6

(U//FOUO) The CIO/G-6 is responsible to the Secretary of the Army and to the Chief of Staff of the Army for all Information Technology activities of the Department of the Army. The CIO/G-6 acts as the system owner and proponent by validating operational and functional requirements for IT services, providing initial lifecycle development and sustainment through replacement costs of these services, as well as funding deployment and operations of these services.

(U//FOUO) From a managed service provider perspective, CIO/G-6 activities include:

a. Provide Army policies.
b. Establish Army operating rules and guidelines.
c. Provide enterprise level resources (funds).
d. Control the Decision Point to conduct Spiral 2 of the EMCS initiative.

## 2.2 (U) PROGRAM MANAGER ARMY KNOWLEDGE ON-LINE (PM-AKO)

(U//FOUO) PM–AKO is the product developer and integrator for the intended EMCS acquisition. PM-AKO will work with CIO/G-6 and the 9th and 7th Signal Command to consolidate operational and functional requirements to provide necessary capabilities within the delivered service.

(U//FOUO) Within PM-AKO, the Product Manager for Area Processing Centers (PdM APC) will:

a. Provide overall project oversight and responsibility for the migration process.
b. Develop the EMCS interface requirements.
c. Serve as the enterprise material developer for design and development of EMCS capabilities.
d. Integrate future Global Network Enterprise Construct (GNEC) initiatives with enterprise business systems including Army Knowledge Online, Windows Server and Exchange migration, and others as appropriate.
e. Provide engineering support relative to GNEC messaging systems design and deployment.
f. Establish and manages integration of the EMCS Global Address List and the Joint Enterprise Directory Service (JEDS).
g. Implement interfaces for the GNEC environment.
h. Ensure all migration tools, software systems and scripts are approved (CoN, ATO…etc).
i. Provide a list of credentialed individuals from the EMCS provider that will have Top Level OU elevated privileges to support migration tasks.

j. Provide for the establishment and implementation of the Army Tier 1 Enterprise Service Desk.

## 2.3 (U) ENTERPRISE SERVICE DESK

(U//FOUO) The Enterprise Service Desk allows for the widest window of coverage using the most efficient level of staffing. It leverages the skills of customer-centric analysts to log, categorize, prioritize, and in some cases resolve incidents; thus freeing the more technically focused Tier II help desk from routine issues. Army business users also benefit from having a "single point of contact" to report problems, ask questions, request information, and provide feedback. The ESD will:

a. Ensure a representative is on site for the acceptance meeting conducted after migration is complete. This individual will assist the local NEC staff with initial calls to the ESD for email support.
b. Accept responsibility for Tier 1 Help Desk issues after installation migration is complete.

## 2.4 (U) 9TH ARMY SIGNAL COMMAND

(U//FOUO) The 9th Signal Command (Army), also known at Network Enterprise Technology Command (NETCOM) establishes the standards and configuration management and is the technical Command and Control (C2) authority for the Army's messaging system. NETCOM is responsible for implementing Army IT operational and management policy as established by CIO/G-6. Consistent with these broad IT responsibilities, NETCOM is the central manager for all enterprise messaging operations. NETCOM manages and controls the system and service within operational and functional requirements and reports the status of the system as necessary to ensure nominal service levels are maintained across the enterprise.

(U//FOUO) NETCOM will:

a. Provide oversight over the execution of Managed Services and delivery for the Enterprise.
b. Ensure that the Army's consolidated active directory is the authoritative source for Army GAL information.
c. Ensure DoD enterprise naming conventions are followed.
d. Resource 7th Signal Command to execute Spiral 1 of EMCS.

## 2.5 (U) ARMY GLOBAL NETWORK OPERATIONS AND SECURITY CENTER (AGNOSC)

(U//FOUO) The AGNOSC supports Army NETOPS with status reporting, situational awareness, and operational support for the Army's portion of the Global Information Grid (GIG). The AGNOSC also provides technical direction to, and obtains status from the CONUS Network Operations and Security Center (CNOSCs) with regard to CONUS based Enterprise services. (U//FOUO) The AGNOSC:

a. Identifies, tracks, and manages all security areas relative to Enterprise messaging servers within all Army AD forests IAW current policies and procedures.
b. Directs the  CTNOSC implementation of security programs, procedures, policies, and IAVA patches concerning interconnection to Spiral 1 EMCS
c. Notifies and directs remediation actions to appropriate organizations
d. Develops and publishes technical guidance, procedures, and standards such as TECHCON Implementing Memorandums
e. Expands security monitoring and management supporting spiral 1 EMCS to Army white pages
f. Provide operational oversight and management of theaters of operation and delivery of services throughout the enterprise environment.
g. Establish NETOPs and execute oversight of managed services

## 2.6 (U) 7TH SIGNAL COMMAND (THEATER)

(U//FOUO) The Signal Command (Theater) (SC(T)) is responsible for operating, managing, and defending the LWN within theater in accordance with the Army's Global Network Enterprise Construct (GNEC). The SC(T) provides situational awareness/ Network Common Operational Picture (NETCOP), assigns restoration priorities, directs/coordinates restoration activities, and ensures compliance with NetOps policy, direction, and processes for all IT services in the theater to include managed services. The SC(T)'s major mission components are life cycle management and operation of theater LWN assets, command and control (C2) of theater NetOps, CND of the LWN, and direct and general support to NECs and deployable units (e.g., Brigade Combat Teams) stationed in the theater. The 7th Signal Command will:

a. Serve as the Army Signal Command (Theater) user proponent for the delivery of enterprise services and provide C2 for the Network Operations and Security Center during Spiral 1
b. Advise the Mail Service Provider of priorities of service. The priorities will be consistent with the ARFORGEN model and Army priorities of work.
c. Ensure the on boarding NEC Director and Principal Staff understand the procedures for migrating email accounts and follow on O&M responsibilities.
d. Ensure the on boarding NEC Director understands that security of the email system will be ensured by the Mail Service Provider during the migration process.

## 2.7 (U) CONUS THEATER NETWORK OPERATIONS AND SECURITY CENTER (C-TNOSC)

(U//FOUO) The C-TNOSC is responsible for providing the Theater Signal Commands with status reporting, situational awareness, and operational support for their portion of LandWarNet. For spiral 1 of the Army EMCS, the C-TNOSC will:

a. Execute NETOPs within the regional Domains.
b. Provide oversight of delivery of services from the Network Enterprise Centers (NECs) within their regions.
c. Provide MSP with outage information that might affect their service.
d. Receive and distribute MSP outage information to the affected AOR.
e. Coordinate the execution of spillage reports from the MSP via secure channels (SIPRNet).
f. Perform operation, management, and defense of the TCP/IP networks that provide wide area network connectivity.
g. Manage, direct and/or coordinate all resolution of all incidents and attendant restoration actions.
h. Provide situational awareness of the LandWarNet hosted applications to include performance, availability, Computer Network Defense (CND), and network perimeter security.
i. Execute a change management process to ensure the prompt and efficient handling of all changes to the operational environment while minimizing risk and impact to the delivery of service. Also, provide configuration management capability to record, maintain, store and audit changes to an asset, device, application, operating system, etc.
j. Direct and ensure backups, exercise of disaster recovery plans and disaster recovery in accordance with the Continuity of Service Plans.
k. Provide near real time reports regarding the performance of the MSP and the availability of the messaging service. Report on compliance within SLA provisions and performance.

## 2.8 (U) SIGNAL BRIGADES

(U//FOUO) Signal Brigades operate, manage, and defend a portion of the Army's IT services within the Theater. Brigades consist of multiple components to include: Regional Operation Centers (ROCs), Network Operation Centers (NOCs), and Network Enterprise Centers (NECs).

## 2.9 (U) NETWORK ENTERPRISE CENTER (NEC)

(U//FOUO) The Network Enterprise Center (NEC) is responsible for operation of the installation information technology infrastructure and is the provider of services at the installation. This includes situational reporting activities, planning and engineering, enforcement of local NetOps and IA policies, and Service Request support for installation tenants.

(U//FOUO) Prior to migration of user accounts, the NECs will:

a. Conduct C2 to assist in the provider migration effort.
b. Serve as a liaison between the customer support base and the on-site contact team.
c. Provide a dedicated primary point of contact for the MSP during migration.
d. Grant permissions to MSP and AD User Objects so the MSP can perform migration actions.

(U//FOUO) Upon completion of provider migration actions, the NECs will:

a. In conjunction with the service provider and TNOSC, coordinate and conduct Tier II touch labor support.
b. Provide support for client configuration to support connectivity to the MSP service.
c. Provide the MSP with outage information that might affect their service.
d. Receive and distribute MSP outage information to the installation users.
e. Receive and assist in spillage reporting and event handling with the MSP via secure channels (SIPRNet).
f. Ensure network throughput and capacity is sufficient to support remote mail capability.

## 2.10 (U) INFORMATION MANAGEMENT OFFICER (IMO)

(U//FOUO) The IMO is the office/individual who reports to a commander/director/chief for coordination service. It includes management oversight, advice, planning, and funding coordination of all IM/IT requirements (business and mission) for their organization. The IMO assists the commander/director/chief in effectively managing the organization’s IM/IT processes and resources that enable the organization’s business and mission processes(U//FOUO) Information Management Officers will:

a. Serve as the primary interface between the NEC and the supported organization.
b. Serve as the organization interface to the NEC for troubleshooting of IT equipment, software or process failures.

## 2.11 (U) EMAIL MANAGED SERVICE PROVIDER (MSP)

(U//FOUO) The MSP is responsible for:

a. Configuration and operation of the email service using MS Exchange 2010 in a manner that achieves or exceeds defined service levels.
b. Collaborate with TNOSC, ESD, and NEC in troubleshooting and developing solutions for email incidents.
c. Monitoring the operating status of production systems and system logs.
d. Ensuring compliance with DOD and Army security policies to include Security Technical Implementation Guides (STIG), Information Assurance

Vulnerability Management (includes IAVA reporting to the TNOSC) and computing facility security certification and accreditation.

e. Performing disaster recovery per continuity of service plan.
f. A Tier II Service Desk for resolution of email problems.
g. Maintaining a “self help” website for common email problems.  The website can be integrated into the ESD Tier-0 (Knowledge Base) if required.
h. Continually providing the C-TNOSC and ESD with current server and connection status information.
i. Execution of spillage recovery actions IAW proper policy under the direction of the C-TNOSC.
j. Providing an on-site technical representative during migration to support the migration process.
k. Providing specific guidance on how to interact with the MSP after migration is complete.  This can be a “smart book,” technical guide, procedures book, etc. but must contain the information required for the NEC to connect to the mail servers, decommission/create/request user email accounts, etc.
l. Executing a process to recover/remedy accounts that fail to migrate.
m. Begin cutover process only on an organization that has ESD deployed at their site.
n. Not departing the migration site until all required accounts have been successfully migrated to the service providers email servers.
o. As part of the design plan, creating a DRAFT CONOPS for O&M of the email system for review by stakeholders.  The DRAFT O&M CONOPS will detail how the NECs will interface with the ESD/MSP operations and maintenance of the email system.  The CONOPS will address the responsibilities and actions of all stakeholders in the O&M of the email system.

(U//FOUO) NOTE:  This is not designed to be an all encompassing list of actions provided by the MSP.  Detailed information is provided in the Performance Work Statement.

# 3 (U) CONCEPT OF OPERATIONS

## 3.1 (U) OPERATIONAL ENVIRONMENTS

(U//FOUO) The ultimate end state of the Army EMCS (Figure 1) will support users located at home station, established, and austere operational environments. Spiral 1 capabilities requirements are focused at supporting approximately 230k users in a CONUS home station based operational environment.

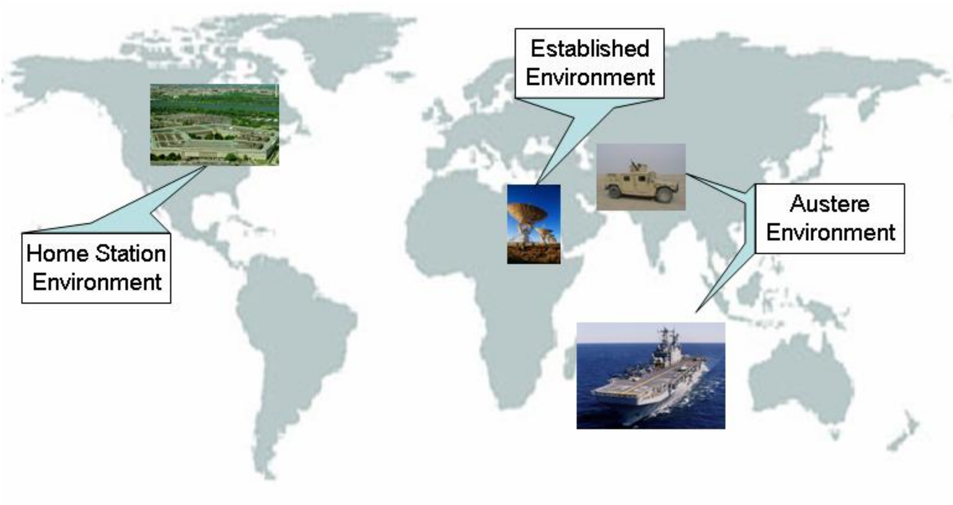

**Figure 2. (U) Depiction of Operational Environments**

### 3.1.1 (U) HOME STATION OPERATIONAL ENVIRONMENT

The home station operational environment encompasses users that operate from continental United States (CONUS) locations and strategic locations outside the continental United States (OCONUS) such as U.S. installations in Europe, Korea, and Japan. These CONUS and OCONUS locations have well-established, robust infrastructures – military forts, bases, camps, and stations, as well as other fixed national defense and intelligence facilities, such as the Pentagon.

### 3.1.2 (U) ESTABLISHED (SEMI-PERMANENT) OPERATIONAL ENVIRONMENT

The established operational environment encompasses users that operate from fixed and established operational environments outside the U.S., such as Kuwait or Bahrain. The infrastructure at these locations is constrained by limitations of the local site and hosting country, as well as geographical separation from CONUS operations, but normally consists of permanent infrastructure and connectivity.

### 3.1.3 (U) AUSTERE OPERATIONAL ENVIRONMENT

The austere operational environment encompasses users that operate from forward deployed locations, such as battle groups, forward operating bases, and other temporary locations in hostile areas (e.g., Iraq and Afghanistan), in response to events around the world. The deployed forces carry the required supporting infrastructure to all operating locations to accomplish required missions. It is imperative that forward deployed forces have the ability to operate for extended periods of time, independent of external infrastructure capabilities, and without reach-back to sustaining base support. These forces also need the ability to dynamically reconfigure assets to optimize mission operations such as shutting down non-essential communication.

NOTE: The Operational Environment paragraph and throughout this document, details the desired end-state of a consolidated email system. In this way, leaders working on Spiral 1 understand the Army's vision for the future. It in no way guarantees or is meant to imply this will be the final end-state.

## 3.2 (U) USERS

Users of the EMCS have full enterprise email capabilities. These users depend on email to perform their daily mission functions. Typically, users are active military (or reservists activated for duty/deployment), civilian employees, and designated support contractors that support U.S. Army mission operations from long-term duty locations in the home station environment. When working from their office desktop (or using a portable computer with a VPN connection), users have the option to access the Army EMCS using either a thick client application (e.g., Outlook or Entourage) or directly, using a web-browser (e.g., Internet Explorer, Firefox, or Safari). In addition, these users can access Army EMCS using a wireless handheld device (e.g., Blackberry or Windows Mobile).

## 3.3 (U) LEVEL OF SERVICE

Although the Army desires varying levels of service, especially responsiveness for senior personnel, Spiral 1 may only have a single level of service with an ability of the service desk to escalate issues for general officers and senior executive service personnel.

## 3.4 (U) MIGRATION OF USERS TO EMCS

### 3.4.1 (U) CONDITIONS

Army EMCS Spiral 1 provider will be responsible for the migration plan of users from existing Army exchange servers to the EMCS servers.

Depending on the migration plan, the Migration Team will be granted OU Admin rights for each installation requiring migration but will not receive Forest or Domain admin privileges.

There will be windows when the users/machines are available at the selected sites. Up to 24hrs in advance a standard site migration can be terminated for emergency reasons.

While the majority of the migrated clients will exist on the agreed to support baseline EMCS, the Migration Team will be prepared to deal with exceptions.

Migration reporting and help desk issues will not fall on or use the ESD. The EMCS provider will provide direct help desk for migration issues.

The 7th SC (T) will assist in the establishment of a single phone number for use by the Migration Team for onsite needs.

The Migration Team shall establish procedures for problem accounts and all lessons learned shall be incorporated into a knowledge base for use as the migration continues from site to site.

The Migration Team shall develop a plan for reverse migration should the need arise.

## 3.4.2 (U) Site Activities Concepts to be Performed by The Army

(U//FOUO) A Draft Warning Order will be issued to the Signal BDEs and the C-TNOSC at the release of the RFP. This WARNORD will identity the pilot sites and provide 14 days for the sites to answer the data call included in the Site Notification. The below steps are expected to be repeated until all sites have migrated. Stakeholders Meetings and AAR will only be conducted as necessary after the initial sites have migrated. It is expected that the overall migration timeline will decrease from site notification to site completion as the migration matures.

### 3.4.2.1 (U) PILOT SITE AND FOLLOW ON SITES

### 3.4.2.2 (U) STEP 1 - SITE NOTIFICATION (TO BE RELEASED WITH THE DRAFT MIGRATION PLAN)

The Army will issue a site notification that outlines and includes the following items:

1. Data Call (all items of information necessary for provider to understand the scope of the effort at the site, user break down by Tiers for migration (Tier 1 (Generals/SES/VIPs) and Standard users). The PILOT NEC will be given 30 days to respond to the data call. All other site NECs will be given 14 days to respond.
2. Initial Project Timeline.
3. POC list for the Migration Team, EMCS Provider and PdM APC. personnel.
4. Equipment list and software being delivered to the site.

5. On site resources required by the PdM APC the EMCS Provider and the Migration Team (office space, network drops, etc.).

### 3.4.2.3 (U) STEP 2 - STAKE HOLDER MEETING (5 DAYS AFTER RECEIPT OF DATA CALL INFORMATION FROM PILOT SITE)

1. Members include: EMCS provider, PM AKO, 7th SC (T), Pilot Site Key Stakeholders, BDE email support teams and Migration Team.
2. The purpose of the meeting is to resolve any information gaps, resource issues, and technical issues. A finalized timeline including user availability will be developed. Finalized set of procedures shall also be developed.

### 3.4.2.4 (U) STEP 3 - SITE SPECIFIC MIGRATION PLAN

The Migration Team publishes the site migration plan 30 days prior to the start of the pilot site migration. The plan will include:

1. The approved and tested tools/scripts to support migration.
2. The migration schedule for standard users.
3. The migration schedule for Tier 1 users.
4. Required TTPs, User Guides and training material.
5. Last minute changes.
6. Required Government resources.
7. Specific required subject matter expertise (e.g. Tumbleweed, DoD PKI…etc).

### 3.4.2.5 (U) STEP 4 - MATERIAL FIELDING BRIEF/MEETING (7 DAYS PRIOR TO SITE MIGRATION START)

This meeting serves as the final checkpoint before the Migration Team’s travel to the site. The 7th SC (T), BDEs and NEC will confirm that the organization is on track for the migration and all tasks and preparations have been completed in accordance with the site-specific migration plan. The NEC will provide the PdM APC and the Migration Team with a dedicated phone number for their use and the building number and location of required resources. The NEC will map users to the timeline slots provided by the site-specific migration plan.

### 3.4.2.6 (U) STEP 5 - MIGRATION TEAM ARRIVES AND BEGINS MIGRATION

### 3.4.2.7 (U) STEP 6 - PAUSE AT THE 500 ACCOUNT MIGRATION POINT

After the first 500 user accounts are migrated at each site there will be a pause and customer feedback will be gathered by at least 10% of the migrated users. Once the feedback is collected and organized, a meeting between the 9th SC (A), 7th SC (T), BDE, NEC, PdM APC, and the Migration Team will occur to assess the data. The decision to continue migration will be made if the migration is viewed as successful. If the migration of the 500 users is not successful, the PdM APC will provide guidance as to a way ahead.

#### 3.4.2.8 (U) STEP 7 CONTINUE MIGRATION

During migration the following reports shall be provided to the PM, 7th SC (T) and the NEC.

a. Planned versus Execution of migration
b. Trend analysis of issues
c. User created issues (top 5 items)
d. NEC created issues (top 5 items)
e. Provider created issues (top 5 items)
f. Unknown issues (top 5 items)

The trend data will provide real time feedback and recommendations for changes to the migration guide, future plans and the ESD call trees used to assist with the O&M tasks.

#### 3.4.2.9 (U) STEP 8 MIGRATION COMPLETION

The 7th SC (T) as described in the Material Fielding regulations shall conduct a formal acceptance. The provider will be required to remove all tools or scripts used for the migration. 7thSC (T) reserves the right to verify that no trace is left. If applicable, 7th SC (T) will issue guidance on the disposition of the existing exchanges servers. The CTNOSC will provide input to the acceptance decision based on the reporting/performance of the provider with respect to migration and service to the users migrated.

#### 3.4.2.10 (U) PILOT AAR

Upon completion of the PILOT site, an AAR will be conducted with all key stakeholders. All issues and process changes will be discussed and a final timeline for future migrations shall be presented and agreed to. A back brief will be provided to 9th SC and the CIO/G6 Senior leadership.

## 3.5 OPERATIONS AND MAINTENANCE OF EES

### 3.5.1 (U) CONOPS

A DRAFT CONOPS for O&M will be published by the provider as part of the design plan. The DRAFT CONOPS will be reviewed by 7th Signal Command (T) and associated Stakeholders for acceptance into the final plan for delivery of additional services.

### 3.5.2 (U) LEVEL OF SERVICE

Army EMCS Spiral 1 shall function as a MAC II capable system. (U) Upgrades of Storage

The monitoring of the mail box storage capability is reported in accordance with the performance management plan and SLA established for the program. It is expected that communications between the EMCS provider and the CTNOSC will facilitate proactive management of the EMCS for its users. The elevation of the average mailbox size storage limit is tightly controlled by the 7th SC (T) and the PM AKO for EMCS.

### 3.5.3 (U) ENTERPRISE SERVICE DESK

(U//FOUO) A centralized Army Enterprise Service Desk (ESD) provides the first level of service to all enterprise email users across the Army community to ensure quality service delivery to all Army users, at all levels, and across all operational environments. The ESD monitors the system and provides the supported user base with the status of email services:

- The focal point for enterprise email operations and decisions involving service and restoration priorities and the first tier of Army customer support.
- Support on a 24 x 7 basis where all users are able to contact the ESD via a single phone number, a web form, live chat, or email to report all problems or inquiries related to the service.
- A user “self-help” web site.
- A disciplined process to receive customer contacts, catalog all requests in a centralized database, and resolve issues as appropriate.
- A mechanism to elevate unresolved trouble calls to the system administration response team.

The ESD provides for common policies, tools, and training related to email and enhances the ability to comply with security auditing and reporting requirements. A centralized ESD provides for a dramatic reduction in the number of service desk personnel distributed around the globe. Where a physical presence is required (primarily hardware related and life-cycle maintenance) local NECs perform component replacement and on-site support to respond to service requests and system problems that cannot be resolved remotely by the ESD center.

The current ticketing system for the ESD is ITSM/Remedy and CA. The EMCS provider should use tools to minimize or eliminate any swivel chair operations to allow for trouble ticket tracking and resolution and archiving and seamless communications between the ESD and the EMCS provider. The EMCS will have the tools required to integrate into the ESD objective ticketing system.

The EMCS shall provide a Tier 2 service desk in order to solve mail related issues that are above the ESDs capabilities. It is desirable for the EMCS Provider to coordinate with the ESD and provide troubleshooting guides to support maximum possible first call resolution by the ESD. Also the EMCS Provider will have web based troubleshooting guides or tools available to the users, IMOs at the organizations and NECs for locations migrated to the EMCS.

## 3.6 (U) ENTERPRISE EMAIL ADMINISTRATION

### 3.6.1 (U) ACCOUNT PROVISIONING/DE-PROVISIONING

The Army EMCS uses the enterprise identity management service and the DoD Enterprise Username. The Army EMCS GAL is not the authoritative source for attributes in the enterprise email directory. The primary method of provisioning and de-provisioning an enterprise email account is automated and is initiated by Army processes. The secondary method is manual provisioning and de-provisioning of the email account by an enterprise administrator. In the case of manual provisioning and de-provisioning (such as a group mailboxes) the "user" is vetted by a standard process.

Military members and Army Civilian member are provisioned with an account when required by their position.

### 3.6.2 (U) CONTRACT PERSONNEL

Personnel employed by the Army under contract will be provisioned with an account upon the start of work under an Army contract (that requires email). Contract personnel will retain their account only for the duration of their contract.

### 3.6.3 (U) GROUP/ROLE BASED MAILBOXES

The Army EMCS provides mailboxes with names that are based on an organizational group and mailboxes that are based on a role. For example, a particular command may want an organizational (or group) mailbox which several people have permission to read and action the emails that arrive in that mailbox. There are also operational instances where a particular role or "position" must have a mailbox which several people must be able to both read and send as in order to accomplish the mission. An example of this is a battle captain or watch officer.

The request and approval process for these mailboxes will be defined by the CIO/G-6 and executed IAW procedures to be released in a future Technical Authority Implementation Memorandum. The Army Operations Oversight Board will create an approval board (the Army Email Change Management Approval Board) for group and resource mailbox requests. Consideration from an organizational operations (S3/G3) element for support and service will define an organizational requirement. Determination concerning whether this is a baseline service is still being researched and will be documented in a process defined by the CIO/G-6 and executed IAW procedures to be released in a future Technical Authority Implementation Memorandum.

### 3.6.4 (U) RESOURCE MAILBOXES

Requests for creation of a resource mailbox (e.g. conference room calendar or shared vehicle calendar) will be approved by the first O-6 in the chain of command, and will then flow through the Enterprise Service Desk to the Email Service Desk for implementation. Requests for creation of a distribution list must identify the individual(s) who will be responsible for managing that resource mailbox (i.e. receiving/responding to requests for the resource).

### 3.6.5 (U) DISTRIBUTION LISTS

Requests for creation of a distribution list will be approved by the first O-6 in the chain of command, and will then flow through the Enterprise Service Desk to the Email Service Desk for implementation. Requests for creation of a distribution list must identify the individual(s) who will be responsible for managing that distribution list (i.e. adding/removing membership in the list).

### 3.6.6 (U) NAMING AND ADDRESSING

#### 3.6.6.1 (U) MAILBOXES WITHIN THE ENTERPRISE SYSTEM

The Army EMCS uses an underlying email domain name that is applicable to all users (e.g. @mail.army.mil) however each of the military services uses an aliased email domain name for their service (e.g. @us.army.mil, @navy.mil, etc) mailboxes in deployed organizations.

The Army EMCS will comply with the provisions listed in ALARACT 021-2010 with regard to naming conventions and mailboxes.

An intent of enterprise email is to provide a single email address for soldiers, no matter where they are, whether deployed or not. The enterprise email system will be configured to forward mail to tactical Exchange servers for those users who are getting service from a tactical unit’s Exchange server. In order to retain the appearance of a single email, the Exchange servers of deployed and tactical forces must be properly configured. Specific configuration details will be defined by the CIO/G-6 and executed IAW procedures to be released in a future Technical Authority Implementation Memorandum.

### 3.6.7 (U) SYSTEM ADMINISTRATION

The Army EMCS employs a centralized system administration function that operates twenty-four hours per day, seven days a week. The System Administration function spans both the enterprise data center network and the distributed nodes at the tactical edge. The use of a single email service:

- Greatly reduces diverse breadth of knowledge required for effective email system administration relative to that required to sustain multiple disparate organizational email systems.
- Allows for increased depth of expertise through enterprise-wide focused training and certification programs.

- Significantly reduces the number of system administrators required to support the Army enterprise.

While centralized enterprise email system administration has many advantages, it presents some continuity of operations challenges. The following enterprise email actions mitigate continuity of operations risks:

- Establish safeguards to protect from inadvertent and malicious damage;
- Establish a rigorous vetting process to select system administrators;
- All email administrator accounts will be configured/provisioned with a smart card, and accessed only using smart card authentication.
- Require system administrators to meet increased training and certification levels;
- Allocate roles and functions to ensure redundancy, i.e., ”second set of eyes” for critical operations;
- Increase restricted access and limit authorizations – no single system administrator has total access or is authorized to perform all functions; and
- Enhance monitoring and recording of system administration actions.

### 3.6.8 (U) NETOPs Oversight AND SITUATIONAL AWARENESS

Currently, the Army’s ITSM is BMC ITSM (Remedy 7.6) and CA Unicenter, used by the AGNOSC and TNOSCs. The Enterprise Email Managed Service Provider is encouraged to identify, and eventually implement, an optimum approach for interoperation between their ITSM and the Army’s ITSM. This will allow the ESD to seamlessly interface with the email service provider. As stated in 3.5.8, the EMCS provider should use tools to minimize or eliminate any swivel chair operations to allow for trouble ticket tracking and resolution, and archiving and seamless communications between the ESD and the EMCS provider.

### 3.6.9 (U) INDIVIDUAL TRANSFER/DEPLOYMENT

The Army EMCS has administrative tools that enable user mailboxes to easily and quickly move to accommodate user transfers and deployments. An individual transfer and/or deployment is a simple process whereby a user’s email moves from an email server in one location to another email server in a different location (i.e. different data center) that is more efficient for network access because the user has physically relocated. This mailbox move is accomplished by central system administrators and is invisible to the average user. The Enterprise Email Managed Service Provider will provide a method in which user email data stores can me migrated/moved between forests or individual enclaves as necessary.

### 3.6.10 (U) ORGANIZATIONAL DEPLOYMENT

In the same fashion as individual transfers, the Army EMCS has administrative tools that enable the transfer (and pre-positioning) of groups of user mailboxes to easily and quickly move to accommodate organizational deployments. When a remote node is required (for the organization), mailbox information must be copied/pre-positioned onto the remote node to minimize WAN bandwidth consumption upon re-connection and synchronization. When an organization is deploying and requires the stand up of their own remote node with copied/pre-positioned mailbox information, the 7th Signal Command will work with the MSP (and the PdM APC) to coordinate the transfer of data.

## 3.7 (U) ARCHITECTURE

(U//FOUO) The architecture for the ultimate end state Army EMCS (Figure 2) includes an enterprise data center network, Wide Area Network (WAN), and distributed nodes that extend enterprise email to the tactical edge. The architecture must provide email service for all types of users across all operational environments. The architecture is configured to link the sustaining base to the tactical edge, and optimized for conducting joint and interagency operations. Data centers work as a synchronized enterprise email capability to optimize user responsiveness. As mentioned above, Spiral 1 is expected to support only CONUS based users.

### 3.7.1 (U) EMAIL PROCESSING NODES

(U//FOUO) In the ultimate end state of Army enterprise email, there will be four types of email processing nodes However, Spiral 1 only consists of enterprise processing nodes and correct configuration to support forwarding to tactical processing nodes. It is expected there will be two enterprise processing nodes located in CONUS. The managed service provider is not responsible for any operation of email in tactical processing nodes; however they will be responsible for ensuring that the managed service is correctly configured to allow the forwarding of email for users in those nodes.

#### 3.7.1.1 (U) ENTERPRISE PROCESSING NODES

(U//FOUO) Enterprise Processing Nodes are data centers, located either in Defense Enterprise Computing Centers ((DECCs) or in commercial facilities that meet DoD security requirements and are services by an Army Top Level Architecture (TLA) stack.

#### 3.7.1.2 (U) INSTALLATION PROCESSING NODES

(U//FOUO) Installation Processing Nodes (IPNs) are operated in Army data processing centers and are logical extensions of the Area Processing Centers. These are located on large bases and exist to minimize WAN traffic. IPNs are not part of the Spiral 1.

#### 3.7.1.3 (U) REMOTE INSTALLATION PROCESSING NODES

(U//FOUO) Remote IPNs are also operated in Army data processing centers, but are located on remote bases that have limited connectivity. Remote IPNs exist to minimize the impact of the limited connectivity by reducing WAN traffic. Remote IPNs are not a part of Spiral 1.

### 3.7.2 (U) TACTICAL PROCESSING NODES (DISTRIBUTED NODES AT TACTICAL EDGE)

Enterprise email users in the austere operational environment at the tactical edge must be equipped to continue their mission functions when disconnected from the WAN. .Tactical Processing Nodes are operated by Brigade Combat Teams (BCTs), other Army brigades, or higher level Army organizations for the purposes of retaining local functionality, and the nodes move with the brigade from training to deployment and back. Local authentication and directory services will be used when a distributed node is operating in disconnected mode. Each tactical processing node has a local email server that:

- Operates in “stand-alone” mode when disconnected from the WAN.
- Preserves full enterprise email functionality among tactical edge users at disconnected nodes.

When deployed, tactical edge user mailboxes move to the tactical processing node servers supporting the deployed users. The Army EMCS will be configured to allow users to forward email to the deployed node so that there is no need to change the primary email addresses of deployed users.

### 3.7.3 (U) ACCESS METHODS

#### 3.7.3.1 (U) THICK CLIENT METHOD

Users can access the Army EMCS using a thick client application (Outlook 2007 or newer, or Entourage) on their desktop. This access method enables users to experience all available functionality and operate in cached mode so they can still access email and calendars locally when disconnected from the WAN.

#### 3.7.3.2 (U) WEB CLIENT METHOD

Users can access the Army EMCS using a web browser (e.g., Internet Explorer, Firefox, Safari) when connected to the appropriate network (NIPRNet or SIPRNet).

#### 3.7.3.3 (U) WIRELESS HANDHELD DEVICE METHOD

Users can access the Army EMCS using Army issued/approved wireless handheld devices (e.g., Blackberry, Windows Mobile). Wireless access is more limited than the web client.  Since there are two main handheld devices – one operating in a push delivery method and the other operating in a pull method – offline access is determined by the delivery method as well as the type of device used.  Wireless handhelds must have the capability to sign and encrypt/decrypt email messages.

## 3.8 (U) INTERDEPENDENCE

The Army EMCS relies on DoD and interagency capabilities to maximize complementary and reinforcing effects while, at the same time, minimizing vulnerabilities.  Key enablers for the Army EMCS are identity management (including Public Key Infrastructure (PKI)) and security services, authoritative directory services, and the Global Information Grid (GIG).

## 3.9 (U) ENTERPRISE EMAIL SERVICE

The Army EMCS supports the Army enterprise by enabling the exchange of information required to keep commanders and leaders informed worldwide and achieve the information advantage.  It  is an important medium used to exchange information among those supporting and executing the U.S. Defense missions.  The Army EMCS enables the following key operational capabilities:

- Discovery – users can use enterprise directory services to easily discover the contact information for anyone in the Army enterprise.
- Ubiquitous Access – users have the ability to access their enterprise email from any terminal attached to the DoD network in any operational environment without loss of features or service level (using PKI certificate authentication); and from their Army laptop/wireless handheld device when traveling.
- Stable Contact Information – user contact information is available and accurate so that users can quickly and easily contact others that have information or knowledge required to solve a problem.

### 3.9.1 (U) MESSAGE GENERATION, EXCHANGE, STORAGE, AND SEARCH

The Army EMCS provides standard email functionality to include sending, receiving, storing, and archiving messages to ensure compliance with an enterprise document/record management system; transporting multi-media file attachments and rich text; accessing contact information for all Army users regardless of location; and performing full text search of email messages and attachments.  The Army EMCS requirements are specified in the Army Enterprise Email Requirements Specification Spiral 1, Version 2.0, dated 7 December 2009.

### 3.9.2 (U) ARMY GLOBAL ADDRESS LIST

The Army EMCS provides a global address list (GAL) that contains all Army non-sensitive personnel and shared resources.  The GAL must use standard, consistent metadata for naming conventions, be easy to use, and support distribution lists. Specific GAL requirements are specified in the Army Enterprise Email Specification Spiral 1. The managed service provider takes authoritative data from the Army's AD forests (via EDS-Lite) and provides it to the GAL.

### 3.9.3 (U) GLOBAL CALENDARING

The Army EMCS provides calendaring capabilities to include enterprise-wide sharing of individual, organization, and resource calendars. Specific global calendaring requirements are identified in the Army Enterprise Email Requirements Specification for Spiral 1. When the Army migrates to Exchange 2010, the MSP will federate its Exchange with the Army to allow cross-forest visibility of calendars.

### 3.9.4 (U) TASK MANAGEMENT

The Army EMCS provides task management capabilities to include creating, editing, deleting, sorting, and grouping tasks, as well as displaying task deadlines within the calendar. Specific task management requirements are identified in the Army DoD Enterprise Email Requirements Specification for Spiral 1.

### 3.9.5 (U) SECURITY FEATURES

The Army EMCS provides security capabilities to include the ability to sign and encrypt messages and attachments; perform email classification markings in accordance with DoD security policies; and filter email transmissions. Specific security requirements are specified in the Army Enterprise Email Requirements Specification for Spiral 1.

### 3.9.6 (U) SECURITY / MISSION ASSURANCE

The Army EMCS is envisioned to be an essential U.S. National, Defense, and Intelligence asynchronous communication capability. Therefore, it is imperative that no potential adversary is capable of disabling the Army EMCS or exploiting the service in order to deceive. The Army enterprise email architecture includes distributed data centers that are configured with no single point of failure or vulnerability – human, physical, network, or technology. Robust continuity of operations plans (COOP) and disaster recovery plans are in place. The Army EMCS is configured to preclude any potential adversary from intruding on national Army email communications or inflicting any harm by Army EMCS exploitation. Army EMCS transmissions and data at rest are secure and protected against any unauthorized access.

#### 3.9.6.1 (U) POLICY AND GPO IMPLEMENTATION

The Army sees value in retaining the ability to implement policy and GPOs on its schedule however, the Army also understands the need to implement controls on policy implementation. The EMCS and the government will develop a "GPO implementation schedule", based on geographical time, in order to implement GPOs within 24 hours of receipt, but to implement those only during the times that will have the least operational impact, unless the government directs immediate implementation due to a severe security risk. Most policies, such as the requirement to edit using plain text format and a policy to enforce editing in plain text only, will be determined by the AGNOSC.

#### 3.9.6.2 (U) FILTERING AND IRONPORTS

The Army will operate Ironport devices at the routing hubs in order to ensure consistent filtering across the CONUS, and provide anti-spam services for email into and out of CONUS Exchange. The filtering rule sets will be routinely provided by the AGNOSC. Changes to the filtering rule sets will be approved by the AGNOSC IAW Technical Authority Implementation Memorandum TA 2006-003, 15 Sept 2009.

#### 3.9.6.3 (U) MAIL RELAYS AND ROUTING HUBS

Mail relays and routing hubs will be operated by the Army. All email inbound email will traverse Exchange Routing Hubs, all outgoing email from the enterprise email servers will traverse the Routing Hubs.

#### 3.9.6.4 (U) DNS

The Army CONUS TNOSC will manage the DNS records for the enterprise email system. The managed service provider will coordinate with the CTNOSC for any changes as they are required.

### 3.9.7 (U) GOVERNANCE

Army governance structure is employed for enterprise email and other enterprise information services. Consistent with DoD and IC policy, this governance structure consists of a governance board whose membership includes senior leadership from Office of the Secretary of Defense, Director of National Intelligence, IC Agencies, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, and Defense Agencies (hereafter referred to collectively as the “DoD Components”). Consumers of enterprise services are represented in the governance structure.

The Army governance structure addresses DoD enterprise email requirements, architecture, services determinations, and service level agreements in coordination with the Executive Agent (EA) for the Army EMCS. The EA is established to execute Army EMCS day-to-day operations with oversight by the Army enterprise service governance structure, consistent with other Army enterprise information services. The EA addresses unresolved issues with the Army EMCS governance board.

The governance structure is supported by the DoD Rate Management Council (RMC), which identifies the fair method of cost sharing by determining the cost per user based on the level of service and type of access.  For example, guest users are essentially "web" users and do not have the entire capability of standard users, so per seat cost is adjusted appropriately.  Additionally, some organizations have many remote nodes and the administration burden (training, operations, and life cycle replacement) for those nodes adds a greater cost, which factors into the final rates determined by the DoD RMC.

# 4 (U) SUMMARY

The current environment has inherent deficiencies that can be corrected by implementing enterprise-wide information services. Implementing an enterprise email service with over 5 million users extending across the DoD enterprise from the sustaining base to the tactical edge is a massive undertaking. Executive leadership is committed to the challenge and has provided direction to move forward with Spiral 1 of the implementation of an enterprise email service. Implementation involves an aggressive timeline. The Spiral 1 implementation will be closely followed by Army leadership and will assist in making a decision for an expanded implantation of EMCS. The CONOPS described in this document is needed to guide the consolidation of the many current email systems into a single enterprise email service, that when implemented, will deliver high mission value. In summary, Army EMCS:

- Improves mission effectiveness by providing seamless messaging capabilities built upon common, standard, and unified enterprise services.
- Improves security by eliminating the vulnerability among the many disparate domain mail systems.
- Produces large cost savings by providing a unified solution that consolidates and streamlines email implementation and administration across the Army enterprise.

# APPENDIX A - (U) ACRONYMS

(U) This appendix is **UNCLASSIFIED**.

| | |
|---|---|
| CONOPS | Concept of Operations |
| CONUS | Continental United States |
| COOP | Continuity of Operations Plans |
| DoD | Department of Defense |
| EA | Executive Agent |
| EMCS | Enterprise Email Service |
| EMCSD | Enterprise Email Service Desk |
| FOC | Full Operational Capability |
| FY | Fiscal Year |
| GAL | Global Address List |
| GIG | Global Information Infrastructure |
| IC | Intelligence Community |
| IOC | Initial Operational Capability |
| JP | Joint Publications |
| JWICS | Joint Worldwide Intelligence Communications System |
| NIPRNET | Unclassified but Sensitive Internet Protocol Router Network |
| NSA | National Security Agency |
| OCONUS | Outside Continental United States |
| PKI | Public Key Infrastructure |
| RMC | Rate Management Council |
| SIPRNET | Secret Internet Protocol Router Network |
| US | United States of America |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

# APPENDIX B - (U) GLOSSARY

(U) This appendix is **UNCLASSIFIED**.

- **Architecture:** the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. **[DoD Integrated Architecture Panel, 1995, based on IEEE STD 610.12]**
- **Cyber Attack:** is the use of computers and the Internet in conducting warfare in cyberspace. **[WEB]**
- **Cyberspace:** A global organization within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. **[Joint Publication 1-02, DOD Dictionary of Military and Associated Terms]**
- **Data Center:** A facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. **[WEB]**
- **Deployment:** The relocation of forces and materiel to desired operational areas. Deployment encompasses all activities from origin or home station through destination, specifically including intra-continental United States, intertheater, and intratheater movement legs, staging, and holding areas. See also deployment order; deployment planning; prepare to deploy order. **[Joint Publication 1-02]**
- **Distribution List:** A facility in electronic mail systems to enable a large number of subscriber mail addresses to be reached through a single (list) name. **[WEB]**
- **Organization:** A organization is the main subdivision of internet addresses, the last three letters after the final dot, that indicate an organizational affiliation. Some top-level organizations widely used are: .com (commercial) .edu (educational), .net (network operations), .gov (US government), .mil (US military) and .org (organization). **[WEB]**
- **Organization Name:** The unique name that identifies an Internet site. Organization Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. A given machine may have more than one Organization Name but a given Organization Name points to only one machine. **[WEB]**
- **Email:** Mail composed and transmitted on a computer system or network. **[WEB]**

- **Enterprise:**
  - A unit of economic organization or activity; *especially***:** a business organization. **[WEB]**
  - For the purposes of the DoD/Intelligence Community AATT, the *enterprise* consists of the Intelligence Community, DoD, and their partners. **[AATT, 24 June 08]**
- **Environment**: Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IS. **[CNSSI-4009]**
- **File Attachment:** A binary file attached to a text message (e.g., word document file, PowerPoint file, excel spreadsheet file, picture file). **[WEB]**
- **Identity Management:** The act of registering identities and issuing, maintaining, and revoking globally unambiguous, assured identifiers for human and non-human subjects (e.g., individuals, organizations, work roles, COIs, devices, and automated processes). Identity management is performed in a federated manner. Subjects will exchange and must reliably interpret federated identifiers; therefore, identifiers must be defined and communicated according to open standards. Identity Management is fundamentally integrated with Credential Management, the ESM capability where identity proofing is performed. **[ESM]**
- **Global Address List:** A directory that contains entries for every group, user, and contact within an organization's implementation of email. **[WEB]**
- **Global Information Grid:** The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. Also called GIG. See also grid; information. **[Joint Publication 1-02]**
- **Node:** In communications and computer systems, the physical location that provides terminating, switching, and gateway access services to support information exchange. **[Joint Publication 1-02]**
- **Provisioning:** The process of providing users with accounts, the appropriate access to those accounts, all the rights associated with those accounts, and all of the resources necessary to manage the accounts. **[WEB]**
- **Service:** A mechanism to enable access to one or more capabilities. **[AATT]**
- **Tactical Edge:** The environment in which US forces directly engage adversaries (e.g., Iraq, Afghanistan).
- **Thick Client:** A user computer that host applications (e.g., Outlook) using the machines internal processing and storage capacity. **[WEB]**

- **User:**
    - A person, organization entity, or automated process that accesses a system, whether authorized to do so or not. **[RFC 2828]**
    - Individual or process authorized to access an IS. **[CNSSI-4009]**
    - (PKI) Individual defined, registered, and bound to a public key structure by a certification authority. **[CNSSI-4009]**

- **VPN Connection:** A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. **[WEB]**

- **WEB-browser:** A software application that allows for the browsing of the World Wide Web. **[WEB]**

- **Wide Area Network:** a computer network that spans a large geographical area. **[WEB]**

# APPENDIX C - (U) REFERENCES

(U) This appendix is **UNCLASSIFIED**.

- *The 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA)*
- The 9/11 Commission Report
- Executive Order 13311, *Homeland Security Information Sharing*, July 29, 2003
- Executive Order 13356, *Strengthening the Sharing of Terrorism Information To Protect Americans*, August 27, 2004
- Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October 25, 2005
- The 2005 National Intelligence Strategy
- National Security Strategy
- Quadrennial Defense Review Report
- DoD Directive (DoDD) 8500.01E, *Information Assurance (IA)*, Issued October 24, 2002 and Certified Current as of April 23, 2007
- DoD Instruction (DoDI) 8520, *Public Key Infrastructure (PKI) and Public Key Enabling (PKE),* October 7, 2003
- Assistant Secretary of Defense for Networks and Information Integration and DoD Chief Information Officer and Associate Director of National Intelligence, Chief Information Officer Memorandum, "Department of Defense (DoD) and Intelligence Community (IC) Commitment to an Interoperable Services-Based Environment," July 13, 2007
- The Director of ODNI's *500 Day Plan for Integration and Collaboration*
- JP 3-0 Joint Operations (Available at http://www.dtic.mil/doctrine/jpcsystemsseriespubs.htm.)
- JP 6-0 Doctrine for Communications System Support to Joint Operations (Available at http://www.dtic.mil/doctrine/jpcsystemsseriespubs.htm.)
- Net-Centric Environment Joint Functional Concept (Available at http://www.dtic.mil/futurejointwarfare/jfc.htm.)
- Net-Centric Operational Environment Joint Integrating Concept (Available at http://www.dtic.mil/futurejointwarfare/jic.htm.)
- Protection Joint Functional Concept (Available at http://www.dtic.mil/futurejointwarfare/jfc.htm.)

- Military Support to Stabilization, Security, Transition, and Reconstruction Operations Joint Operating Concept (Available at http://www.dtic.mil/futurejointwarfare/joc.htm.)
- Joint Command and Control Joint Functional Concept (Available at http://www.dtic.mil/futurejointwarfare/jfc.htm.)
- Irregular Warfare Joint Operating Concept (Available at http://www.dtic.mil/futurejointwarfare/joc.htm.)
- Homeland Defense and Civil Support Operations Joint Operating Concept (Available at http://www.dtic.mil/futurejointwarfare/joc.htm.)
- DoD Enterprise Email Tiger Team (EETT) Requirements Specification, Version 1.1, 2 August 2008 (Available at https://www.intelink.gov/inteldocs/view)
- DoD Enterprise Email Tiger Team (EETT) Report-out Brief, September 18, 2008 (Available at https://www.intelink.gov/inteldocs/view.php?fDocumentId=72534.)
- ONEmail Implementation Tiger Team Final Report