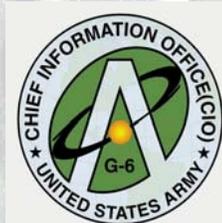


Headquarters Department of the Army



The Army Knowledge Management Implementation Plan

1 September 2003



Prepared by:

Office of the Army Chief Information Officer/CIO

FOREWORD

America's Army is continuing its transformation journey to maintain its global military prowess in the 21st Century. In August 2001 we published the initial Army Knowledge Management Strategic Plan that codified our vision for becoming a network-centric, knowledge-based force and identified the Army's goals for achieving that vision. Our vision:

"A transformed Army, with agile capabilities and adaptive processes powered by world class network-centric access to knowledge, systems, and services, interoperable with the joint environment."

Much has been accomplished in less than two years - the power of network-centric, knowledge-based operations has been demonstrated on the battlefield; new organizations have been stood up and are now operational; the culture has started to change to collaboration, teamwork, innovation, and enterprise processes; however, much remains to be done. This AKM Implementation Plan identifies the current actionable initiatives and tasks that will be undertaken in support of our AKM vision, goals, and objectives.

This Plan is divided into two parts. The first part identifies those remaining "Critical Enablers" necessary to achieve our vision for becoming a network-centric, knowledge-based force. The initiatives identified in Part 1 will be monitored by the Director of the Army Staff (DAS) with the full support of the Army Audit Agency as part of the overall reorganization effort of the Army. These initiatives are in total support of the direction being taken with the ongoing DOD Transformation efforts, the President's Management Agenda, and the new roles and organizations being established to support Homeland Security and Critical Infrastructure Protection.

Part 2 – Irreversible Momentum - identifies those initiatives supporting our overall AKM strategy that fall under the purview of the Army Chief Information Officer (CIO)/G-6 with the full support of the Army CIO Executive Board.

This plan is aggressive and requires us to accomplish tasks inside of our normal resourcing and documentation windows. We need your continued advocacy, support and commitment to implement this plan.



John M. Keane
General, United States Army
Vice Chief of Staff

TABLE OF CONTENTS

EXECUTIVE SUMMARY	ES-1
INTRODUCTION	I-1
1.0 PRIORITIES	I-1
2.0 REFERENCES	I-2
3.0 AKM STRATEGIC GOALS	I-3
4.0 COORDINATING OFFICIAL AND POINTS OF CONTACT.....	I-3
PART 1 – CRITICAL ENABLERS FOR THE FUTURE.....	1-1
1.0 NETWORK-CENTRIC, KNOWLEDGE-BASED DECISION SUPPORT FOR AKM IMPLEMENTATION- AKM GOALS 1 & 2.....	1-1
2.0 ENTERPRISE RESOURCING - AKM GOAL 1.....	1-3
2.1. CAPITAL PLANNING AND INVESTMENT MANAGEMENT	1-4
2.2. ENTERPRISE PORTFOLIO	1-7
3.0 ARMY KNOWLEDGE ENTERPRISE – AKM GOALS 1, 2, 3, 4 AND 5 	1-8
3.1. DOCUMENT AND EXECUTE ARMY NETOPS CONOPS - AKM GOAL 3	1-9
3.2. DEVELOP AND EXECUTE THE ARMY KNOWLEDGE ENTERPRISE ARCHITECTURE (AKEA) - AKM GOAL 1, 2, 3, 4 AND 5 	1-11
3.3. ARMY ENTERPRISE INFOSTRUCTURE - TRANSPORT (AEI-T) - AKM GOAL 3	1-18
3.4. Foster the growth of an Enterprise Knowledge Base - AKM GOALS 2, 3, AND 4	1-25
3.4.1. Transform Army Processes End-to-End - AKM Goals 2, 3, and 4 	1-25
3.4.2. Consolidate and Webify Applications - AKM Goals 2 and 4....	1-28
3.4.3. Functional Processing Centers – AKM Goal 3.....	1-31

3.5. SUPPORT STRATCOM CNO AND FULLY IMPLEMENT IA DEFENSE IN DEPTH – AKM GOAL 3.....	1-33
3.5.1. Protect the Army’s Portion of the GIG from Cyber Attack – AKM Goal 3	1-33
3.5.2. Support STRATCOM and Computer Network Operations (CNO) - AKM Goal 3.....	1-36
4.0 ENTERPRISE ENGINEERING SUPPORT TO AKE – AKM GOAL 3	1-38
4.1. CORE ENTERPRISE ENGINEERING SUPPORT – AKM GOAL 3 	1-38
4.2. CENTRAL DESIGN ACTIVITY DIVESTITURE – AKM GOAL 3...1-40	
5.0 AKM TRANSFORMATION TO SUPPORT OBJECTIVE FORCE - AKM GOAL 1, 2, 3, 4 AND 5.....	1-42
5.1. SUPPORT OF HOMELAND SECURITY MISSIONS – AKM GOALS 1, 2, 3, 4, AND 5.....	1-42
5.2. ANALYSIS OF SIGNAL FORCE STRUCTURE – AKM GOAL 3 .1-44	
5.2.1. Building the Interim Signal Force (TAA-11).....	1-44
5.2.2. Building the Objective Signal Force	1-48
5.3. INTEGRATE THE ARMY RESERVE/ARMY GUARD INTO THE AKE – AKM GOAL 1 AND 3.....	1-50
5.3.1. Integrate the Army Reserve	1-50
5.3.2. Integrate the Army Guard	1-52
PART 2 – IRREVERSIBLE MOMENTUM	2-1
1.0 GOAL 1 - ADOPT GOVERNANCE AND CULTURAL CHANGES TO BECOME A KNOWLEDGE-BASED ORGANIZATION	2-1
1.1. AKM CAPABILITY MATURITY MODEL.....	2-1
1.2. RECORDS MANAGEMENT	2-3
1.3. DOIM BUDGET	2-7
1.4. MACOM AND FUNCTIONAL PROPONENT C4IM BUDGET.....	2-9

1.5. ARMY REGULATION AND POLICY REVISION.....	2-10
1.6. AKM STRATEGIC COMMUNICATIONS PLAN.....	2-12
2.0 GOAL 2 – INTEGRATE KNOWLEDGE MANAGEMENT CONCEPTS AND BEST PRACTICES TO PROMOTE THE KNOWLEDGE-BASED FORCE	2-15
2.1. KNOWLEDGE SHARING AND COLLABORATIVE PROCESSES	2-15
2.1.1. Support Communities of Practice and Collaborative Environments	2-15
2.1.2. Mitigate Risk in the Transformation to a Knowledge-based Force	2-17
2.2. IMPLEMENT WARRIOR KNOWLEDGE NETWORK.	2-19
2.3. ACHIEVE E-ARMY TRANSFORMATION.....	2-22
2.3.1. Develop the e-Army Environment	2-22
2.3.2. Transform Processes to Achieve the AKE.....	2-26
3.0 GOAL 3 – MANAGE THE INFOSTRUCTURE AS AN ENTERPRISE TO ENHANCE CAPABILITIES AND EFFICIENCIES	2-29
3.1. MISSION ONE – DEVELOP AND IMPLEMENT THE ARMY ENTERPRISE INFOSTRUCTURE	2-32
3.1.1. Installation Bandwidth Modernization.....	2-32
3.1.2. Army Enterprise Infostructure - Repository	2-33
3.1.3. Implement Enterprise Directory Services.....	2-35
3.1.4. Migration to Next Generation Desktop Operating System – Implementing Active Directory.....	2-39
3.1.5. CONUS TNOSC Consolidation.....	2-42
3.1.6. Relocation Of ANOSC To Fort Belvoir	2-43
3.1.7. Disaster Recovery And Continuity Of Operations Planning	2-44
3.2. MISSION TWO –PROVIDE OVERSIGHT AND POLICY TO THE ARMY	2-47

3.2.1.	AEI Governance.....	2-47
3.2.2.	Implement Enterprise Systems Management	2-49
3.2.3.	AEI Systems Integration	2-52
3.2.4.	Single DOIM Concept	2-53
3.2.5.	Visual Information	2-56
3.2.6.	Sub-Installation Support And Relationships.....	2-59
3.3.	MISSION THREE – REDUCE TOTAL COST OF OWNERSHIP ...	2-60
3.3.1.	Business Case Analysis.....	2-60
3.3.2.	Acquisition of IT	2-61
3.3.3.	Server Consolidation.....	2-63
3.3.4.	Enterprise Email and Web Server Strategy	2-69
3.3.5.	Commercial Activities for Completed A-76 Studies.....	2-71
3.4.	MISSION FOUR – DELIVER SECURE WEB-BASED, INTEROPERABLE, AND OPEN SYSTEMS	2-73
3.4.1.	Army Enterprise Networkiness Certification.....	2-73
3.4.2.	Data Interoperability.....	2-78
3.4.3.	Remote Services.....	2-82
3.4.4.	CAC and PKI	2-84
3.4.5.	Cryptographic (CRYPTO) Modernization Program	2-86
3.4.6.	Biometric Technologies.....	2-89
3.5.	MISSION FIVE – MOVE TO PERFORMANCE-BASED ENTERPRISE SERVICE APPROACH.....	2-92
3.5.1.	Baseline Services and Service Level Management	2-92
3.5.2.	Enterprise Support Center	2-96

4.0	GOAL 4 – INSTITUTIONALIZE ARMY KNOWLEDGE ONLINE	2-99
4.1.	SCALE AKO AND AKO-S	2-100
4.2.	LEVERAGE AKO	2-101
4.3.	SELF-SERVICE CENTER FOR NETWORKED KNOWLEDGE MANAGEMENT	2-102
4.4.	STRATEGIC READINESS SYSTEM (SRS) SCORECARD	2-103
4.5.	REQUIREMENT AND CONFIGURATION MANAGEMENT BUSINESS PROCESS	2-103
4.6.	CONFIGURATION MANAGEMENT	2-105
4.7.	INFORMATION RETRIEVAL AND KNOWLEDGE DISCOVERY	2-105
4.8.	CONTENT LIFECYCLE MANAGEMENT	2-106
4.9.	DYNAMIC FEEDBACK MECHANISMS	2-107
5.0	GOAL 5 – HARNESS HUMAN CAPITAL FOR THE KNOWLEDGE- BASED ORGANIZATION	2-108
5.1.	THIRD WAVE AKE ORGANIZATIONAL DESIGN PLAN	2-108
5.2.	HUMAN RESOURCES PLANNING	2-110
5.3.	PROFESSIONALIZATION OF THE C4IM WORKFORCE	2-111
5.4.	INSTITUTIONALIZE AKE IN ARMY SCHOOLHOUSES AND SENIOR LEVEL SCHOOLS	2-113
5.5.	UTILIZATION OF INFORMATION OPERATIONS ASSETS	2-114
APPENDIX A: ACRONYMS AND GENERAL ABBREVIATIONS		A-1
APPENDIX B: COMMONLY USED KNOWLEDGE MANAGEMENT TERMS	 B-1

EXECUTIVE SUMMARY

“Transformation is a process, not a one-time event. It’s not easy, because it requires balancing two sometimes conflicting priorities, the need to train and maintain our forces, to meet all our security responsibilities in the world right now, with the need to research, develop, plan and deploy new systems and strategies that will allow us to meet our responsibilities in a much different world.”

“Transformation is important because the decisions we make today, or put off, will shape our nation’s security for decades to come.”

George W. Bush
President of the United States

What This Plan Does - This plan implements the Army’s Knowledge Management (AKM) Strategic Plan and Information Management (IM) Transformation initiatives. It is the Army’s single implementation plan for IM Transformation, AKM directives (such as AKM Memo #2), and other critical AKM initiatives. The initiatives of this plan are aligned to the AKM Strategic plan. It supersedes some previous implementation memorandums and collects in one place the critical tasks we must accomplish to move the Army further towards a knowledge-based, network-centric force. The plan also includes an annex of the terms of reference, which will become the blueprint for future policy and regulatory updates.

Enterprise Resourcing – This plan contains many initiatives that are not funded or are only partially funded. To accomplish this transformation, the plan details a new funding strategy for enterprise resourcing, however, it requires support from Army leadership to make it a reality. As a part of this strategy, the CIO/G-6 is using the Technical Guidance Memorandum response to highlight the priorities and outline a funding strategy.

Stakeholders – Initiatives in this plan comprise the Army’s roadmap for transforming itself into a network-centric, knowledge based force. Collectively, they establish capabilities that are essential to transformation in all functional areas. Therefore, actions must be addressed in and integrated with action in other Army management processes; e.g. TAA, FDU, PPBES. Further, all Army functional proponents are stakeholders in the outcome of this plan and will share in responsibilities detailed herein. Organizations designated lead responsibilities in this plan will engage stakeholders in coordination and ensure that planned actions are appropriately addressed in Army processes.

Basic Theme - The basic themes of the Army’s AKM Implementation Plan are to build upon the baselines set forth in the IM Phase I Execution Plan and AKM Memos (#1, #2, #3, and draft #4), continuing the momentum to achieve the Chief of Staff, Army’s (CSA) guidance of moving to “one network, one data

base,” and supporting the Army’s Transformation in a rapidly changing and evolving Information Operations (IO) threat environment. In August 2002, the CSA approved the Army Knowledge Enterprise (AKE) concept, which redefines how the Army looks at the Objective Force and how the Army’s three components will move toward becoming a knowledge-based organization. In general, the Objective Force is defined now as not only the tactical part of the Army but as extending from the Continental United States (CONUS)/sanctuary base to the foxhole. The AKE construct, consisting of infostructure and knowledge, ties the Army’s functionals (G1, G3, etc.) into the development and execution of the AKE construct. The term “Army” in this plan refers to Active Component (AC), Army National Guard (ARNG) and United States Army Reserve (USAR) forces.

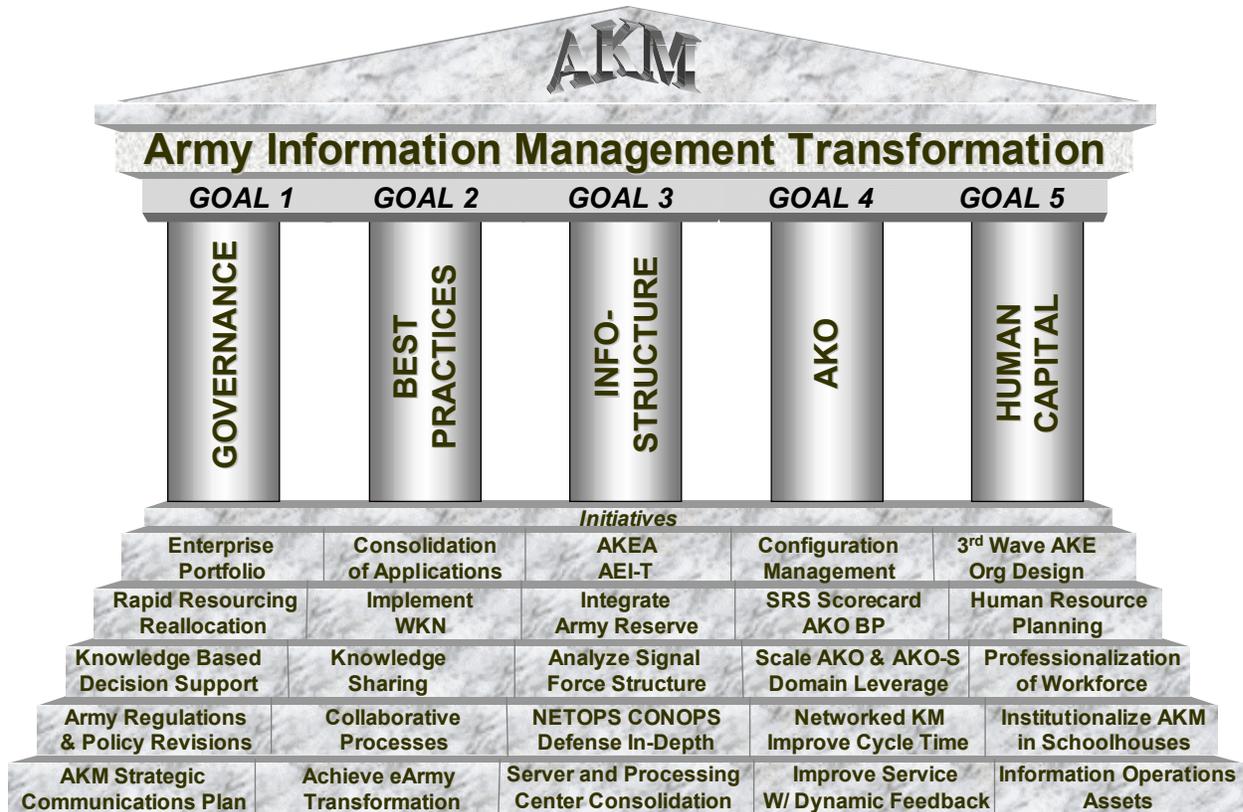


Figure ES-1 AKM is Army Information Management Transformation

Joint/DoD Interoperability – The Army’s AKM Transformation Plan is not developed in isolation, but as an integral part of the Joint/DoD Information Operations intent. There are various Joint/DoD initiatives such as the Global Information Grid – Bandwidth Expansion (GIG-BE), Transformation Communications Systems (TCS), GAPFILLER, TELEPORT, Management Initiative Decision (MID) 905, etc., which can and will provide the Army with

needed bandwidth, enterprise level transport and other services. The Army must move aggressively to leverage the growing DoD capabilities and become a solid partner in developing and shaping the DoD systems through requirements definition and full participation in Strategic Command (STRATCOM), Northern Command (NORTHCOM), and Joint Network Operations (NETOPS) Concept of Operations (CONOPS) implementation. Our goal is to provide increased service levels to Army commanders and a Common Relevant Operational Picture (CROP) to commanders at all levels. During transformation it is the intent to deliver services at current or higher levels. NETCOM/9th ASC has tied their Army Enterprise Infostructure Campaign Plan to the initiatives contained within this plan --these include the NETOPS CONOPS and the Army Enterprise Infostructure – Transport of Part 1 and most of the Goal Three initiatives in Part 2.

Basic Structure of this Plan - Two Parts

This plan has two parts, Critical Enablers for the Future and Continuing the Momentum.

Part 1 – Critical Enablers for the Future – Major initiatives representing fundamental enterprise level changes which will enable the Army to provide IM services to a knowledge-based, network-centric force in the contemporary IO and future Objective Force environment. These key initiatives will be approved by the Army leadership for implementation and tracked by Army Audit Agency (AAA) as part of the Army's transformation. Here are the major initiatives:

- Implement a network-centric, knowledge-based decision support capability to facilitate management of change and provide relevant and accessible knowledge to leaders.
- Implement a strategy to resource IM initiatives at the enterprise level (includes AC, ARNG, and USAR).
 - Support approved AKE/NETOPS concepts, and realign resources and policy to support the concepts.
 - Implement a strategy for optimizing investments and recapitalization.
- Implement the SecArmy/CSA approved AKE initiatives.
 - Implement the Army NETOPS CONOPS.
 - Implement the Army Knowledge Enterprise Architecture (AKEA).

- Implement the Army Enterprise Infostructure – Transport (AEI-T) to further integrate all Army networks into the Army enterprise, to include the , ARNG and National Guard Bureau (NGB), USAR, Corps of Engineers (COE), Community and Family Support Center (CFSC), US Army Accessions Command (USAAC) and Medical Command (MEDCOM).
- Transform the Army's functional end-to-end processes to support application and server consolidation and integration of applications into the enterprise construct.
- Support STRATCOM Computer Network Operations (CNO) and fully implement Information Assurance Defense In Depth.
- Establish core-engineering support to the AKE (e.g. NETCOM, PEOs, CIO, and operational commands).
- Restructure the Army's signal force to provide required interim and objective force capabilities.
- Integrate the Army Reserve and Army Guard into the Army's IM Enterprise.

Part 2 – Continuing the Momentum – Organized around the five Goals of the AKM Strategy, Part 2 initiatives will be approved and tracked by the Chief Information Officer (CIO)/G-6 for implementation as part of the Army's transformation.

This part contains many separate, but integrated initiatives, which implement the Army's five AKM goals. These initiatives and the initiatives of Part 1 are inextricably linked and are critical to reaching the Army's goal of a knowledge-based, network-centric force, requiring the total commitment of the Army. Part 2 initiatives (or their intent) have been approved by the Secretary of the Army (SA)/CSA in the past or are under the purview of the CIO/G-6. The initiatives contained in Part 2 effect implementation of a technology or process associated with building the blueprint of the AKE. Successful execution of these initiatives constitutes steady progress in the on-going transformation of Army as it moves toward its Vision. Without successful implementation of these initiatives, the Army will continue to be an aggregation of separate IM environments characterized by local and sub-optimal solutions that cost too much and deliver too little. The Army CIO/G-6 and the CIO Executive Board (CIO EB) will track these initiatives. Periodic reports will be made to the Army leadership.

INTRODUCTION

1.0 PRIORITIES

"In the cold war, the big ate the small. In globalization, the fast eat the slow."

Tom Friedman
New York Times

The Department of Defense priorities for transformation, as defined in the Quadrennial Defense Review, are:

- *First, to defend the U.S. homeland and other bases of operations, and defeat nuclear, biological and chemical weapons and their means of delivery;*
- *Second, to deny enemies sanctuary—depriving them of the ability to run or hide—anytime, anywhere.*
- *Third, to project and sustain forces in distant theaters in the face of access denial threats;*
- *Fourth, to conduct effective operations in space;*
- *Fifth, to conduct effective information operations; and,*
- *Sixth, to leverage information technology to give our joint forces a common operational picture.*

The Department of the Army with the Chief Information Officer (CIO)/G-6 is fully engaged in transforming the Army. *"To succeed, the army must accomplish three critical tasks at the same time.*

- *First, we must help win the global war on terrorism;*
- *Second, we must transform to meet the challenges of future conflicts; and*
- *Third, we must secure the resources needed to pursue both the war on terror and army transformation."*

Thomas E. White
Secretary of the Army

Army Knowledge Management (AKM) is the strategy to transform the Army into a network-centric, knowledge-based force. The Army realignment of the CIO/G-6, the establishment of the Network Enterprise Technology Command/9th Army Signal Command (NETCOM/9th ASC), and the realignment of the Program Executive Officers (PEOs) to the Assistant Secretary of the Army for Acquisition, Logistics, and Training (ASA(ALT)) are critical to the degree of success the Department of the Army will achieve in meeting Army Knowledge Management goals and objectives and in the Army Transformation Campaign Plan for the Objective Force. All of the Department of the Army, military, civilians, and contractors, must drive toward the goal of a capabilities-based, open architecture and common operating environment that spans from the CONUS/sanctuary to forward deployed units.

2.0 REFERENCES

- Department of the Army Transformation Campaign Plan, April 2001.
- Headquarters, Department of the Army (HQDA) Memorandum, 8 August 2001, Subject: Army Knowledge Management Strategic Plan.
- HQDA Memorandum, 8 August 2001, Subject: Army Knowledge Management Guidance Memorandum Number 1.
- Deputy Under Secretary of Army, International Affairs (DUSA-IA), memorandum, 5 September 2001, Subject: HQDA Realignment Implementation Plan.
- HQDA Memorandum, 30 October 2001, Subject: Guidance from the Realignment Follow-On Meeting.
- Secretary of the Army (SA)/Chief of Staff (CSA), memorandum, 30 November 2001, subject: Information Management Implementation Plan (IMIP) Phase 1.
- SA/CSA, memorandum, 4 January 2002, subject: Implementation Plan for Realignment.
- HQDA Memorandum, 25 January 2002, SUBJECT: HQDA Directorate of Information Management (DOIM) Implementation.
- Department of Defense Strategic Plan for Transforming DOD Training, March 1, 2002.
- HQDA Memorandum, 19 June 2002, Subject: Army Knowledge Management Guidance Memorandum Number 2.
- HQDA Information Management Execution Plan Phase I with Annexes A through N dated 1 July 2002.

- National Strategy for Homeland Defense, July 2002.
- DoD MID 905 Network-centric Business Transformation and e Government, 24 December 2002.

3.0 AKM STRATEGIC GOALS

- GOAL 1: Adopt governance and cultural changes to become a knowledge-based organization.
- GOAL 2: Integrate knowledge management concepts and best practices to promote the knowledge-based force.
- GOAL 3: Manage the infostructure as an enterprise to enhance capabilities and efficiencies.
- GOAL 4: Institutionalize Army Knowledge Online (AKO) as the enterprise portal to provide universal secure access for the entire Army.
- GOAL 5: Harness human capital for the Knowledge-based organization.

4.0 COORDINATING OFFICIAL AND POINTS OF CONTACT

The Army Knowledge Management Division of the Enterprise Integration Directorate (SAIS-EIK) of the CIO/G-6 will be the coordinating office for all actions included in this plan. The points of contact will provide an update of actions and accomplishments under the schedule established by the EIK. The Chief Integration Officer (CXO) will use such outside assets as consultants, AAA etc., as required, to assess progress of completing tasks contained or implied within the plan.

PART 1 – CRITICAL ENABLERS FOR THE FUTURE

1.0 NETWORK-CENTRIC, KNOWLEDGE-BASED DECISION SUPPORT FOR AKM IMPLEMENTATION- AKM GOALS 1 & 2

a. Desired End State

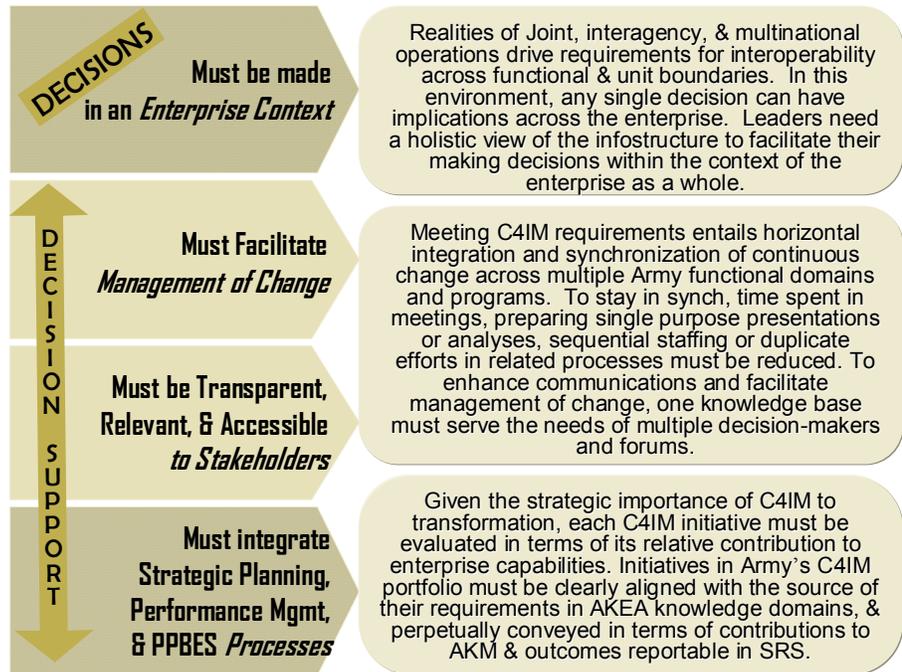
A common, relevant operational picture (CROP) with web-based access to point-of-decision knowledge that Army leaders rely on to make Army Knowledge Enterprise (AKE) decisions.



b. Actions

Initiatives in the AKM Implementation Plan comprise the Army's roadmap for transforming itself into a network-centric, knowledge-based force. Collectively, they establish strategic capabilities that are prerequisite to transformation — a *knowledge-based workforce* and the *Army Enterprise Infostructure (AEI)* vital to its success. These capabilities are crucial to achieving decision dominance throughout the Army enterprise; therefore, all Army leaders have a stake in decisions that pertain to establishing them. Leaders across the enterprise

share a need for a network-centric knowledge base to support decisions they make that depend upon enterprise infostructure and AKM implementation.



share a need for a network-centric knowledge base to support decisions they make that depend upon enterprise infostructure and AKM implementation.

Fundamental changes in the nature and form of decision support are required to insure that relevant knowledge is readily available and used by Army leadership. Change entails actions to:

- Revolutionize what Army leaders expect and accept for decision support.
- Systemically link relevant information from diverse sources to form a single and virtual knowledge repository on enterprise infostructure and

AKM, *one version of truth* supporting multiple decision-makers and forums.

- Establish leadership dashboards and standard displays to convey relevant information, facilitate a shared understanding of key information amongst decision makers, and provide an enterprise context for decisions.
- Web-publish a capability-based enterprise portfolio of Army infostructure as a framework for perpetually conveying the strategic relevance of programs and initiatives, and for aligning them with AKEA, PPBES, and SRS.

c. Specific Responsibilities

1) CIO/G-6

- NLT 1 Aug 03, obtain leadership decision on a plan to “knowledge engineer” key processes for making decisions about AKM and AEI, to incorporate knowledge sharing and collaboration and to optimize knowledge generation for decision-makers.
- Obtain leadership decision on plans to establish a virtual and single AEI/AKM knowledge repository behind the AKO portal.
 - NLT 1 Sep 03, submit plan to pull relevant information from existing and planned databases.
 - NLT 1 Nov 03 submit plan to establish a shared AKM/AEI cyber-library.
 - NLT 1 Feb 04 submit plan to manage repository content, foster progress towards the DoD tenet to “only handle information once,” foster knowledge discovery, and enable productive expansion of the repository.
- Obtain leadership decision on plans to establish leadership dashboards and standard displays.
 - NLT 1 Sep 03, submit plan to web enable the quantitative comparison and ranking of AEI initiatives.
 - NLT 1 Sep 03, submit plan to web-publish a standard display of integrated, multi-goal timelines for progress on AKM implementation.
 - NLT 1 Nov 03, submit plan to webify access to known and relevant recurring analyses.

- NLT 1 Nov 03, submit plan to address key decision maker needs (e.g.; G3, G8, CIO/G-6, ACSIM, and other functional proponent leaders).
- NLT 1 Dec 03, submit plan to address needs of governance bodies and decision forums (e.g., ABIC, AEIMSG, AKO CCB, CIO-EB).
- NLT 1 Jan 04, submit plan to address needs of other stakeholders (e.g., RCIO, DOIM, Unit Commanders).
- NLT 1 Aug 04, submit plan to web-publish standard displays of status on enterprise compliance requirements (e.g., Net-Worthiness; COTS exemptions; ERP waiver lists; and governing checklists published in Army Regulation 25-1).
- NLT 1 Sep 03, obtain leadership decision on a plan to web-publish a capability- based portfolio of Army C4IM, in alignment with AKEA, PPBES, and SRS.
- NLT 1 Sep 04. Establish a Maturity Model and a Performance Plan for continuous improvement of Network-centric Knowledge-based Decision Support for C4IM.

2) ASA(ALT)

- NLT 1 Aug 04, establish and web-publish a standard display of integrated, multi-program timelines for AEI development and fielding activities enterprise-wide. Once established, this capability will be expanded to include all PEOs and their programs.

3) CIO Executive Board

- Participate as a stakeholder in identifying leadership requirements.
- Evaluate decision support and the evolution of the knowledge base; recommend enhancements.

4) Point of Contact:

- CIO/G-6 CXO

2.0 ENTERPRISE RESOURCING - AKM GOAL 1

This plan describes the process by which the Army's C4IM investment policy will be made to enable transformation. The actions and resulting products of the process support the strategic capabilities requisite for transformation to a

knowledge-based workforce and the robust and relevant *infostructure* vital to its success.

The realities of Joint, Inter-agency and Multinational (JIM) operations, as well as operational requirements for CROP and situational awareness, demand that information be shared extensively within and across organizational boundaries. Technology must enable information sharing and interoperability across functional and unit boundaries while providing a secure, robust information infostructure to enable power projection and reachback connectivity for split base operations.

These critical capabilities entail horizontal integration of diverse actions across multiple communities; it involves enterprise-wide oversight for managing C4IM resources and the ability to synchronize the timing and directly impact the flow of resources in the Planning, Programming, Budgeting and Execution System (PPBES) process.

2.1. CAPITAL PLANNING AND INVESTMENT MANAGEMENT

a. Desired End State

An Enterprise Portfolio-based Information Management Capital Planning and Investment Management (CPIM) process that delivers a strategy to the Army for planning, programming, acquisition, execution, and evaluation purposes.

b. Actions

This CPIM process provides a strategy that is used for planning, execution and resource reallocation purposes. The objective of the CPIM process is to develop C4IM investment policy and provide direction that informs Army Leaders and directly impacts their Program Objective Memorandum (POM) decisions on all C4IM expenditures across all functional domains in the Army in compliance with the Clinger-Cohen Act.

It will also be flexible and agile in design to be able to fulfill near-term requirements with rapid resourcing and acquisition solutions while increasing the speed with which development and acquisitions successfully take place.

The CPIM uses a capability-based methodology and incorporates enterprise-wide performance measures as one of its key criteria. The process is collaborative, involving participants from multiple organizations within the HQDA to include G1, G2, G3, G4, G-6, G8, Army Budget Office (ABO), and the Program Evaluation Group (PEG) Co-Chairs of the Installation, Equipping, Sustaining, Manning, Organizing, and Training PEGs; Army Major Commands (MACOM); Installation Management Agency (IMA) Region Directors/Regional CIOs (RCIOs); the Army Reserve and National Guard; NETCOM/9th ASC; Combatant

Commanders J-6s; the CIO Executive Board; and the investment area communities who participate in the development of C4IM investment strategies. In addition, representatives from other Federal agencies and organizations, including Office of the Secretary of Defense (OSD) and the General Accounting Office (GAO), may participate.

The CPIM process results in enterprise resourcing through the oversight of decisions in the Program POM years and in the year of execution. It focuses on C4IM investments and the capabilities they support and provide for the Army Enterprise. These include but are not limited to: manpower, facilities, capital assets, and the current expenditures that maintain these assets. It addresses C4IM investment performance, investment risks, C4IM interdependencies, incorporation of best practices and business cases. In addition, it aligns investments with strategic doctrine and guidance documents while elevating existing capability gaps across multiple areas of C4IM investments. The CPIM is a flexible process. Its resulting enterprise resourcing decisions will enable rapid, continuous, and capability-based resource allocation to support current and dynamic Army mission needs.

The CPIM also serves to maintain resource management methods compliant with administrative and legislative directives on Capital Planning and Investment Management, to integrate strategic planning with performance management and budgeting; and, to comply with MID 905 direction to expand the use of business cases and balanced scorecards. CPIM will serve as the forum through which change catalysts -- policies, processes, and cultural paradigms -- will propel transformation to the AKE.

The resultant strategy will provide increased levels of Army mission effectiveness, C4IM and mission capability enhancement, C4IM system efficiencies, and opportunities for cost avoidance/savings. Complete oversight of C4IM capabilities (programs and initiatives) will provide an enterprise perspective and transparency of information needed to effectively allocate resources and integrate change across functions, in alignment with Army-wide priorities. The CPIM strategy will allow the Army to:

- Ensure compliance with Congressional and Federal guidance (Clinger-Cohen Act, Government Performance and Results Act, etc.) for enterprise-wide oversight over prioritization of C4IM investments, initiatives, and evaluation and management of performance. This would include full integration of the CPIM process and the PPBES process.
- Coordinate and establish a process using all stakeholders to gain commitment for participation and a unified and thorough understanding of the approach, roles and responsibilities that are required to accomplish the CPIM process and achieve its stated outcomes.

- Expand the Army's investment strategy to include oversight of the full life cycle costs of all C4IM.
- Expand the CPIM process to include all functional areas in the Army.
- c. Specific Responsibilities
 - 1) CIO/G-6
 - NLT 1 Oct 03, initiate the expansion of the CIO investment strategy process to address the full life cycle and manage the Enterprise Portfolio of all C4IM capabilities across all functional domains in the Army to develop C4IM investment policy and provide direction that informs Army Leaders and directly impacts their POM decisions.
 - NLT 1 Oct 03, continue to produce an enterprise-wide C4IM investment strategy to facilitate enterprise prioritization of C4IM capabilities (programs and initiatives) in terms of strategic outcomes and other balanced scorecard criteria to include business cases. The use of balanced scorecards and web tools may be used to facilitate this critical data gathering process. The products of this action are:
 - Baseline C4IM information from all functional domains.
 - Data repository for business cases.
 - Database of C4IM investment areas' alignment and contribution to Army missions and strategies, National Security guidance, and Joint strategies.
 - Performance management process to regularly evaluate performance on resourced programs.
 - NLT 1 Oct 03, develop an enterprise strategy for C4IM investments, where each product will be reviewed and approved by the associated stakeholder communities and its leadership, to include:
 - C4IM capability assessments.
 - C4IM investment solutions.
 - Risk assessments and risk mitigation strategies.
 - C4IM interdependency assessments.

- NLT 1 Nov 03, coordinate the resultant enterprise strategy with Army leadership to include but not be limited to: G1, G2, G3, G4, G-6, G8, ABO, Program Analysis and Evaluation (PA&E), and ASA (ALT).

2) Point of Contact

- CIO/G-6 RI

2.2. ENTERPRISE PORTFOLIO

a. Desired End State

A *Rapid Resource Reallocation capability* to facilitate centralized oversight, allocation, and rapid reallocation of resources for Army C4IM capabilities and to provide the "operational agility" required for enterprise operation.

b. Actions

The foundation for *Rapid Resource Reallocation* will be established by systematically removing barriers to agility, factors that constrain or prevent cross leveling of resources within the *enterprise portfolio*. The establishment of a virtual, *Rapid Resource Reallocation capability* will serve as a strategic buffer, providing the *agility* needed to: synchronize and integrate changes in line with changing Army enterprise priorities; mitigate risks; leverage enterprise level initiatives, and take advantage of opportunities for great payoffs in resource savings or improved capabilities.

- Establish a capability for rapid resource reallocation, to provide the agility needed to mitigate risks, leverage opportunities, and synchronize and integrate change in line with changing Army enterprise priorities.

c. Specific Responsibilities

1) CIO/G-6

- NLT 1 Sep 03, develop and obtain CIO decision on alternatives and a plan for establishing a Rapid Resource Reallocation capability; coordinate with MACOMs and functional proponents, include recommendations for change needed in Army programming or budgeting guidance documents.
- NLT 1 Feb 04, commence and continue implementation of the plan to establish a rapid resource allocation capability.

2) Point of Contact:

- CIO/G-6 RI

3.0 ARMY KNOWLEDGE ENTERPRISE – AKM GOALS 1, 2, 3, 4 AND 5

Army Knowledge Enterprise (AKE) is defined as the Army's portion of the Global Information Grid (GIG). This is illustrated in Figure 1.3-1.

AKE is the overarching concept comprised of knowledge and Infostructure. AKE creates an environment for universal access to trusted knowledge anywhere, anytime. AKE supports AKM by facilitating the network-centric and knowledge-based Army Objective Force.

The Infostructure is comprised of five components: Communications, Information Management, Computers, Enterprise Applications, and Network Operations. Knowledge is the result of inter-activities of Enterprise business practices, processes and associated application of doctrine, training, leadership, organizations, material, personnel and facilities (DTLOM-PF).

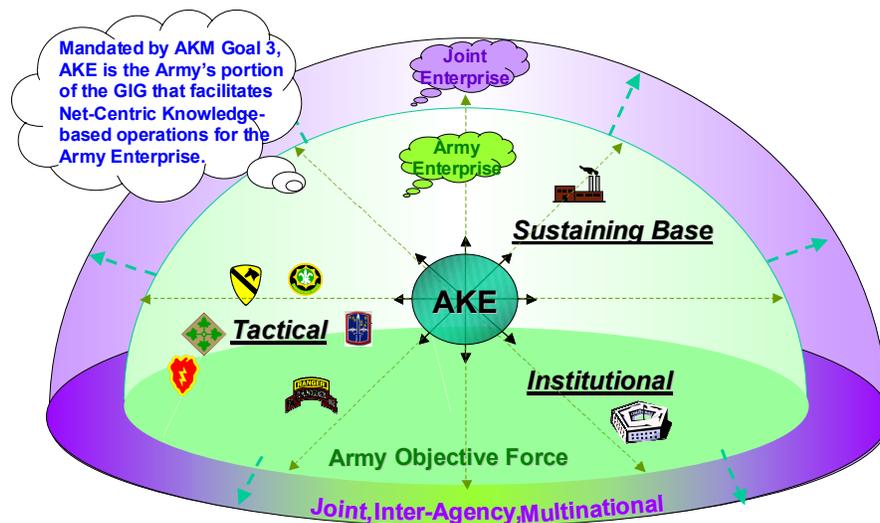


Figure 1.3-1 AKE Facilitating the Network-centric Knowledge-based Army Objective Force

Community of Interest Networks (COINs) have been established by several Army MACOMs, agencies and activities (e.g. NGB, MEDCOM, USAR, COE, USAAC, and CFSC). In varying degrees, these COINs provide highly integrated C4IM services to their respective customer base. Some COINs have achieved a high degrees of centralized management and enterprise-level efficiency in C4IM service delivery. COINs have established virtual private networks (VPN) transcending existing, geographic and political boundaries. These COINs will

integrate into the AKE. It is the intent to preserve COIN-level efficiencies as we integrate.

3.1. DOCUMENT AND EXECUTE ARMY NETOPS CONOPS - AKM GOAL 3

a. Desired End State:

Army leaders and customers universally accessing authorized services and knowledge anywhere in the world via a single sign-on to an "enterprise" network during routine operations as well as in crisis actions, in consonance with the Joint NETOPS CONOPS.

b. Actions

NETOPS consists of three interrelated disciplines, Systems and Network Management (SNM), Information Assurance (IA), and Information Dissemination Management (IDM). The Army NETOPS CONOPS identifies the objective operational environment for each of these disciplines. In the NETOPS Objective State, the Army will be able to accomplish, at a minimum, the following:

- Enable universal and secure access to authorized infostructure services for all customers within the Army infostructure - secure single sign-on "plug & play" capability.
- Accurately display a total, integrated, and tailored CROP of the AEI.
- Predict impacts to the AEI of new/changed systems and operational contingencies through networkiness analysis and simulations.
- Provide dynamic allocation of AEI capabilities in near real-time to support Army responses to crises or unplanned events anywhere within the Army Infostructure.
- Provide IDM services that address awareness, access, and delivery of information; specifically, IDM involves compiling, cataloguing, caching, distributing, and retrieving data; managing the information flow to users; and, enabling the execution of the Commander's information dissemination policy.
- Provide assured defense of Army networks and customer data.
- Perform continuing and non-intrusive technology insertion to improve service levels or reduce cost of providing current base-level services.
- Provide Disaster Recovery capabilities.

NETCOM/9th ASC, as the Army's GIG component lead for NETOPS, will develop and execute the approved Army NETOPS CONOPS. The CONOPS will be synchronized with the AKEA effort and will be in consonance with the DoD NETOPS CONOPS being developed by Defense Information Systems Agency (DISA). The Army NETOPS CONOPS will be reviewed by NETCOM/9th ASC and the CIO/G-6 annually and resubmitted to the CIO EB for approval upon any major revision of the NETOPS CONOPS or, at a minimum, every two years, whichever comes first.

c. Specific Responsibilities

1) CIO/G-6

- Establish policy for the Army's NETOPS CONOPS.
- Designate NETCOM/9th ASC as the Army GIG component lead for NETOPS.
- Approve the Army's NETOPS CONOPS.

2) Reserve Components

- Coordinate with NETCOM/9th ASC to ensure reserve component requirements are included in the NETOPS CONOPS.

3) NETCOM/9th ASC

- Develop the Army's NETOPS/CONOPS, in coordination with the Reserve Components and DISA.
- Maintain and execute the Army's NETOPS CONOPS.
- Provide Army execution guidance and oversight on the NETOPS CONOPS.
- Operate, manage, and defend the AEI as outlined in the NETOPS CONOPS.
- Serve as the Army Deputy Commander, Army Forces (DEPCOM ARFOR) to the Department of Defense (DoD) Joint Task Force (JTF)-CNO.

4) DOIM

- Make/allow no changes to the infostructure not directed/approved by NETCOM/9th ASC.

- Monitor network for compliance.
- Ensure all changes are processed in accordance with NETOPS CONOPS and the Army Networkiness process.
- Deliver consistent C4IM services as outlined in Service Level Agreements (SLA).

5) Point of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC ESTA

3.2. DEVELOP AND EXECUTE THE ARMY KNOWLEDGE ENTERPRISE ARCHITECTURE (AKEA) - AKM GOAL 1, 2, 3, 4 AND 5

a. Desired End State

An Enterprise blueprint for establishing and maintaining the infostructure and knowledge essential to achievement of a network-centric knowledge-based Army.

b. Actions

The AKEA is the Army's portion of the Global Information Grid architecture and it is the Army's implementation of the IT architecture required by the 1996 Clinger-Cohen Act. The AKEA includes the Army Domain architectures and the GIG Infostructure Component architectures (Communications, Computing, Enterprise Applications, NETOPS, and Information Management). The Current Army Domains are:

- Acquisition (ASA(ALT))
- Battle Command (G3)
- Finance (ASA(FM))
- Infostructure (G-6)
- Installations (ACSIM)
- Intelligence (G2)
- Legal (TJAG)
- Logistics (G4)

- Manpower and Personnel (G1)
- Medical (OTSG)
- Operations and Plans (G3)
- Programs (G8)
- Quality of Life/Morale, Welfare, and Recreation (ACSIM/CFSC)
- Readiness (G3)
- Religious Support (Chief of Chaplains)
- Requirements (G3)
- Training (G3)

The Domain list will continue to be refined. Figure 1.3-2 illustrates the relationship between the Domains and the GIG Infostructure Component Architectures. Each Domain is responsible for architecting its business processes (assisted by the Army Architecture Integration Cell (AAIC)). The infostructure enables the Domains to operate by providing a network-centric environment.

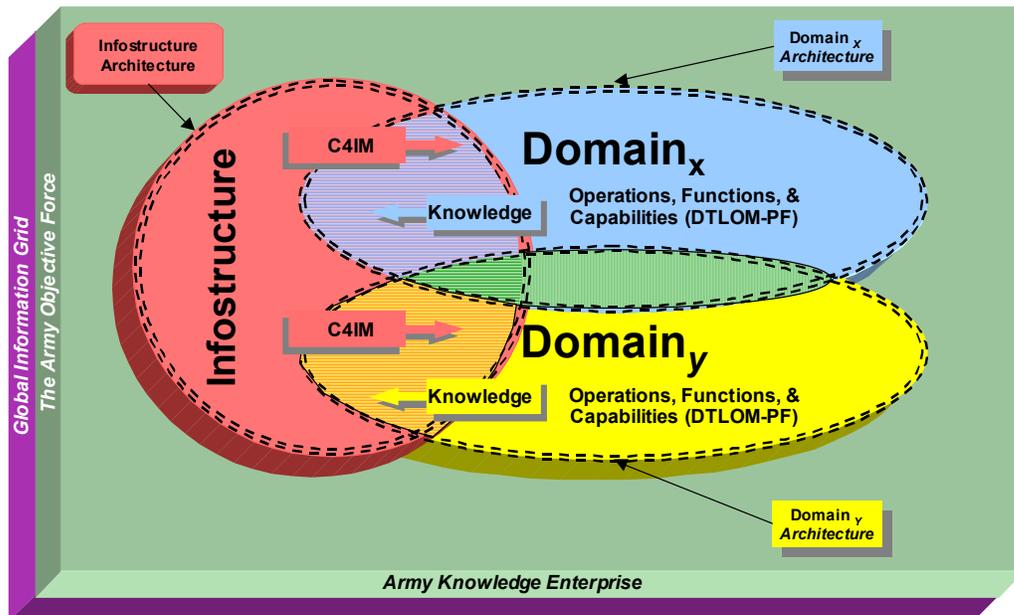


Figure 1.3-2 The AKEA Model

The Army G3 (The Army Chief Architect) and Army G8 provide priorities to the Army Lead Architects and the AAIC for the development of Army architectures.

The Lead Architects for the Army are the CIO/G-6 and the Director, Objective Force Task Force. They provide the strategic direction and vision for Army architecture efforts. The Army CIO/G-6 CXO provides daily operational oversight and direction to the AAIC.

The AAIC establishes, executes, and maintains Army policy for the development and integration of Army architectures in support of Army Transformation. The AAIC will synchronize architecture development and its linkages with JIM architectures throughout the Army enterprise. The AAIC will coordinate and provide direct support to the Army Domain Proponents to develop domain architectures traced to Joint missions, operations, and functions. In addition, the AAIC will facilitate the approval of Army architecture products for support to investment, fielding, and deployment decisions. AAIC governance is shown in Figure 1.3-3.

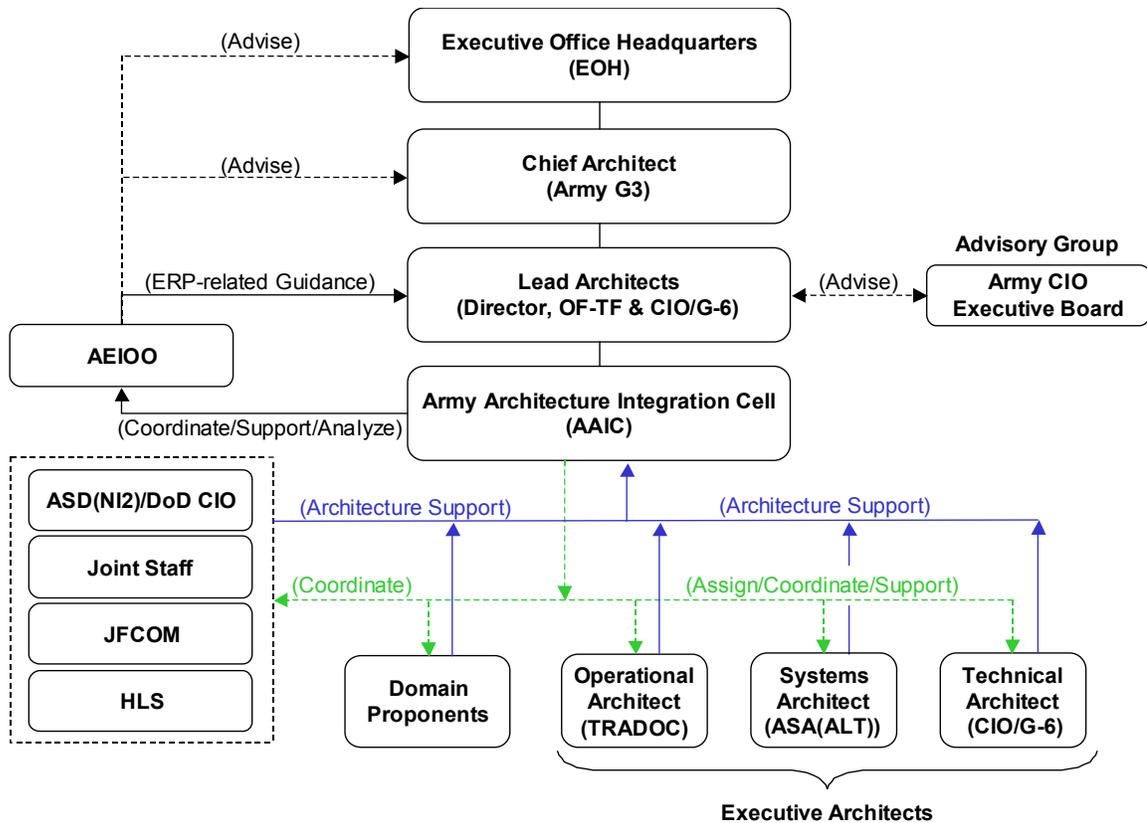


Figure 1.3-3 Army Architecture Governance

The AAIC will provide direction to the Army Executive Architects for the development and integration of Army Operational, System and Technical Architectures based on the established priorities. The Army Executive Architects are Training and Doctrine Command (TRADOC), Executive Architect for Army Operational Architectures; ASA(ALT), Executive Architect for Army Systems Architectures; and the Army CIO/G-6, Executive Architect for Army Technical Architectures.

The CIO/G-6 Director of IONS will develop the Infostructure Architecture in coordination with the Infostructure components and the USAR and NGB. Day-to-day responsibilities for Infostructure Architecture will be conducted by the CIO/G-6 Enterprise Architecture Division.

c. Specific Responsibilities

1) Army Architecture Integration Cell

- Develop a Charter for the AAIC NLT 1 Jun 03.
- Identify the Domain Proponents (end-to-end business process owner). (Completed).
- Establish, execute and maintain Army policy for the development and integration of Army architectures.
- Update the Army Enterprise Architecture Guidance Document (AEA GD) NLT 1 Jul 03.
- Analyze Army architecture products to ensure traceability from Joint strategic directives and supporting JIM requirements through Army Operational Concepts and the fielding of interoperable systems.
- Establish and implement an Army architecture approval process NLT 1 Jul 03, in support of investment, fielding, and deployment decisions.
- Establish and manage a collaborative environment for Army architecture product development.
- Establish and manage a common data repository for approved Army architecture products NLT 1 Sep 03.
- Publish the Army Knowledge Enterprise Architecture AV-1, Overview and Summary NLT 1 Jun 03.

- Define and track architecture performance measures for the Strategic Readiness System.
- Develop and publish the annual Architecture Tasking Memorandum establishing architecture development priorities based on the G3 established Army priorities.
- Manage AKEA MDEP.

2) CIO/G-6

- Establish the AAIC (completed).
- Identify an end-to-end Infostructure Component owner for each of the five GIG Infostructure Components (completed).
- Perform Executive Architecture for Technical Architecture missions in accordance with the AAIC Charter.
- Develop the Infostructure Architecture in accordance with the AAIC methodology and Architecture Tasking Memorandum.
 - Coordinate development of the Infostructure Architecture with the AAIC.
 - Oversee and synchronize the architecture development activities of the five Infostructure Components.
 - Serve as the lead for the Information Management Infostructure Component.
 - Publish instructions on Infostructure Architecture development (AV-1 Overview and Summary).
 - Chair the Army GIG Enterprise Services Configuration Management Board.
- Update AR 25-1 and other HQDA publications and policies to reflect the AKE/AKEA.
- Serve as the Army Executive Architect for Technical Architectures.
 - Coordinate Technical Architecture development and integration with the AAIC.
 - Develop Technology Forecasts.

- Oversee Weapon System Common Operating Environment.
 - Ensure Army requirements are incorporated into the GIG Enterprise Services.
 - Ensure technical architecture products are All Core Architecture Data Model (CADM) conformant.
 - Ensure compliance to the AKEA and the JTA-A.
 - Establish and implement an Army Networkiness Certification process NLT 1 Jun 03.
 - Review Technical Views (TV-1s).
 - Ensure mutual support and synchronization between the Infostructure Architecture and other CIO/G-6 efforts.
- 3) G3
- Serve as the Army Chief Architect.
 - Develop and provide the AAIC with annual architectural priority list.
 - Participate in architectural reviews and forums.
- 4) G8
- Assist G3 in determining architecture priorities.
 - Identify needed decisions the architecture will help answer and ensure that the answers are implemented through Force Development/Force Management processes.
- 5) ASA(ALT)
- Serve as the Executive Architect for Systems Architectures.
 - Work with the AAIC to define lines of demarcation, mission clarity/definition.
 - Coordinate System Architecture development with the AAIC.
 - Execute and produce architectural products in accordance with the annual Architecture Tasking Memorandum.

- Insure all Program Executive Officer (PEO) managed programs and systems develop the required architectural views in accordance with the Army architecture development methodology.
 - Perform Executive Architecture for Systems Architecture missions in accordance with the AAIC Charter.
 - Ensure system architecture products are All CADM compliant.
 - Provide a full-time representative to the AAIC NLT 1 Jun 03.
- 6) Objective Force Task Force (OFTF)
- Provide a full-time representative to the AAIC NLT (completed).
- 7) TRADOC
- Serve as the Executive Architect for Operational Architectures.
 - Work with the AAIC to define lines of demarcation, mission clarity/definition.
 - Coordinate Operational Architecture development and integration with the AAIC.
 - Perform Executive Architecture for Operational Architecture missions in accordance with the AAIC Charter.
 - Execute and produce architectural products in accordance with the annual Architecture Tasking Memorandum.
 - Ensure operational architecture products are all CADM compliant.
 - Responsible for developing the Army Operating Concepts, Army Functional Concepts, and Force Operating Capabilities, with traceability to the Joint Operating Concepts.
 - Provide a full-time representative to the AAIC NLT 1 Oct 03.
- 8) MACOM and Functional Proponents
- Assist CIO/G-6 and AAIC in developing the AKEA by developing Domain architectures for assigned area of responsibility end-to-end and all phases of employment.
 - Develop architectures in accordance with the methodology provided by the AAIC.

- Resource architecture development for specified sub-mission areas as part of core mission.

9) Infostructure Components

- Infostructure Component Leads are: Communications – Communications Engineering Command (CECOM); Computing – ASA (ALT); Enterprise Applications – CECOM; Information Management – CIO/G-6; NETOPS – NETCOM.
- Infostructure Component Leads will assist CIO/G-6 and AAIC in developing the Infostructure Architecture and AKEA by developing Component architectures for assigned area of responsibility end-to-end and all phases of employment.
- Develop architectures in accordance with the methodology provided by the AAIC.
- Coordinate architecture development through the CIO/G-6.

10) Point of Contact

- CIO/G-6 AAIC and IOE.

**3.3. ARMY ENTERPRISE INFOSTRUCTURE - TRANSPORT (AEI-T) - AKM
GOAL 3**

a. Desired End State

All Army networks integrated into the Army Enterprise Infostructure – Transport (AEI-T) (e.g. tactical, deployed, SATCOM, AR Net II, GuardNet, COE, CFSC, USAAC, MEDCOM, etc.) establishing the network-centric environment that enables seamless communications, anywhere, anytime.

b. Actions

The CSA has directed the Army move to one Army network, the AEI-T. The CIO/G-6 proposes a phased strategy, which will result in one logical network, that permits Army users to access authorized network resources regardless of where those resources are located or where the user is located. As the transformation of the network occurs, functional and associated NETOPS/component capabilities will merge into one Army Network. This will be done through a collaborative effort with each of the network proponents involved.

The Army will move to an integrated, AEI-T in a series of phased actions. The end state is a single logical Army network under the operational control of NETCOM/9th ASC providing services and savings to the Army.

- Phase I (Oct 02-Sep 03) Establish one “virtual” Army enterprise network as the Army’s portion of the DoD GIG. Effective 1 Oct 02, the current Army wide area networks (WANs) began to operate under the TECHCON of NETCOM/9th ASC to enable the Army to see the operational status and health of the various Army networks. The establishment of the “virtual” Army enterprise network consists of multiple physical networks that are interconnected and interoperable. This will include all of the current COINs and functional Network Operating Centers (NOCs) providing NETCOM/9th ASC Theater Network Operations and Security Centers (TNOSC) both the equipment and data to have real-time visibility of the current status of the various networks, status of any trouble ticket or action items related to the network, and critical performance indicators on the health of the network, to include information assurance status. In addition, NETCOM/9th ASC will issue operational orders to ensure the various Army networks support the operations of the Army and JIM. NLT 1 Sep 03 reporting should be automated and iterative. The Phase I Objective Enterprise Transport is illustrated in Figure 1.3-1.
- Phase II (Oct 03 – Mar 04). Implementation of common policies, structures, and tool sets. Develop and implement critical common network management and defense policies necessary to migrate the Army to AEI-T NLT 1 Jul 04. This includes development/implementation of a common Army network security posture, enabling the NETCOM/9th ASC TNOSCs to view all network elements within the Army Enterprise Infostructure. This visibility of assets extends to global centralized monitoring of the Army networks as a “detection” subset of defense-in-depth coverage. The responsibility and authority to operate existing COINs will remain under the day-to-day operational control of the functional RCIOs defined in Annex D of the Information Management Execution Plan (IMEP), Phase 1, dated 1 July 2002 and other functional network proponents, such as USAAC. NETCOM/9th ASC will continue to exercise TECHCON of these COINs, as stated in the IMEP. The COINs will actively participate in and support all AKM initiatives for achieving full C4IM integration. Functional RCIOs will operate as virtual regions, on an equal standing with geographic IMA regions. NETCOM/9th ASC is the final authority for coordination and integration of C4IM delivery within these virtual regions and across geographic regions. Update Army regulations, including AR 25-1, as required to reflect the changes in responsibility.

Objective Enterprise Transport

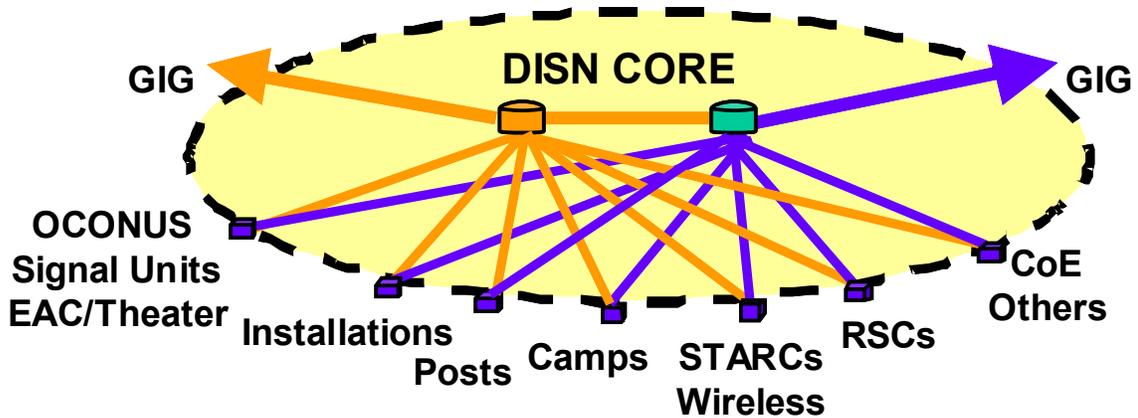


Figure 1.3-1 Phase I Objective Enterprise Transport

- Phase III (Oct 03 – Sep 05). Migration to the AEI-T. All Army WANs not currently operated by a NETCOM/9th ASC TNOSC will migrate to the AEI-T under the operational control of NETCOM/9th ASC. The integration is illustrated in Figure 1.3-2. The expected networks for migration include, but are not limited to:
 - DLS (formerly TADLP)
 - MTMC
 - AR Net II
 - GuardNet
 - ARSTRAT (SMDC)
 - TRADOC (Accessions Command)
 - IG Net
 - JAG Net
 - MEDCOM
 - COE

CIO/G-6 in coordination with Army Material Command (AMC) CECOM and NETCOM/9th ASC, in full coordination with the proponents, will publish an initial migration plan NLT 1 Sep 03.

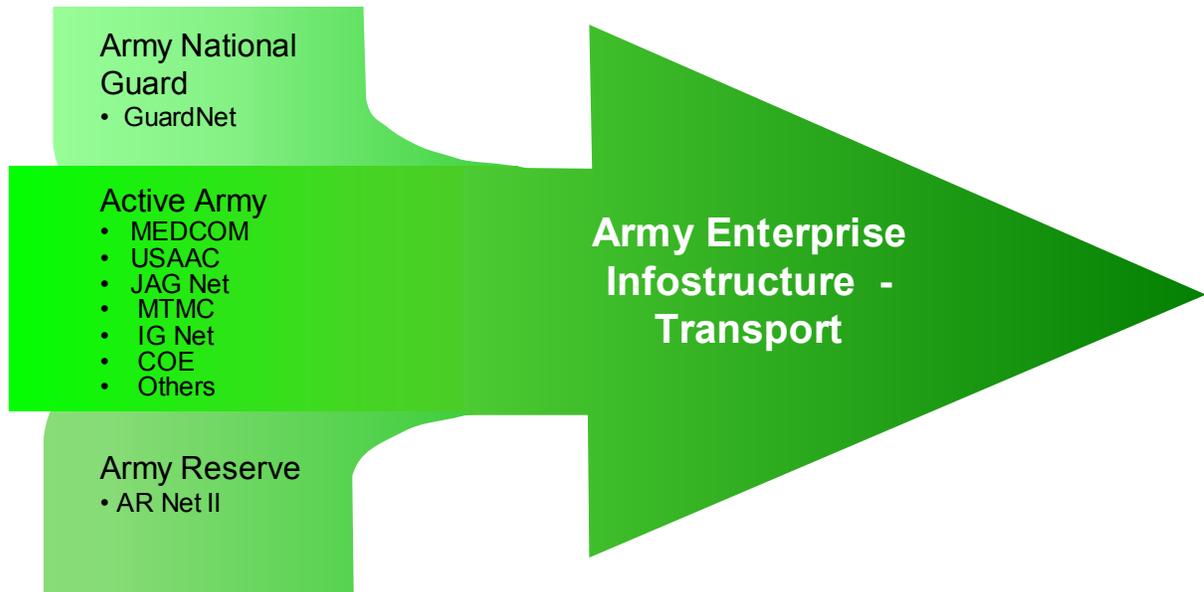


Figure 1.3-2 Phase III - Merge Networks into the AEI-T

Using an Enterprise Systems Engineering (ESE) approach, the CIO/G-6 AEI-T Reengineering Work Group in coordination with AMC CECOM and NETCOM/9th ASC has developed a strategy to migrate to one “virtual” Army enterprise network in the following steps:

- Step I - Collect Data on Existing Networks - Ongoing. Collect existing data, modeling and analysis of major proponent network topology and primary interfaces between the Active Army (NIPRNET), AR Net II, Army GuardNet, Corps of Engineers (COE), Medical Command (MEDCOM), USAAC, and Department of Defense (DoD) Defense Information Systems Agency (DISA). This step seeks to identify data for reuse from the existing databases that have evolved within disparate networks and produce an Army Enterprise Network topology, costs, and capabilities, enabling optimization within and consolidation between components.
- Step II – Migration Strategy to Integrate Networks. Develop the migration strategy to integrate the Components into a single network of networks managed at the service boundaries. This effort will result in optimizing the cost and performance of the

existing networks and will define the courses of action leading to the objective network. The estimated time to complete this effort is 12 months from inception. The migration strategy should examine the strengths of all existing networks to enable transition to one enterprise network.

- Step III – Enterprise Applications and Enterprise Data Storage. Develop the strategy to implement enterprise applications and enterprise data storage. Thus, creating the network infostructure for the "One Database" concept paralleling the "One Network" concept.

The first network migration will occur in FY04. The proponents currently responsible for operations and funding of these networks will identify the resources expended in support of those networks for FY02, the budgeted resources for FY03, and the resources contained in the POM for FY04 – FY09. NETCOM/9th ASC, in conjunction with the network proponents, will evaluate the current operations supporting each of these networks and determine the optimum disposition of the operations and resources (e.g. capitalization, elimination, retention). It is expected that common user functions will transition to NETCOM, with proponents retaining operational control of MACOM or functional proponent unique missions. The Army Network will form the transport common carrier for the Army's enterprise applications for personnel, logistics, etc.

Essential to AEI-T is continuity of Network Operations and Security Center (NOSC) operations. Each NOSC must have a viable Continuity of Operations (COOP) plan to prevent extended interruptions to operations. Continuity planning includes disaster recovery as well mitigating risks that may prevent operations. COOP planning and implementation will leverage existing resources and partnerships. It is planned to virtually integrate existing CONUS NOSCs into one CONUS TNOSC. These NOSCs will migrate into a consolidated TNOSC structure in Phase III. The Army has activated a Southwest Asia (SWA) TNOSC as part of the AEI-T.

The Army will implement a virtual private network (VPN) that will use, to the maximum extent possible, the physical Defense Information Systems Network (DISN) backbone and infostructure. This VPN will provide a protected network at the NIPRNET level that connects all Army users in a trusted environment.

Ultimately the AEI-T will provide a high bandwidth network backbone linking all Army customers with needed bandwidth at short notice at required security levels. The AEI-T will guide investment strategy and build on existing bandwidth expansion programs (i.e. GIG Bandwidth Expansion, Installation Information Infostructure Modernization Program (I3MP), etc.), which will provide links into the DISN (NIPRNET and SIPRNET), and to the Internet.

c. Specific Responsibilities

1) CIO/G-6

- Publish Army policy directing the migration of separate Army networks, in coordination with functional network proponents and Components NLT 1 Sep 03.
- Develop the initial AEI-T operational architecture that defines the one Army network including the Army Intranet NLT 1 Jul 03.
- Publish an initial Phase III migration plan NLT 1 Sep 03, in coordination with AMC CECOM, NETCOM/9th ASC, and functional network proponents.
- Determine and direct the necessary manpower and resource transactions to support the migration.
- Through ASA (ALT), direct PEO EIS to execute tasks in support of this initiative.
- Ensure changes in policy are updated in Army Regulations, including AR 25-1.

2) ASA (ALT) PEO EIS and PEO C3T

- Perform Business Case Analysis (BCA) to guide AEI-T implementation NLT 1 Jan 04.
- Work with CIO/G-6 to produce the Army Intranet Migration Plan NLT 1 Sep 03.
- Program, budget and develop resource strategy to support AEI-T in all phases of life cycle.
- Manage cost, schedule, performance and supportability.
- Execute tasks as directed by CIO/G-6 in support of this initiative.
- System engineer, acquire and field necessary infostructure to implement the AEI-T in accordance with the architecture.

3) NETCOM/9th ASC

- Develop and implement critical common network management and defense operational policies necessary to migrate the Army to AEI-T NLT 1 Jul 04.

- NLT 1 Sep 03 reporting should be automated and iterative.
 - Work with the CIO/G-6 to publish an Army Intranet Migration Plan NLT 1 Sep 03, based upon the initial AEI-T architecture.
 - Begin operational control (OPCON) of Army networks NLT 1 Oct 03. Complete NLT 1 Oct 04.
 - Publish an Army NOSC Consolidation Plan NLT 1 Sep 03.
 - Assist CIO/G-6 in determining resources supporting each network and in the determination of necessary manpower and resource transfers and requirements to support implementation and COOP/disaster recovery.
 - Operate, manage, and defend the Army Intranet WAN.
 - Input changes to Army Regulations, including AR 25-1.
- 4) Functional Network Proponents (DLS, MTMC, TRADOC, IG, JAG, MEDCOM, COE, USAR, NGB, ARNG, etc.)
- Identify the equipment, communications capabilities, and data display capabilities currently used to provide real-time visibility on the current status of the various networks, status of any trouble ticket or action items related to the network, and critical performance indicators on the health of the various networks NLT 1 Jun 03.
 - Provide the necessary resources for the appropriate NETCOM/9th ASC TNOSC to have visibility of and exercise TECHCON over Army WANs NLT 1 Jul 03.
 - Assist in determining the optimum transition strategy for proponent and component networks and resources.
 - Implement the migration strategy in coordination with NETCOM/9th ASC. Prepare to OPCON networks to NETCOM/9th ASC beginning 1 Oct 03.
- 5) Point of Contact:
- CIO/G-6 IOM
 - NETCOM/9th ASC ESTA Governance and NETOPS Directorate

3.4. FOSTER THE GROWTH OF AN ENTERPRISE KNOWLEDGE BASE - AKM GOALS 2, 3, AND 4

Old organization + new technology = very expensive old organization.

The success of a knowledge-based force is dependent on the growth of knowledge. For knowledge to grow and be relevant, information must be shared efficiently and widely. Stand-alone functional processes limit information flow to within functional boundaries and thereby hinder knowledge growth. In contrast, end-to-end (E2E) processes connect people to people for sharing information across functional and organizational boundaries.

To grow an enterprise knowledge base, Army must transform stand-alone functional processes into streamlined, integrated, enterprise-wide processes and multi-functional E2E processes.

Transformed, E2E processes promote efficiencies that are not apparent from a functional stovepipe perspective, increasing the value of investments made in time, money, or people. Notably, they can promote efficiencies of particular significance to growth of a relevant knowledge base by bring redundancy to light, allowing for streamlining, consolidation, and even elimination of applications.

In a network-centric environment multiple E2E processes will share data from common sources, from a virtually single knowledge base. Content owners will refresh, and manage the information they produce; however, all processing will be done at enterprise-level facilities to enable secure, ubiquitous access and leverage enterprise services.

3.4.1. Transform Army Processes End-to-End - AKM Goals 2, 3, and 4

a. Desired End State

Enterprise-wide end-to-end (E2E) processes that improve decision outcomes and operational excellence by facilitating real-time information sharing and collaboration across functional and organizational boundaries.

b. Actions

Transform stand-alone functional processes into streamlined, integrated enterprise-wide processes and multi-functional end-to-end (E2E) processes.

Build information sharing and collaboration into Army E2E Processes, insuring adherence to MID 905 tenets to include “only handle information once (OHIO)” and “post before processing”, to accelerate information dissemination and maximize horizontal sharing of common data sources.

Transform 'forms management' into 'content management for forms data,' to minimize time spent on data collection and entry by capturing data input to web enabled forms and storing it for access and use in a shared knowledge base.

Manage and execute the Army's MID 905 Horizontal Fusion process to implement net-centric initiatives and establish Net-Centric Enterprise Services (NCES), to provide users with assured access to heterogeneous, disparate, and geographically dispersed mission-critical data as well as cutting edge applications that translate the data into relevant information.

Employ Knowledge Process Reengineering (KPR) to optimize knowledge generation capabilities that matter to the decision-maker. KPR is the fundamental rethinking and explicit redesign of processes and systems to improve the creation, sharing, and use of the knowledge critical at the point of decision.

Exploit automated management decision tools to provide the 'business intelligence' necessary for better decision-making.

Synchronize Enterprise Resource Planning (ERP) implementations within the Army to streamline and enhance the effectiveness of support to warfighter operations and achieve the Objective Force's goal of 'foxhole to factory' continuum of operations.

c. Specific Responsibilities

1) CIO/G-6

- NLT 1 Jul 03, in conjunction with Army Enterprise Integration Oversight Office (AEIOO) and AAIC, E-publish guidance for MACOM and functional proponent use in planning and executing process transformation for their respective knowledge domains.
- NLT 1 Aug 03, establish and lead Army IPT to: identify opportunities to integrate cross- and multi-functional processes and create E2E enterprise processes; and to eliminate redundancy across MACOM and functional proponent boundaries by utilizing horizontal fusion tools.
- NLT 1 Oct 03, in coordination with AEIOO and AAIC, develop and E-publish self assessment guidelines for MACOM and functional proponent use in assessing and reporting performance on process transformation.
- NLT 1 Jun 03, in coordination with the Army Publishing Directorate (APD), AA, support transformation from "forms management" to "content management for forms data."

- Approve process transformation plans and exercise oversight of MACOM and functional progress on plans, in coordination with AAIOO and AAIC.
- NLT 1 Mar 04. Develop plan to institutionalize the use of web-enabled decision support tools in Army enterprise processes.
- Ensure process transformation plans are consistent with: approved DoD and Army enterprise processes, through Army ERP integration.
- Identify business processes that are applicable across the DoD and Army enterprise and assure they are addressed in the appropriate process transformation plans (FY 03 and beyond).
- Ensure integration with other related efforts to include: e-army, the Business Initiative Council (BIC) at the DoD and Army levels, joint, DoD and government e-Business/e-Government programs.

2) Administrative Assistant

- NLT 1 Jun 03, develop strategy, with CIO/G-6 support, to transform forms management and achieve a 'revolution in content management' for forms data.

3) MACOMs and Functional Proponents

- Lead process transformation for respective knowledge domains, using the operational architecture in the capstone AKEA as a blue print for transforming and as a basis for managing change to processes.
- NLT 1 Dec 03, submit process transformation plans for approval, in accordance with CIO-G6 guidance
- NLT 1 Oct 05, complete process transformation in accordance with approved plans.
- NLT 1 Jun 03, designate SME to participate in an Army IPT chartered to: identify opportunities to integrate cross- and multi-functional processes and create E2E enterprise processes; and to eliminate redundancy across MACOM and functional proponent boundaries by utilizing horizontal fusion tools.
- Coordinate with CIO/G-6 on appropriate and optimal use of technology to facilitate process transformation (FY 03 and beyond).

- In accordance with schedule approved in process transformation plans, assess the impact and outcomes of process transformation, using the CIO/G6 developed process readiness tool, and e-publish results in a shared, stakeholder environment.

4) Point of Contact

- CIO/G-6 EIO, EIP, and AAIC

3.4.2. Consolidate and Webify Applications - AKM Goals 2 and 4

a. Desired End State

Streamlined, webified Army applications, with real-time access to relevant information and a shared knowledge base, through one Army portal – AKO.

b. Actions

NLT 1 Oct 04, execute AKM guidance Memorandum #2 for applications at all levels of the Army hierarchy, from HQDA functional proponents fielding Enterprise Resource Planning (ERP) systems to uniquely developed unit level systems:

- 'Webify and streamline' applications.
- Reduce the Army application inventory by 50%, through the consolidation and elimination of applications rendered redundant or inefficient by process transformation or webification initiatives.
- Migrate application access to behind Army Knowledge Online (AKO).

c. Specific Responsibilities

1) CIO/G-6

- NLT 1 Oct 04, provide self-assessment tools and guidance to guide proponents and facilitate their transition in migrating applications for access behind AKO.
- Exercise oversight of webification and application consolidation activities across the enterprise.
- Approve application consolidation plans in coordination with ASA(ALT) and AAIC.
- Approve waivers, where applicable.

- Gather requirements from Army Functional Proponents for incorporation and webification on AKO and AKO-S.
- Manage the online Army IT Registry (AITR) database content.
- Track MACOM and functional proponent progress on webification and application consolidation; maintain e-published status on progress in a shared environment, available for pull by leadership and other stakeholders on demand.

2) ASA(ALT)

- Ensure all new software developed under PEO/PMs is developed in accordance with AKM Policy Memo #2.
- Provide updates to the AITR database.
- In coordination with CIO/G-6 approve application consolidation plans.

3) MACOM and Functional Proponents

- NLT Jun 04, execute AKM guidance to 'webify and streamline' applications behind AKO, in accordance with AKM guidance Memorandum #2.
- Report progress towards systems reduction and webification through the Army IT Registry (AITR).
- Enter and keep current all AIS systems in the AITR and fill in all required data fields.
- Include requirements for webification in Mission Need Statements (MNS) and Operational Requirements Documents (ORD).

4) IMA

- Report installation application status to the CIO/G-6 on the AITR.

5) NETCOM/9th ASC

- Build, maintain, and provide system administration of the AITR to meet the requirements specified by CIO/G-6 EIP. Systems Administer AITR until it transitions to AEI-R.
- System Administer AEI-R.

6) AMC CECOM SEC-BEL

- Data administer the online AITR database to track webification status of Mission Critical and Mission Essential Systems. Act as the AITR Help Desk.
- Work with MACOMs and HQDA functional proponents to ensure data within the AITR is complete and up to date.
- Provide input to CIO/G-6 to determine and prioritize improvements to AITR.
- Provide reports to Army CIO/G-6 and the Army CIO Executive Board on MACOM/HQDA proponent system webification status.
- Create and maintain an online user's manual for the AITR.
- Work with NETCOM/9th ASC to prepare AITR to track all systems (MC, ME and other), webification and system elimination/reduction efforts NLT 1 Jan 04.

7) Functional RCIOs

- Report on all existing applications running on the network through to the NETCOM/9th ASC.

8) DOIM

- Report on all existing applications running on the network through the Regional Director/Regional CIO (RCIO) to the ACSIM.
- Identify to NETCOM/9th ASC all applications running on network.
- Develop NCES capable of providing capabilities such as enterprise system management, storage, knowledge discovery, security, messaging, collaboration, and data pull.

9) Point of Contact:

- CIO/G-6 IOS and IOP
- CIO EIP

3.4.3. Functional Processing Centers – AKM Goal 3

a. Desired End State

All functional processing centers are eliminated and processing is transferred into either a DOIM server farm or an Army Processing Center; all processing will be done in an enterprise facility.

b. Actions

Functional Processing Centers (FPC) migrate into general purpose Army Processing Centers (APC) and/or regional server farms under the command, management and operation of NETCOM/9th ASC. Functional proponents retain responsibility for content and applications management. The NETOPS CONOPS is the management concept to be used in support of APCs and the development of implementation strategy and migration plans. The TNOSC supports the management of the APCs.

Concurrent with initiatives to streamline applications and consolidate servers, and in coordination with functional proponents, NETCOM/9th ASC will assume responsibility for a phased transition of FPCs. This phased approach will include:

- Provide NETCOM/9th ASC with visibility and TECHCON over the existing FPCs.
- Plan and implement regional COOP for consolidated services (Enterprise storage servers and applications).
- Migrate selected FPCs within an installation under the operational control of the installation DOIM.
- Migrate selected FPCs to NETCOM/9th ASC APC as regional server farms.
- Convert selected FPCs into NETCOM/9th ASC regional or theater-level APCs by adding functionality and capability to the location. Key among this additional capability will be the location of Area Enterprise Storage systems for use by various installations and organizations within geographic proximity.

NETCOM/9th ASC, in coordination with the owning MACOMs and Functional Proponents, will develop an overall transition plan NLT 1 Apr 04 and begin implementation of the associated transition plan NLT 1 Oct 04.

c. Specific Responsibilities

1) CIO/G-6

- Establish policy on migration of FPCs into APCs. Publish guidance NLT 1 Jan 04.
- Execute the necessary Schedule 8 and other resource transfer actions to implement the migration plan.
- Program and provide funds for enterprise migration, consolidation and sustainment.
- Monitor progress and report as required to Senior Army Leadership.

2) MACOMs and Functional Proponents

- Assist NETCOM/9th ASC in developing an overall implementation strategy and identify resource transfers NLT 1 Apr 04 and begin implementation of the associated migration plan NLT 1 Oct 04.

3) NETCOM/9th ASC

- Develop APC transition plan NLT 1 Apr 04 and assist in the development and execution of resource transfers. Begin executing plan 1 Oct 04.
- Integrate continuous operations into migration plans.
- Work with MACOMs and functional proponents to facilitate process.

4) Point of Contact

- CIO/G-6 IOM and RI
- NETCOM/9th ASC ESTA Service Management Directorate

3.5. SUPPORT STRATCOM CNO AND FULLY IMPLEMENT IA DEFENSE IN DEPTH – AKM GOAL 3

3.5.1. Protect the Army's Portion of the GIG from Cyber Attack – AKM Goal 3

a. Desired End State

The Army enterprise infostructure and network is defended in-depth, as part of the overall defense of the DoD GIG.

b. Actions

The Army Enterprise must adequately protect its networks and infostructure. It must ensure the Army Enterprise information services are available to authorized personnel and that information (public, private, and classified) is not disclosed to or altered by unauthorized personnel and it is protected against individual or state sponsored threats. This requirement applies to legacy Army networks and infostructures as well as the transformation of these networks into the AEI-T. The secured AEI will ensure the Army's portion of the GIG is operational and protected. AEI information assurance will be provided through a robust defense in depth strategy as outlined below:

- Defend the Network and Infostructures. The first layer of AEI defense will be implemented at network and infostructure boundaries. These boundaries include physical and logical boundaries and network, system, and security boundaries (e.g., backbone networks, wireless networks, remote access, etc.).
- Defend the Enclave Boundaries. The second layer AEI defense will be located at Army enclave boundaries. An enclave is defined as a portion of the Army AKEA that has a different security policy and may require additional IA mechanisms (e.g., a deployed communications team may be considered an enclave).
- Defend the Computing Environment. This final layer of AEI defense is the actual IT system itself. The objective for this layer is to secure and protect system applications, servers, networks components, and all computing platforms.
- Enabling Technologies. The supporting infostructure refers to the enabling technologies that support the three Defense-in-Depth IA categories (e.g., public key infostructure (PKI), Common Access Card (CAC), and Biometrics) as well as the management, and detect and respond aspects of the Army defense-in-depth security architecture.

NETCOM/9th ASC, in coordination with the various MACOMs, intelligence organizations and functional proponents, will develop the IA architecture and supporting blueprint for the AKEA.

c. Specific Responsibilities

1) CIO/G-6

- Develop and execute a resource strategy to implement the approved IA architecture.
- Provide IA Policy and oversight.
- Provide guidance for an end-to-end IA architecture and effective security posture that supports Army Transformation.
- Develop and execute the Certificate of Networthiness (CON) policy.

2) ASA(ALT)

- Assure acquisition development programs are in compliance with the Army IA Architecture and are certified as networthy in accordance with Army network policy. Complete the CON prior to Milestone C.

3) G2

- Ensure appropriate resources and priorities are provided and assigned to enable timely intelligence support in accordance with AR 381-11.

4) NETCOM/9th ASC

- Execute IA and CND functions (less intelligence support) as the Army's single focal point for NETOPS/ Computer Network Defense (CND) actions - Defending in Depth.
- Develop a functional description of the objective Army Enterprise IA Architecture View NLT 1 Jun 03.
- Coordinate with MACOMS and Army Components to gather current information assurance status and requirements.
- Act as the Information Assurance functional proponent for all enterprise infostructure initiatives (e.g., Win2K, Active Directory, Enterprise Directory Services (EDS), etc).

- Develop an Army Enterprise Security Policy for the AKEA by 1 Jan 04.
- Develop a phased IA roadmap, migration plan, systems design plan and cost estimate that includes hardware, software, personnel, and the objective Army Enterprise IA defense in depth architecture component of the AKEA NLT 1 Oct 03.
- Begin phased implementation of the IA modernization, integration, and migration plan by 1 Oct 04.
- Develop a phased IA roadmap, migration plan, systems design plan and cost estimate that includes hardware, software and personnel for incorporating the Army non-installation based assets (e.g., Corp of Engineer, USAREC, USAR, ARNG, etc.) into the objective Army Enterprise IA defense in depth architecture component of the AKEA NLT 1 Oct 04.
- Develop and implement a phased migration plan and cost estimate that includes hardware, software, and personnel required to establish an Intelligence Support to NETOPS capability within the NETCOM/9th ASC G2 NLT 1 Apr 04.
- Begin phased implementation of the Army non-installation based assets IA modernization, integration, and migration plan NLT 1 Oct 05.
- Act as intelligence support point of contact for all enterprise infostructure initiatives not supported by another organization, providing support to PEOs and PMs under the auspices of AR 381-11.
- In cooperation with the 1st IO Command, identify and analyze threats to the components of NETOPS (i.e., Network Management, IDM, and IA).
- Provide intelligence support to Enterprise recapitalization, technology insertion initiatives, examination of emerging technologies, Army Infostructure Architecture and Systems Design Reviews (ASDR), and the CON/Certificate to Operate (CTO) process.
- Identify foreign ownership, control, and influence (FOCI) issues relating to vendors seeking to provide IT products and services to the AEI.

- Provide intelligence support to security certification and accreditation activities impacting the AEI.
- Act as the intelligence support proponent for all enterprise infostructure initiatives (e.g., Win2K, Active Directory, EDS, etc).

5) Point of Contact

- CIO/G-6 IONS
- G2
- NETCOM/9th ASC ESTA IA and ACofS, G2

**3.5.2. Support STRATCOM and Computer Network Operations (CNO) - AKM
Goal 3**

a. Desired End State

CROP and situational awareness of the health and defense of the Army's portion of the GIG.

b. Actions

NETCOM/9th ASC, as the Army's single focal point for NETOPS/CND will provide an IA/CND CROP and situational awareness capability for the Army Enterprise. The IA/CND CROP to be integrated as part of the NETOPS CROP and situational awareness. Situational awareness will be in accordance with DoD Computer Network Operations (CNO) directives, and will be provided to U.S. Strategic Command (USSTRATCOM), the DoD CNO proponent, and other service level CNO providers to support a DoD wide IA CROP and situational awareness capability.

Army's single focal point for NETOPS/ CND, NETCOM/9th ASC will execute, through a tiered Network Operations and Security Center (NOSC) structure, appropriate CND directives stipulated by USSTRATCOM and implement the Joint CONOPS for NETOPS requirements for IA, thus providing the "defend, detect and react" components of the Army's Enterprise. NETCOM/9th ASC, in coordination with the various MACOMs, intelligence organizations and functional proponents, will develop the supporting blueprint for an Army IA CROP and situational awareness capability across the Army infostructure.

c. Specific Responsibilities

1) CIO/G-6

- Develop and execute a resource strategy to implement approved IA CROP/ situational awareness capability frameworks as part of the NETOPS capabilities.
- Act in concert with G2 and G3 to coordinate CNO and IA CROP/ situational awareness capability reporting requirements.
- Provide guidance for an End-to-End (E2E) security posture in support of first fielding of the Objective Force Units of Employment and Units of Action.

2) ASA(ALT)

- Require PEOs/PMs compliance with NETOPS CONOPS and AKEA publications and guidelines.
- Assure acquisition development programs are in compliance with the Installation Information Assurance Architecture (I2A2), to include completion of CON certification, prior to Milestone C.

3) NETCOM/9th ASC

- Perform as the Army's single focal point for NETOPS/CND actions.
- Develop a functional description of the objective Army Enterprise IA/CND CROP/situational awareness capability NLT 1 Jun 03.
- Develop and implement a phased migration plan, systems design plan and cost estimate that includes hardware, software and personnel for developing an Army Enterprise IA CROP/situational awareness capability NLT 1 Apr 04. This plan will include incorporating the Army non-installation based assets (e.g., Corp of Engineer, USAREC, USAR, ARNG, etc.).
- Integrate CND and selected CNO operations into the NETCOM/9th ASC NETOPS capabilities to fully implement GO #5, 13 Aug 02. (Completed)
- Operate and maintain the Army components to the Global NETOPS in support of CNO.

- Act as the Information Assurance functional proponent for all enterprise infostructure initiatives (e.g. Win2K, Active Directory, server consolidation).
- Support implementation of E2E security posture in support of first fielding of the Objective Force Units of Employment and Units of Action.
- Develop a concept of operations and supporting resource plan to focus various components of the intelligence process to benefit defense of the AKEA; NETOPS (IA, IDM, telecommunications network management), and security certification and accreditation. Submit CONOPS for CIO approval NLT Dec 02 (completed), and inclusion in POM submission.

4) Point of Contact

- CIO/G-6 IONS
- NETCOM/9th ASC ESTA IA

4.0 ENTERPRISE ENGINEERING SUPPORT TO AKE – AKM GOAL 3

4.1. CORE ENTERPRISE ENGINEERING SUPPORT – AKM GOAL 3

a. Desired End State

A core funded capability for C4IM enterprise engineering support, dedicated to execution of the AKE.

b. Actions

The Army will examine existing C4IM engineering capabilities and determine options to achieve the desired end state.

These options and recommendations will be briefed to the Army Secretariat for decision on implementation.

The C4IM engineering capability will provide the Army with core expertise and competencies to perform:

- Systems engineering to support the implementation of the AEI Campaign Plan and AKM Goals 2, 3, and 4, above acquisition program levels.
- Operational engineering support for Army NETOPS at the local, regional, theater, and enterprise levels.

- Technical engineering support to the Army's Networthiness process and for issuing CON and CTO.
- Engineering support for development of the AKEA.

The examination of engineering capabilities will consider, at a minimum the following organizations:

- AMC CECOM
- Research, Development, and Acquisition Information Systems Activity (RDAISA)
- MACOM and functional proponent engineering assets
- NETCOM/9th ASC ESTA

End state options will consider: outsourcing of functions currently performed by Army military and civilian personnel; centralizing funding and oversight; best practices; consolidating capabilities; the continued need for existing contract engineering support; and, retention of Subject Matter Experts (SME).

c. Specific Responsibilities

1) CIO/G-6

- Identify, in coordination with NETCOM/9th ASC and AMC CECOM, the C4IM engineering capability required to meet the desired end state, NLT 1 Jul 03.
- Lead an Army task force to develop courses of action for achieving desired end state and present recommendations for Army leadership decision NLT 1 Oct 03.
- Ensure that courses of action are in consonance with the Third Wave AKE organizational design plan addressed in Part II paragraph 5.1.
- Based on adopted course of action, develop transition plan NLT 1 Mar 04, with implementation of approved course of action to begin in FY 05.
- Take required PPBES actions to affect resource transfers and establish funding in the FY 06 POM.

2) Specified MACOMs and Functional Proponents

- 1 Jun 03, designate SME to participate in a CIO/G-6 led task force to collect supporting data and develop courses of action to achieve end state.

3) AMC CECOM

- Assist CIO/G-6 and NETCOM/9th ASC in identifying the C4IM engineering capability required to meet the desired end state, NLT 1 Jul 03.
- By 1 Jul 03, designate SME to participate in a CIO/G-6 led task force to collect supporting data and develop courses of action to achieve end state.

4) NETCOM/9th ASC

- Assist CIO/G-6 and AMC CECOM in identifying the C4IM engineering capability required to meet the desired end state, NLT 1 Jul 03.
- By 1 Jun 03, designate SME to participate in a CIO/G-6 led task force to collect supporting data and develop courses of action to achieve end state.

5) Point of Contact

- CIO/G-6 CXO
- NETCOM/9th ASC ESTA

4.2. CENTRAL DESIGN ACTIVITY DIVESTITURE – AKM GOAL 3

a. Desired End State

Expand use of Commercial Off-The-Shelf (COTS) software and divest Central Design Activities (CDA) without any adverse operational impact while yielding cost savings.

b. Actions

OSD issued MID 905 on 18 Dec 02, directing all Military Departments (MILDEP) to evaluate their CDAs for divestiture. As DoD migrates to expanded use of COTS software, the need for in-house software development may significantly diminish as demonstrated by the recent divestiture of civilian and contractor personnel supporting the Army's Commodity Command Standard System and

Standard Depot System, once performed by the St. Louis, MO and Letterkenny, PA CDAs. The funds recouped from divestiture of these two CDAs were reallocated to the Army's Wholesale Logistics Modernization program.

In accordance with MID 905, each MILDEP is directed to review the efficacy of its CDAs (supporting all sustaining base, command and control, intelligence and weapon systems) and forward divestiture plans that identify expected Full-Time Equivalent (FTE) reductions and related savings to the DoD CIO NLT 1 Jun 03 for inclusion in the FY05-09 Budget Estimate Submission. In addition, the MILDEPs are directed to identify the modernization initiatives to which FTEs and projected savings from anticipated divestitures will be reallocated. The Army was asked by DoD CIO to co-lead the CDA divestiture effort by assisting in the development of implementing instructions and review of agency CDA divestiture plans.

For clarification purposes, OSD defined CDA (under Defense Management Report Decision 918, Defense Information Infrastructure, 1992) as a designated organization within a DoD Component which, as a minimum, has responsibility for developing, maintaining, or providing technical assistance on IT/National Security System (NSS) in use at more than one location (Component-wide, MACOM-wide, and/or at multiple installations).

c. Specific Responsibilities

1) CIO/G-6

- Provide guidance to MACOMs to develop divestiture plans (completed).
- Develop Army's CDA divestiture plan, with input from the MACOMs and functional proponents. Submit to the DoD CIO NLT 30 Jun 03.
- Assess impact of Army's "third wave" outsourcing initiative on MID 905 CDA divestiture to eliminate any duplication.

2) Army Material Command (AMC)

- Assist DoD CIO/Army CIO/G-6 by providing lessons learned in the logistics divestiture.
- Determine if any activity meets the criteria of CDA and provide divestiture plans to CIO/G-6 NLT 30 May 03.

3) MACOMs and Functional Proponents

- Determine if any activity meets the criteria of CDA and provide divestiture plans to CIO/G-6 NLT 30 May 03.

4) Point of Contact

- CIO/G-6 IOM
- AMC

5.0 AKM TRANSFORMATION TO SUPPORT OBJECTIVE FORCE - AKM GOAL 1, 2, 3, 4 AND 5

5.1. SUPPORT OF HOMELAND SECURITY MISSIONS – AKM GOALS 1, 2, 3, 4, AND 5

a. Desired End state:

Seamless and adequately protected interoperability between military, governmental, and civil agencies in support of Homeland Security.

b. Actions

The New Homeland Security Department is chartered to develop a national emergency communications plan that will link federal, state and local communities into an interoperable communications system. NORTHCOM is the Combatant Commander of the CONUS Theater. The Army Service Component Command (ASCC) for NORTHCOM is the Commanding General (CG), Forces Command (FORSCOM) in his capacity as the CG Army North (ARNORTH).

If the Army is designated the DoD Executive Agent (EA) for Homeland Security communications, the ASCC for NORTHCOM will coordinate signal provisioning for Homeland Security with NETCOM/9th ASC.

The Installation Management Agency (IMA) regions are designed to facilitate military support to civil authorities. The NETCOM/9th ASC and its RCIOs will work appropriate connectivity and restoral issues with NORTHCOM, NGB, USAR, Federal Emergency Management Agency (FEMA), and other agencies within the region.

The Army may be designated the DoD EA for NETOPS in support of NORTHCOM. NETCOM/9th ASC has the mission to operate, manage and defend the Army's CONUS infostructure in support of both STRATCOM and NORTHCOM. There are multiple initiatives outlined in this plan to move the current fragmented CONUS infostructure to the AEI-T. The additive requirements to support emerging NORTHCOM and STRATCOM needs may

generate a change to current force structure requirements. The signal force structure impacts to support emerging NORTHCOM Homeland Security communications requirements, the CONUS NETOPS mission, and STRATCOM should be explored by CIO/G-6 in conjunction with FORSCOM, USAR, IMA, and NGB.

c. Specific Responsibilities

1) CIO/G-6

- Coordinate with the J-6 and the Army G3 to have the Army designated the DoD EA for Homeland Security communications.
- If designated as the EA, coordinate with NORTHCOM/Army Component to determine and implement communications requirements using existing capabilities of the Army's components.
- Explore with NGB/OCAR/FORSCOM/IMA/NETCOM/9th ASC signal force structure changes required to support NORTHCOM (FORSCOM, state and regional) Homeland Security communications requirements and other initiatives in this plan.

2) G2

- Ensure Army intelligence priorities are periodically reviewed to ensure resources are available to identify and analyze threats to the Army's Executive Agency role.

3) NETCOM/9th ASC

- Support J2, NORTHCOM ASCC with NETOPS-related intelligence and production requirements to identify knowledge gaps relating to threats to Army communications resources and functions relating to Homeland Defense support.
- Support NORTHCOM ASCC, as the Army's EA to operate, manage and defend the Army's CONUS Infostructure.
- Provide the CONUS IT connectivity for NORTHCOM ASCC within the ARFOR in accordance with standard connectivity procedures.
- Identify, in coordination with RCIOs, connectivity support requirements between the Army and FEMA Regional HQS within their IMA region.

- Support C4IM operations for homeland security, disaster relief, terrorist prevention, and intelligence planning with the IMA Regional Director, in coordination with USAR and ARNG.

4) IMA

- Program for and provide for local connectivity for homeland defense requirements, for example, National Crime Information Center (NCIC) database, FBI Joint Terrorism Task Force databases, Force Protection IT systems, and Mass Casualty and Emergency Operations Center planning.
- Participate in the communications integration planning efforts for the Installation with surrounding communities.
- Support military support to civil authority missions when required.

5) Point of Contact

- CIO/G-6, IONS
- NETCOM/9th ASC G3 and G2

5.2. ANALYSIS OF SIGNAL FORCE STRUCTURE – AKM GOAL 3

The analysis of the Signal Force structure is comprised of two interrelated initiatives. The first is the Total Army Analysis (TAA)-11 Signal Capabilities Study, which will enable the Signal Corps to support Army Operations through 2011 and provide a bridge to the Objective Force. The second initiative transforms the Signal Force to support the Objective Force across the full spectrum of Army Operations 2010 and beyond.

5.2.1. Building the Interim Signal Force (TAA-11)

a. Desired End State

By 2011, a Signal Force that provides the Army a robust, viable signal support capability across the spectrum of operations, supports the TAA-11 Force, and bridges to the Objective Force.

b. Actions

TRADOC, in coordination with CIO/G-6, NETCOM/9th ASC, FORSCOM, USAR, and NGB will form an integrated concept team (ICT) and conduct a study that will lead to the shaping of the Interim Signal Force. The Signal Corps requires an integrated Interim Signal Force strategy to synchronize diverse efforts, develop Total Army Assessment (TAA-11) input, submit Force Design Updates, and

ensure units of the Interim Signal Force are relevant and deployable with the required capabilities.

The following ongoing actions have been identified for inclusion in the Interim Signal Force integrated plan:

- Force Design Update (FDU) 02-1. Theater Structure. Implementation of the HQDA approved Theater Tactical Signal Battalion Version 2 (TTSB V2) for the 7th Signal Brigade, and implementation of the TAA-09 approved Theater Injection Point (TIP) into three theater Signal Brigades.
- FDU 02-2. NETOPS Structure. Establishes the Army's Enterprise NETOPS backbone. Develops a standard Table of Organization and Equipment (TOE) organization for the seven TNOSC, the Army Network Operations Security Center (ANOSC), and Regional NOSC's (RNOSC).
- FDU 03-1. Interim tactical Theater Signal Force. Implements the DA-directed Integrated Theater Signal Battalion (ITSB), the updated Theater Installation and Networking (TIN) Company, and the Joint Command, Control, Communications and Computer Package (JC4P) in support of Army Service Component Command (ASCC) headquarters.
- The TSC-Army (TSC-A) Study. The 335th TSC-A initially led this study. It now needs to be led by TRADOC (Signal Center) and included as a part of the Objective Signal Force Study.
- Organizing the CONUS Theater Signal Force. Study activation of a CONUS Theater Signal Command and CONUS TNOSC in support of NORTHCOM, and Homeland Security. With the emergence of CONUS as a separate theater under NORTHCOM, support requirements must be determined and implemented. These actions must be worked in consonance with the other Interim Signal Force Actions.
- Establishing the SWA Theater Signal Force. Implementing the HQDA approved SWA strategic signal brigade (160th), complete with TNOSC and Regional Computer Emergency Response Team (RCERT).
- Corps and Division initiatives. Implement standard data packages/SATCOM additions in Corps/Division Signal Units; submit necessary FDUs to bring the Echelons Corps and Below (ECB) force to Interim Force capabilities.

The Signal Capabilities Study and TAA-11 should address all of the above Interim Signal Force Actions and be completed NLT 1 Sep 03.

c. Specific Responsibilities

1) CIO/G-6

- Designate members to participate in TRADOC led ICT.
- Coordinate with appropriate staffs and commanders to assist TRADOC in the study effort.
- Coordinate resourcing of approved study results.

2) G3

- Provide priorities and guidance, validate requirements and approve the TAA-11 Signal Force structure.
- Participate as a member of the TRADOC ICT.
- Assist TRADOC in processing approved changes through the TOE/FDU/TAA cycles.

3) TRADOC

- Designate Signal Center (SIGCEN) to be TRADOC's Executive Agent for the conduct of Signal Force Capabilities Assessment. (completed)
- Task SIGCEN to analyze after action reports and formulate lessons learned regarding Signal Force capabilities required by warfighters in Somalia, Bosnia, Afghanistan, and Operation Iraqi Freedom, and revise current doctrine to reflect warfighting requirements and Signal Force capabilities. (completed)
- Establish an ICT to conduct study, with members from the HQDA staff, SIGCEN, FORSCOM, NGB, USAR, NETCOM/9th ASC, and other MACOMs, etc. Standup ICT NLT 1 Jun 03.
- Develop and submit revised rules of allocation for the TAA-11 Signal Force to HQDA G3 for approval and inclusion in TAA-11 NLT Jul 03.
- Brief study results to TAA-11 General Officer Steering Committee (GOSC) in Sep 03.
- Implement approved actions in TAA-11, FDUs, and other appropriate processes.

4) FORSCOM

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to the CONUS Corps/Division and Echelons above Corps (EAC) Signal Force structure.

5) Outside CONUS (OCONUS) MACOMs/ASCCs

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to theater Signal Forces.

6) USAR

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to Army Reserve Signal Forces.

7) ARNG/NGB

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to Army Guard Signal Forces.
- Identify specific Homeland Security (HLS) Signal requirements.

8) NETCOM/9th ASC

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to the Army's theater, strategic, and sustaining base Signal Forces.

9) Point of Contact

- TRADOC
- CIO/G-6
- HQDA G3
- FORSCOM

- NETCOM/9th ASC G3
- USAR Signal Organizational Integrator (OI)
- ARNG/NGB Signal OI

5.2.2. Building the Objective Signal Force

a. Desired End State

A transformed network-centric Army supported by a transformed Signal force that provides Signal support across the full spectrum of Army Operations.

b. Actions

TRADOC will have the Objective Force Echelonment Decision completed in Jun 03. This decision will substantially impact the composition of the Objective Signal Force structure.

Building on the recommendations of the Signal Capabilities study, TRADOC SIGCEN will reconvene the ICT addressed in paragraph 5.2.1, to develop the Signal Objective Force. Identify the required changes in signal force structure to meet the capabilities required in the Objective Force; recommend structural changes and enhancements; and align the force with the Objective Force echelonment decisions. The outcome is expected to focus, at a minimum, on: missions and roles of the Theater Signal Commands; missions and roles of Division, Corps, and Theater signal forces; the role of NETOPS across all echelons; and the structuring/equipping of the Army's Components to insure all signal forces are relevant, in the Objective Force. The results of this study should be used to develop Objective Force structure and TAA-13 rules of allocation and baselines.

c. Specific Responsibilities

1) CIO/G-6

- Designate members to participate in TRADOC led ICT.
- Coordinate with appropriate staffs and commanders to assist TRADOC in the study effort.
- Coordinate resourcing of approved study results.

2) G3

- Provide priorities and guidance, validate requirements and approve the TAA-13 Signal Force structure.

- Participate as a member of the TRADOC ICT.
- Assist TRADOC in processing approved changes through the TOE/FDU/TAA cycles.

3) TRADOC

- Develop the Objective Force echelonment.
- Reconvene the ICT established above (5.2.1) to develop the Signal Objective Force.
- Develop and submit revised rules of allocation for the TAA-13 Signal Force to HQDA G3 for approval and inclusion in TAA-13.
- Implement approved actions in TAA-13, FDUs, and other appropriate processes.

4) FORSCOM

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to the CONUS Corps/Division and EAC Signal Force structure.

5) OCONUS MACOMs/ASCCs

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to theater Signal Forces.

6) USAR

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to Army Reserve Signal Forces.

7) ARNG/NGB

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to Army Guard Signal Forces.
- Refine HLS Signal requirements.

8) NETCOM/9th ASC

- Participate as a member of the TRADOC ICT.
- Provide input to TRADOC on recommended changes to the Army's theater, strategic, and sustaining base Signal Forces.

9) Points of Contact

- TRADOC
- CIO/G-6
- HQDA G3
- FORSCOM
- NETCOM/9th ASC G3
- USAR Signal OI
- ARNG/NGB Signal OI

**5.3. INTEGRATE THE ARMY RESERVE/ARMY GUARD INTO THE AKE –
AKM GOAL 1 AND 3**

To meet the design of the Objective Force, all Components must be fully integrated to eliminate redundancy, combine staff for efficiency, and consolidate Component stovepipe networks and systems. This includes Enterprise Networks, a single NETOPS operation, and multi-component staff at all levels, and operation of the AKE as an Enterprise.

5.3.1. Integrate the Army Reserve

a. Desired End State

Army Reserve fully integrated as part of the AKE to support the Objective Force.

b. Actions

Many of the actions to achieve full integration of the Army Reserve into the AKE have been discussed in the previous paragraphs. The integration of NETOPS CONOPS is outlined in Part 1, paragraph 3.1. The AKEA is discussed in Part 1, paragraph 3.2. Combination of the Component Networks is detailed in Part 1, paragraph 3.3. The USAR is included as a partner in the development of support to Homeland Security as outlined in Part 1, paragraph 5.1. The USAR is also included as a partner in the redesign of the Signal Force Structure, addressed in

Part I, paragraph 5.2. This section will discuss how USAR CIO will be integrated into the CIO/G-6 of the Army, USAR NOSC operations will be integrated into NETCOM/9th ASC, and in coordination with FORSCOM examine the transfer of theater level signal units to NETCOM/9th ASC.

Merge the CIO functions of USAR into the CIO/G-6. Align personnel, resources, and missions as jointly agreed from USAR CIO to CIO/G-6. Ensure that all personnel are fully engaged in the AKE mission.

In coordination with FORSCOM examine the realignment of operational theater signal units under the USAR into NETCOM/9th ASC. Combine USAR NOSC operations into the TNOSC redesign, which will be defined and based on best business practices and operational imperatives.

Ensure realigned staffs, TNOSCs, and unit assignments meet the capabilities required for the Objective Force.

c. Specific Responsibilities

1) CIO/G-6

- In coordination with the USAR CIO, merge the USAR CIO functions and resource alignments into the CIO/G-6, NLT 1 Oct 03.
- Ensure all USAR personnel realigned to the CIO/G-6 are fully integrated into the mission of the CIO/G-6, placing individuals in positions of responsibility commensurate with grade and skills, NLT 1 Oct 03.

2) USAR

- In coordination with the CIO/G-6, merge the USAR CIO functions and resource alignments into the CIO/G-6, NLT 1 Oct 03.
- In coordination with CIO/G-6 and NETCOM/9th ASC, determine the appropriate realignment of USAR personnel into NETCOM/9th ASC.
- In coordination with NETCOM/9th ASC, combine USAR NOSC operations into the TNOSC redesign, which will be defined and based on best business practices and operational imperatives, NLT 1 Oct 04.
- Coordinate with NETCOM/9th ASC and FORSCOM in examining the assignment of USAR theater signal units to NETCOM/9th ASC, NLT 1 Oct 05.

3) FORSCOM

- Coordinate with NETCOM/9th ASC and USAR in examining the assignment of USAR theater signal units to NETCOM/9th ASC, NLT 1 Oct 05.

4) NETCOM/9th ASC

- Combine USAR NOSC operations into the TNOSC redesign, which will be defined and based on best business practices and operational imperatives, NLT 1 Oct 04.
- Ensure all USAR personnel aligned to NETCOM/9th ASC are fully integrated into the mission of the NETCOM/9th ASC, placing individuals in positions of responsibility commensurate with grades and skills.
- In coordination with USAR and FORSCOM, examine the realignment of USAR theater signal units to the command of NETCOM/9th ASC, NLT 1 Oct 05.

5) Points of Contact

- CIO/G-6 CXO/EI
- USAR
- NETCOM/9th ASC

5.3.2. Integrate the Army Guard

a. Desired End State

Army National Guard fully integrated as part of the AKE to support the Objective Force.

b. Actions

Many of the actions to achieve full integration of the Army National Guard into the AKE have been discussed in the previous paragraphs. The integration of NETOPS CONOPS is outlined in Part 1, paragraph 3.1. The AKEA is discussed in Part 1, paragraph 3.2. Combination of the Component Networks is detailed in Part 1, paragraph 3.3. The NGB is included as a partner in the development of support to Homeland Security as outlined in Part 1, paragraph 5.1. The ARNG is also included as a partner in the redesign of the Signal Force Structure, as addressed in Part 1, paragraph 5.2. This section will discuss other actions

recommended by the TAGs/NGB to further integrate the ARNG into the AKE. These actions include:

- Develop a Memorandum of Agreement (MOA) between the Chief NGB and the Army Staff, which outlines the integration of the ARNG into the AKE.
- Stand up a second CONUS TNOSC using the current Guard Network Operations Center (NOC) in Arlington, VA. (TNOSC redesign)
- Establish a Guard acquisition entity in ASA(ALT) PEO EIS.
- Establish SLA with each TAG to provide Enterprise IM services.

The CIO/G-6 will work in coordination with the Chief, NGB to establish an MOA that details the integration of the ARNG into the AKE. This will include as a minimum the definition of enterprise services and how they will be delivered; relationships of NGB elements and TAGs to NETCOM/9th ASC and RCIOs; acquisition support for TAGs and ARNG elements; TNOSC redesign; and development of the NGB CONOPS and Architecture and how they are integrated into the NETOPS CONOPS and AKEA.

The ARNG NOC will become part of the TNOSC redesign, integrating GUARDNET, and other assigned missions into the Enterprise. As a minimum, the TNOSC will be under the operational control of NETCOM/9th ASC. This will be an Enterprise operation comprising multi-component staff.

Per the 11 Mar 03 meeting with the SA, ASA(ALT) will establish an acquisition entity within PEO EIS to provide IT acquisition support to the NGB.

NETCOM/9th ASC and NGB will establish SLAs with each state TAG to identify the baseline services provided by the enterprise and the resourcing strategy,

c. Specific Responsibilities

1) CIO/G-6

- Work in coordination with the NGB to establish an MOA that details the integration of the ARNG into the AKE, NLT 1 Jul 03.
- Coordinate all actions at the headquarters level to ensure that TNOSC redesign and acquisition entity are established.
- Establish a joint CIO/G-6, USAR, and NGB task force to address TAG goals and concerns, and integration into the Enterprise, NLT 1 May 03.

- Work with NETCOM/9th ASC and NGB to establish the baseline services and funding strategy for SLAs with the TAGs.

2) ASA(ALT) PEO EIS

- In coordination with NGB, establish an acquisition entity in PEO EIS to execute NGB missions, using the existing NGB Program Management (PM) organization, NLT 1 Oct 03.

3) NGB

- In coordination with ASA(ALT), establish an acquisition entity in PEO EIS to execute NGB missions, using the existing NGB PM organization, NLT 1 Oct 03.
- Designate a Brigadier General to head the NGB IM Enterprise effort and work as part of the CIO/G-6, USAR, and NGB task force to address TAG goal and concerns, NLT 1 Jun 03.
- Participate in the TNOSC redesign effort, focusing on the integration of the Guard NOSC in the WASH DC area under the OPCON of NETCOM, NLT 1 Oct 03.
- In coordination with NETCOM/9th ASC, establish SLA with each state TAG, starting in 1 Oct 03.

4) USAR

- Work as part of the CIO/G-6, USAR, and NGB task force to address TAG goal and concerns, NLT 1 Jun 03.

5) NETCOM/9th ASC

- In coordination with the NGB and USAR, execute TNOSC redesign and establish OPCON over the Guard NOSC in Arlington, VA, NLT 1 Oct 03.
- In coordination with NGB, establish SLA with each state TAG, starting in 1 Oct 03.

6) Points of Contact

- CIO/G-6 CXO
- NGB
- USAR

- ASA(ALT) PEO EIS
- NETCOM/9th ASC

PART 2 – IRREVERSIBLE MOMENTUM

1.0 GOAL 1 - ADOPT GOVERNANCE AND CULTURAL CHANGES TO BECOME A KNOWLEDGE-BASED ORGANIZATION

1.1. AKM CAPABILITY MATURITY MODEL

a. Desired End State

An AKM strategy executed in progressive levels that build upon the previous level results.

b. Actions

The AKM Capability Maturity Models (CMM) will be developed, baselined, and promulgated to facilitate AKM Strategy execution across the enterprise.

This approach to improving organizational performance has been successfully used in industry and government as evidenced by the Software Engineering Institute's CMM. The AKM CMM (Figures 2.1-1 and 2.1-2) consists of the following levels:

Level 1: Knowledge Sharing:

Individuals provide access to information and knowledge to all members of their community. Individuals perform their knowledge work activities alone without assistance from others; however, they are enabled to obtain or share information/knowledge with others.

Level 2: Knowledge Collaboration:

Individuals team with others in performing knowledge work activities (acquiring, analyzing, organizing, codifying, transmitting, using, or learning from the application of information or knowledge).

Level 3: Knowledge Innovation:

Innovations occur in the performance of knowledge work activities or in the quality of the mission/function knowledge base. This builds on sharing and collaboration established in the previous maturity levels.

Stages within each of these maturity levels depict an increasing scope of influence and participation ranging from the smallest functional team to the largest global environment. See Figures 2.1-1 and 2.1-2.

AKM CMM					
Maturity Level Stages					
3 Innovation	Team	→	Functional Domain	→	Mission → Enterprise → Global
2 Collaboration	Team	→	Functional Domain	→	Mission → Enterprise → Global
1 Sharing	Team	→	Functional Domain	→	Mission → Enterprise → Global

Figure 2.1-1 AKM CMM Maturity Level Stages

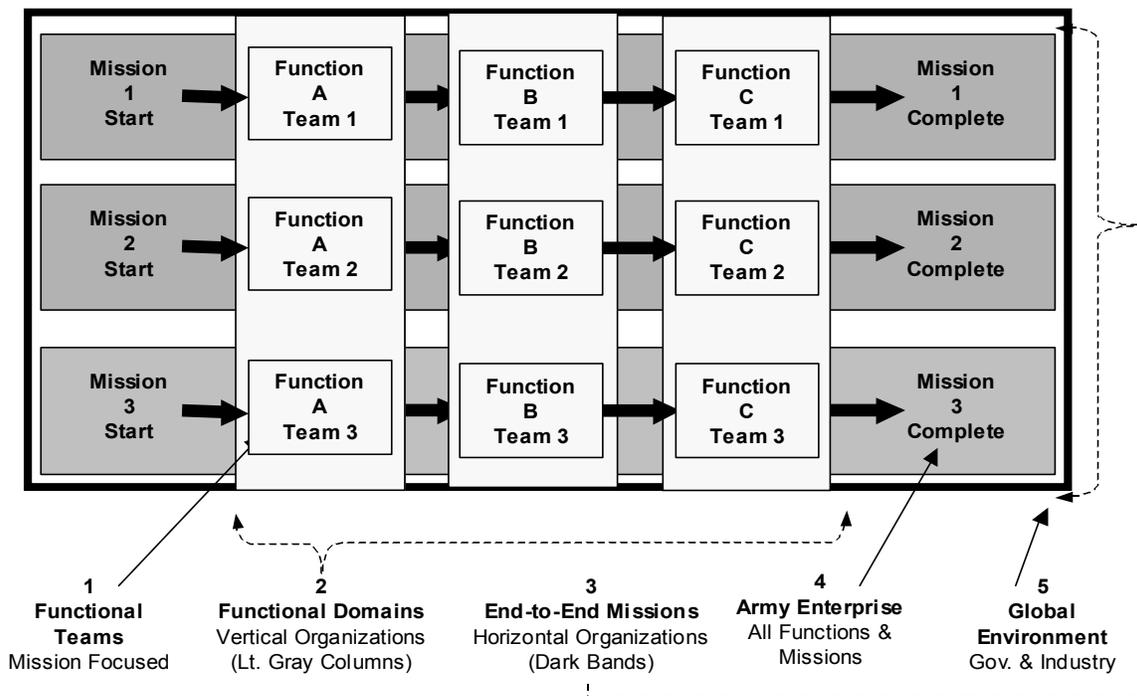


Figure 2.1-2 AKM CMM Stage Descriptions

c. Specific Responsibilities

1) CIO/G-6

- Develop partnerships with Functional Domains to promulgate the AKM CMM and facilitate AKM strategy execution.

2) MACOMs and Functional Proponents

- Implement the AKM CMM to optimize mission accomplishment.

3) Point of Contact

- CIO/G-6 AKM

1.2. RECORDS MANAGEMENT

a. Desired End State

The transition of the Records Management Program and its subprograms to the garrison Adjutant General staff and continue transition to a paperless environment with continued Army G1 proponentcy and oversight by the CIO/G-6.

b. Actions

Phase I Actions:

The Director of Information Management (DOIM) is the staff proponent responsible for the records management program at the garrison level.

The Chief Information Officer/G6 (CIO/G-6) is responsible for the development of the reporting chain of all requirements through the Installation Management Agency (IMA) to the Army G1.

The CIO/G-6 will coordinate with the ACSIM, NETCOM, IMA, and the Army G1 on the issues of Freedom of Information Act (FOIA) release authority and Official Mail Management (OMM) reporting.

The CIO/G-6 will coordinate with the Army G1 on the future support of document management and data warehousing issues.

The CIO/G-6 with the Army G1 will identify within the 14 Major Army Commands (MACOM) the records management/official mail spaces for movement to the Table of Distribution and Allowances (TDA) of the IMA Regional Director (RD) to support the mission. These personnel will be under the OPCON of the NETCOM/9th ASC RCIO until such time as the garrison Adjutant General (AG) takes over the mission.

The Army G1 will appoint the IMA RD release authorities for FOIA and Privacy Act issues. The Army G1 and the CIO/G-6 will fix the doctrinal mission assignment for these areas within appropriate (AG or Signal) deployable assets. This will be an item of special interest in the signal force structure study. The IMA will ensure requirements are vetted through the CIO/G-6 to the Army G1.

The Army G1 will initiate actions during the transition period to link the Army's FOIA program (AR 25-55 and 5 U.S.C. Section 552) with the Army's Operations Security (OPSEC) Program (AR 530-1). The Army's OPSEC program and a Commander's Essential Elements of Friendly Information (EEFI) (as defined in AR 530-1) will be appropriately considered, consistent with the FOIA's exemptions, when evaluating information for public release.

The G3 is the Army proponent for the Operational Security (OPSEC) program. The G1 is the Army proponent for the FOIA program.

Phase II Actions:

The Army G1 will develop a plan NLT 1 Oct 03, to move records management functions to the Adjutant General on the garrison staff NLT 1 Oct 04, as the DA proponent for the Records Management Program and its subprograms, including:

- Army Records Information Management System (ARIMS)
- Official Mail and Distribution
- Army Correspondence
- Freedom of Information Act
- Army Privacy Program
- Rulemaking
- Dictionary of US Army Terms
- Authorized Abbreviations and Brevity Codes
- Compilation of Army Addresses
- Office Symbols
- Research of Unit Records Program
- Management Information Control
- Declassification of Records over 25 years old

c. Specific Responsibilities

1) CIO/G-6

- In accordance with GO #3 and the FOIA, the CIO/G-6 has oversight of these functional areas.
- With the Army G1 fix the doctrinal mission assignment for these areas.
- With the ACSIM, IMA, and the MACOMS identify Records Management positions for transfer to IMA G1 TDAs.
- Develop and execute a resource strategy to implement approved NETCOM/9th ASC requirements until Records Management/Official Mail is taken over by garrison AG staff.

2) G1

- DA functional proponent for the records management and its subprograms.
- Identify G1 responsibilities of planning for emergency management of vital records.
- Identify the current MACOM records management and official mail manager spaces and determine how many man-years are required to execute the records management and official mail missions.
- In Phase II, work with IMA and MACOMs to identify and transfer personnel from MACOMs to Region Director staffs and identify which positions on installation transfer to garrison AG staff.
- Identify FOIA and Privacy Act release authorities above the garrison level.
- With the CIO/G-6 fix the doctrinal mission assignment for these areas.
- Develop a plan to transform the mission responsibility at the installation and regional levels.
- Provide oversight and implementation guidance

3) IMA

- In Phase II, work with G1 and MACOMs to identify and transfer personnel from MACOMs to Region Director staffs and identify which positions on installation transfer to garrison AG staff.

4) MACOMs

- In Phase II, work with G1 and IMA to identify and transfer personnel from MACOMs to Region Director staffs.

5) NETCOM/9th ASC

- Via the RCIOs provide OPCON of Records Management personnel at the IMA RD until these functions are taken over by garrison AG staff.
- Provide interim oversight and implementation guidance.
- Monitor interim delivery of baseline services for metrics purposes.
- In the interim, forward reports to CIO/G-6 from RCIO.
- Work with RD, CIO/G-6, and Army G1 to resolve implementation issues.
- In OCONUS, the RCIO has overall responsibility for records management, publishing management, and all subordinate subprograms for all Army units in the RCIOs area of responsibility and will continue to have this responsibility until it is taken over by garrison AG personnel.

6) DOIM

- Provide interim services in accordance with baseline services and applicable Service Level Agreements for above baseline services.
- Identify outyear funding requirements; short-fused UFRs as applicable.
- Provide interim reports as required through the RCIO.
- Work with RCIO to resolve issues.
- In OCONUS, supporting signal battalions are responsible for records management, publications management, and all subordinate subprograms for all Army units supported by the

installation until these functions are taken over by garrison AG personnel.

7) Points of Contact

- CIO/G-6 CXO and EIS
- G1

1.3. DOIM BUDGET

a. Desired End State

The DOIM budget will support DOIM operational requirements and baseline services.

b. Actions

The ACSIM in conjunction with the CIO/G-6 and IMA will decide how to resource baseline services. A DOIM budget blueprint will be produced NLT 1 Jun 03. The blueprint will include but not be limited to, requirements for current operations, Temporary Duty (TDY), awards, overtime, labor, contracts, and infostructure revitalization. The CIO/G-6 will, with NETCOM/9th ASC, DOIMs, IMA, and ACSIM, define the baseline service requirements on a yearly basis for implementation two years in the future.

c. Specific Responsibilities

1) CIO/G-6

- Support the ACSIM in resourcing the baseline service requirements on a yearly basis for implementation in the POM.
- Support the ACSIM in monitoring execution of baseline services and coordinate appropriate strategies to match DOIM resources with baseline service objectives.

2) ACSIM

- Publish the baseline services that will be implemented two years out.
- Resource the baseline service requirements on a yearly basis for implementation in the POM.

3) IMA

- Coordinate appropriate strategies to match DOIM resources with baseline service objectives.
- Manage resources to support baseline services.

4) NETCOM/9th ASC

- Make recommendations to CIO/G-6 on modifications to baseline services (i.e., discontinuance of old technology/replacement with new).
- Identification of cost saving/improved service alternatives and enterprise solutions.
- As an advocate for DOIM baseline services, defend requirements to CIO/G-6, ACSIM, and IMA, prioritize requirements for the enterprise and solicit support.
- Provide IMA RD the technical review and validation of the consolidated C4IM budget for each region. The budgets will separately identify DOIM resource requirements to achieve baseline service objectives.

5) DOIM

- Will develop an annual operating budget for internal DOIM requirements, delivery of common C4IM services, and projected infostructure revitalization.
- Separately identify resources needed to achieve baseline services.
- Manage funding for on-going infostructure operations and migrated AD operations.
- Coordinate and provide budget requirements to the garrison resource management office for inclusion in the garrison budget submission to the RD.

6) Points of Contact

- CIO/G-6 RI and IOM
- NETCOM/9th ASC ESTA/RCIO

1.4. MACOM AND FUNCTIONAL PROPONENT C4IM BUDGET

a. Desired End State

MACOM and Functional Proponent budget will support mission operational C4IM requirements and reimbursable baseline services.

b. Actions

The MACOMs and Functional Proponents, in conjunction with the CIO/G-6 and the ACSIM, will identify C4IM requirements in the POM for workplace information technology requirements above the baseline services provided by the IMA and DOIMs. These requirements will be submitted to the CIO/G-6 for inclusion in the CPIM process. The CIO/G-6, with the G3 and G8, will lead the PEGs in validation and prioritization of C4IM requirements.

c. Specific Responsibilities

1) CIO/G-6

- Support validated MACOM C4IM requirements through the CPIM process for implementation in the POM.
- Task AAA to examine MACOM requirements and develop a methodology to budget for workplace IT (i.e., personal computers, printers, inside-the-building networking and software that enables use of E-mail, word processing, graphics, collaboration, and web-base applications) NLT 1 Jun 03. (completed)

2) ACSIM

- Publish the baseline services that will be implemented two years out.
- Resource the baseline service requirements on a yearly basis for implementation in the POM.

3) AAA

- Examine MACOM requirements and develop a methodology to budget for workplace IT NLT 1 Sep 03.

4) NETCOM/9th ASC

- Forecast and document reimbursable fees for MACOMs' and Functional Proponents' long haul communications.

- Work with MACOMs and Functional Proponents to reconcile bills for long haul communications.

5) MACOMs and Functional Proponents

- Program and justify workplace C4IM requirements for their subordinate tenant organizations in accordance with reimbursable fee rates and C4IM sustainment/refresh requirements.

6) Points of Contact

- CIO/G-6 RI and IOM
- NETCOM/9th ASC ESTA/RCIO

1.5. ARMY REGULATION AND POLICY REVISION

a. Desired End State

Web-based review and publication of Army Regulations and Policy to reflect IM Transformation.

b. Actions

Review and update all CIO/G-6 proponent publications on an annual basis.

Complete revision of AR 25-1 NLT 1 Jun 03 to incorporate the transformation of information management and AKM.

The CIO/G-6 will revise AR 25-1 to reflect the changes of HQDA realignment under the DA GO #3, the establishment of NETCOM/9th ASC under DA GO # 5, the establishment of IMA under GO #4, and the publication of the Information Management Execution Plan Phase I and the AKM Implementation Plan.

The CIO/G-6 and NETCOM/9th ASC will review and revise AR 25-1, as detailed in the Information Management Phase I Execution Plan, 1 July 2002, Annex H.

NETCOM/9th ASC will review and submit recommendations to the Deputy Chief of Staff (DCS) G2 on AR 381-11 for changes necessary to support an enterprise approach to intelligence support to benefit the AEI.

Replace AR 380-19 with AR 25-IA. Review on an annual basis and revise as required.

- Develop Draft AR 25-IA NLT 1 Oct 03.
- Develop Coordination Draft AR 25-IA NLT 1 Jan 04.

- Develop final, obtain signature, and distribute AR 25-IA NLT 1 Mar 04.
- c. Specific Responsibilities
- 1) CIO/G-6
 - Review, revise, and staff the AR 25-1, DA Pamphlet 25-1-1, and DA Pamphlet 25-91.
 - Approve Request for Publication and submit all C4IM proponent regulations and other policy publications to Army Publishing Directorate (APD), AA.
 - Be the proponent for IA policy.
 - Maintain CIO/G-6 Draft Policy Knowledge Center on AKO. Grant author access to developers.
 - 2) IMA
 - Review existing policies and procedures and submit new or revised policy and procedure for input to CIO/G-6 proponent publications to reflect revised/new missions and responsibilities.
 - 3) MACOM and Functional Proponents
 - Review existing policies and procedures and submit new or revised policy and procedure for input to CIO/G-6 proponent publications to reflect revised/new missions and responsibilities.
 - Implement IA plans and procedures.
 - 4) NETCOM/9th ASC
 - Review existing policies and procedures and submit recommendations for input to the AR 25-1, DA Pamphlet 25-1-1, and DA Pamphlet 25-91 to reflect new missions and responsibilities.
 - Review, revise, and staff AR 5-12, AR 380-19 (Draft AR 25-IA and Draft DA Pamphlet 25-IA), AR 25-6, AR 25-10, and AR 25-11. Review every 12 months for currency and revise as required.
 - Submit all administrative publications except regulations to the APD, AA. Forwards regulations and other policy publications to CIO/G-6 for submission to APD.

- Review and submit recommended changes in AR 381-11 to DCS, G2, NLT 30 Jun 03.
- Ensure processes are established to implement published changes. Provide policy interpretation and implementation guidance.
- Ensure DOIMs are notified of published changes and implementation guidance.
- Provide implementation support to DOIMs within regions and track implementation of published guidance.
- Provide policy and oversight for IA.
- Final coordination of AR 25-IA NLT 1 Jan 04
- Forward AR 25-IA to APD NLT 1 Mar 04
- Provide implementation directives

5) DOIM

- Review existing policies and procedures and submit new or revised policy and procedure for input to CIO/G-6 proponent publications to reflect revised/new missions and responsibilities.
- Implement changes as directed.

6) Points of Contact

- CIO/G-6 EIG
- NETCOM/9th ASC IA

1.6. AKM STRATEGIC COMMUNICATIONS PLAN

a. Desired End State

All Army knows, understands and uses AKM.

b. Actions

This plan is a tool for the CIO/G-6 to illustrate how Army Knowledge Management (AKM) is a key communication initiative, one that illustrates The Army's efforts to streamline and integrate our organizations and processes to rapidly meet changing institutional and operational challenges. AKM is The Army's Strategy for transforming into a network-centric, knowledge-based force.

AKM is intended to improve decision dominance by our war fighters and business stewards - in battles pace, in our organizations, and in our mission practices. This transformation requires deep cultural changes from traditional practices to greater collaboration, teamwork, and innovation; from information hoarding to knowledge sharing; from stovepipe systems to enterprise networks and process; and, from traditional skills to internet-age competencies.

The purpose of the AKM Strategic Communications Plan is to unify efforts to communicate central themes and messages to describe how AKM enables The Army - - Soldiers - - Active, Guard and Reserve - - and civilians to achieve decision dominance by rapidly accessing general-level knowledge across secure communications means. The plan is an effort to coordinate, integrate and synchronize strategic communications to appropriately inform various audiences: The Army (field and Institutional Organizations), joint (Services and Staff), Combatant Commands/ASCC, OSD, selected interagency organizations, Congress and the American Public/Industry/Academia audiences. To achieve this there are a number of end state objectives that encompass ensuring that Army, DOD, Government, Industry and the Public have appropriate levels of understanding with respect to AKM. Each of the separate target audiences; Intra-Army, Government (including DoD), Congress and the Private Sector, have specific Public Affairs objectives.

- Intra-Army communications plan objectives include ensuring and understanding of the AKE Construct, ability to identify how the AKE Construct executes the AKM Vision and awareness that AKE supports the Objective Force.
- Communications outreach to Government elements has the objectives of developing an understanding of how AKE extends the global Information Grid and understanding the role of AKEA in achieving Joint, Allied, Coalition and interagency interoperability.
- Outreach to Congress includes the objective of enabling an understanding that AKM supports the overall Army Transformation.
- In the Public Sector, including the Public, Academia and Industry, a Strategic Communications Plan objective is to develop an understanding of how AKM contributes to winning the global war on terror.

Actions required to achieve the Strategic Communications Plan end-state objectives include:

- Developing a central theme for the public affairs campaign and the supporting messages that will be promulgated in support of that theme.

- Establishing a baseline knowledge level of understanding of AKM among elements of CIO/G-6 and the Army at large. This includes publishing an AKM Primer, conducting an online survey via AKO, conducting a random Survey at the Association of the United States Army (AUSA) Annual Meeting and conducting a TRADOC Proponent School Survey.
 - Develop and implement measurable indicators of success directly reflecting how well the messages were communicated to the target audience.
 - Develop campaign plan milestones.
- c. Specific Responsibilities:
- 1) CIO/G-6:
 - CXO SCIO will perform appropriate tasks associated with executing the AKM Strategic Communications Plan.
 - Develop and implement overall Strategic Communications Plan.
 - Develop an AKM Primer and Baseline Understanding Survey.
 - Develop staff oversight and responsibilities for milestones.
 - Coordinate campaign plan actions with CIO/G-6 Directorates and NETCOM.
 - Coordinate/prepare briefings, speeches, and point papers for target audiences for CXO.
 - Coordinate and synchronize all campaign plan briefings, speeches, point papers and related actions through CXO, CIO/G-6, CSA Strategic Communications Office, and Army Public Affairs.
 - Evaluate and obtain feedback on the success of the campaign plan at the Army, Combatant Commands, Joint (Services and Staff), Office of the Secretary of Defense (OSD) (Assistant Secretary of Defense for Networks and Information Integration (ASD(NI2)) and CIO EB), Congress and Public Sector levels on a continuing basis.
 - Directorates will ensure all briefings, speeches, and point papers concerning AKE are developed consistent with the overall AKM Strategic Communications Plan Theme and supporting messages.

2) NETCOM/9th ASC

- Ensure all briefings, speeches, and point papers concerning AKM are developed consistent with the overall AKE Strategic Communications Plan theme and supporting messages.

3) Point of Contact

- CIO/G-6 CXO SCIO

2.0 GOAL 2 – INTEGRATE KNOWLEDGE MANAGEMENT CONCEPTS AND BEST PRACTICES TO PROMOTE THE KNOWLEDGE-BASED FORCE

2.1. KNOWLEDGE SHARING AND COLLABORATIVE PROCESSES

2.1.1. Support Communities of Practice and Collaborative Environments

a. Desired End State

IT-enabled Communities of Practice (CoP) and other collaborative processes allow groups and teams to share information across the globe to solve problems and improve individual and organizational decision-making.

b. Actions

Broadly speaking, a CoP is a group of people who are virtually linked for the purpose of transferring knowledge, collaborative problem solving, mentoring and developing skills among its members and the identification of best practices. CoPs are a force multiplier by providing knowledge from sources outside the organizational construct.

- Develop and nurture CoPs in support of enterprise-wide solutions.
- Leverage lessons learned and best practices on CoPs and other collaborative processes across the AKE
- Develop/identify user requirements for collaborative environments.

c. Specific Responsibilities

1) CIO/G-6

- Provide support to select CoPs and other collaborative programs/initiatives by devoting KM, best practice, and transformation process expertise to their maturation. Current CoPs of interest include Project Exodus, NCO CoP, Company Command CoP, Future Combat Systems (FCS) Advanced Collaborative

Environment (ACE), and the Warrior Knowledge Network (WKN). (FY 03 and beyond).

- By Sep 03, create assessment tools and methodology for CoP/collaboration development based on lessons learned and case histories of impact. Other communities in growing their CoPs and establishing collaborative processes can use this toolkit.
- Chair the Army Collaborative Tools Working Group, under the AKO CCB, to establish policies, processes and tools that facilitate collaborative environments. (FY 03 and beyond).
- Participate in the DoD Collaboration Interoperability Working Group (FY 03 and beyond) to represent Army CIO/G-6 interests on Joint and DoD level collaboration decisions.
- By May 03, define the process for approval and integration for collaborative tools. Maintain list of validated tools that Army communities can use to support collaboration. Validation includes Defense Collaboration Tool Suite (DCTS) - interoperability, Joint Test Interoperability Command (JTIC) - approval, CON - networkiness, and CTO – permission to operate.
- NLT Jan 04, coordinate the establishment of an IM/IT CoP structure and sub-communities (e.g., DOIM, IMO, etc.).

2) MACOM and Functional Proponents

- Develop and promulgate CoPs and other collaborative environments to support operational and functional processes. Use self-assessment tool, methodology, and other lessons learned in CoP maturity to establish CoPs. Incorporate community management, content management and taxonomy and collaboration standards into CoP and collaborative process development (FY 03 and beyond).
- Participate in Collaborative Tools Working Group to design collaborative standards and guiding principles for Army communities (FY 03 and beyond).
- In accordance with CIO/G-6 acquisition guidance, procure and integrate collaborative tools to support functional/community needs that meet the standards and processes as determined by the Army Collaborative Tools Working Group (FY 03 and beyond).

3) Point of Contact

- CIO/G-6 EIO and EIP

2.1.2. Mitigate Risk in the Transformation to a Knowledge-based Force

a. Desired End State

Reduction in the planning and execution cycle by providing proven techniques, performance standards, and role models for the execution of issues decision-makers face.

b. Actions

Develop measurement criteria to assess return on value and progress towards achievement of the knowledge-based organization (KBO). Identify and promulgate the most significant best practices, process innovations and enterprise solutions that promote transformation to a network-centric, knowledge-based.

c. Responsibilities

1) CIO/G-6

- Educate and promote cultural change with functional Army audiences on issues critical to achieving the AKM strategy (FY 03 and beyond).
- Coordinate development of 'KBO Capability Maturity Model' to provide self-assessment tool for communities to determine strategy, objectives and progress towards achievement of AKM vision (FY 03).
- Coordinate development of 'knowledge metrics' methodology that measures impact of knowledge-sharing on performance and productivity in order to show quantifiable return on value. (FY 04).
- Coordinate the Army Knowledge Symposium as the prime venue for face-to-face collaboration, networking opportunity, and sharing of KM best practices for those seeking support, learning and professional and organizational growth in the transformation to a knowledge-based force. (FY 03 and beyond).
- In partnership with the Vice Director of the Army Staff, develop and implement an IT-enabled Best Practices program for the Army NLT Nov 03.

- Develop process, policy guidance and provide oversight for C4IM enterprise best practices process NLT Jan 04. Execute program for identifying, vetting, employing, and improving C4IM best practices FY 04 and beyond.
- Represent Army C4/IT community as the Army representative to the DoD IT Process Functional Board (PFB) of the DoD Business Initiatives Council, chaired by the Service Secretaries, ASD for Acquisition, Technology, and Logistics (ASD(AT&L)), Undersecretary of Defense Comptroller and Personnel and Readiness. (FY 03 and beyond).
- Provide CIO/Clinger-Cohen Act oversight to the Army Business Initiatives Council (ABIC) as member of the ABIC Executive Steering Committee and as Chair for the ABIC IT PFB (FY 03 and beyond).
- In FY 03, institutionalize the Army Knowledge Awards program to recognize those teams and organizations that are leading the transformation to the network-centric, knowledge-based force.

2) Vice Director of Army Staff

- Leads development of Army Best Practices Process that provides a networked Army Best Practices site that will allow subject matter experts to identify, analyze, and implement Army-wide and functional best practices (FY 03).

3) MACOMs and Functional Proponents

- Use KBO capability maturity model and knowledge metrics methodology to assess progress towards achieving AKM vision (FY 04).
- Identify opportunities for process improvement and best practices to Business Initiatives Council (BIC) (FY 03 and beyond).
- Reengineer local best practice processes to support integration in Army enterprise Best Practices program (FY 04).
- Incorporate best practices into solution development processes within organization to reduce planning and execution time (FY 03 and beyond).

4) Point of Contact

- CIO/G-6 EIO and EIP

2.2. IMPLEMENT WARRIOR KNOWLEDGE NETWORK.

a. Desired End State

Web-based learning community to provide leaders preparing for and engaged in military operation with the cross-functional capabilities (attributes, skills, and knowledge) and the real-time collaboration and knowledge creation for taking effective action.

b. Actions

Implement the approved WKN in Army Knowledge Online as the web-based knowledge system and learning community to provide Army leaders preparing for and engaged in military operations with tailored, timely, and relevant knowledge, information and data. Field the electronic arm of WKN as a Warrior Development Center (WDC) within AKO.

- Approved WKN Plans NLT 1 Jun 03.
- Functional Description NLT 15 Nov 04.
- Establish the pilot WDC in AKO NLT 1 May 05.

Develop the processes, tools and structures for virtual teams of high-performance leaders and network-centric crews, and the leader-development toolkit for making them and their members self-aware and adaptive.

- Develop and field a technological platform in the WDC in AKO for virtual teams NLT 1 Jul 03.
- Field a pilot Self-Awareness capability built around 360 degree assessment online by 1 Oct 03.

Deepen and broaden The Army's ability to generate, validate and integrate new tactics, techniques and procedures.

- Provide first working model of how to integrate best practices with lessons learned NLT 1 Jul 03.
- NLT 1 Feb 04, transform the CALL Database into a Warrior Knowledge Base.
- Field pilot at the Field Artillery School NLT 1 Jun 04.

- Apply WKN to doctrine development as a proof of principle NLT 1 Jun 04.

c. Specific Responsibilities

1) CIO/G-6

- Supports G3 in formulating the strategic vision, goals and objectives, in developing the functional design, and in every aspect of orchestrating the horizontal and vertical partnerships across the enterprise upon which WKN depends.
- Serves as the Lead Architect, ensuring that the WKN knowledge system is an authentic enterprise solution, fully integrated into the AKE, the AKEA, and transformation to the Objective Force.
- Supports G3 plans, programs and budgets for Warrior Knowledge Network, and supports G3 and G1 review of the impact of execution.
- Work with functional proponents and Executive Architects to define knowledge architectures.

2) G1

- Determines the competencies and meta-competencies for leadership, and establishes the leadership requirements against which the leader-development capabilities of WKN need to be measured.
- Serves as the functional proponent of the toolkits for fostering self-awareness and adaptiveness, including the mentoring network, and supports G3 in development of the functional requirements for knowledge systems to grow those meta-competencies.

3) G3

- Formulates strategic vision, sets strategic goals and objectives, designs mission, assigns responsibilities, develops enterprise-wide functional design, orchestrations integration with all other functional domains.
- Develop Army Enterprise Learning Architecture within the AKEA, and coordinates the Training, Knowledge Management and Leader Development components of the learning architecture.

- Plans, programs and budgets for WKN, and reviews the impact of execution.

4) NETCOM/9th ASC

- Supports the Functional Executive Agent in articulation of mission needs, operational requirements, functional description and technical specifications.
- Provides the information-technology solutions to meet these requirements.
- Factors WKN requirements into the AEI-T.
- WKN technical proponent, integrator of technical solutions, and manager of the technical dimension of the WKN knowledge system within AKO.

5) TRADOC

- Assigned as the Functional Executive Agent for WKN in the G3, G1, and CIO/G-6 charters.
- Determines demonstrated and anticipated capstone mission needs, operational requirements, and technical specifications for the knowledge system for leader development.
- Develops operational architecture for knowledge for leader development and reach, and serves as functional for the WKN knowledge system, and its online presence in AKO as a Warrior Development Center.
- Manages the functionality of the Online Warrior Development Center.
- Manages Warrior Knowledge Network as the global CoP and learning community for the domain of warrior development.

6) Points of Contact

- CIO/G-6 EIP
- G3 Training and Leader Development

2.3. ACHIEVE E-ARMY TRANSFORMATION

2.3.1. Develop the e-Army Environment

a. Desired End State

Increased productivity and efficiency, timely and reliable information flows, and improved decision cycle by using information technology to transform Army processes.

b. Actions

The Army Knowledge Enterprise is interoperable with appropriate joint, DoD, and interagency programs to achieve the goal of using technology to improve access to knowledge across the government.

Army organizations use information technology to transform the processes that:

- Provide service to its customers and constituents.
- Allow its employees to quickly access the information they need to make decisions.
- Provide timely acquisition of the information, products and services they need from their partners to conduct operations.

Army organizations incorporate these overarching principles while transforming to the e-Army environment that supports the network-centric, knowledge-based force of the Army Knowledge Enterprise:

- Focus on a self-service web-based operating environment so that customers, employees and partners can act quickly and securely by pulling the right information at the right time, eliminating processing delays.
- Provide users the ability to “pull” relevant data versus receiving large amounts of unwanted information being “pushed.”
- Enterprise-wide processes to provide consistency and access to information across the knowledge base within a reliable and secure environment.
- Operating on the foundation of the AKO portal.
- Build processes that operate within the ‘one network, one database’ construct thus, only handling information once.

- Automate processes to achieve a 'paperless' operating environment allowing streamlined access to information for appropriate users.
- Integrate digital signature capability into applicable processes to provide integrity and non-repudiation and permit totally digital processing and storage of actions.
- Incorporating knowledge process reengineering to build IT-enabled transformed processes focused on the point of action/decision that incorporate the knowledge sharing and collaborative activities integral to the achievement of a knowledge-based force.
- Use collaboration technologies that facilitate the extraction and integration of relevant information.
- Exploit automated management decision tools, such as the Army Workload and Performance System (AWPS) endorsed by the Secretary of the Army, to provide the 'business intelligence' necessary for better decision-making.
- Align e-Army activities with AKEA blueprint.
- Ensure alignment of e-Army implementation consistent with the Government Paperwork Elimination Act of 1998, the DoD Financial Management Modernization Program framework, the DoD e-Business strategy, the President's Management Agenda e-Government program, and related MIDs.

c. Specific Responsibilities

1) CIO/G-6

- Develop e-Army strategic intent and guiding principles NLT May 03.
- Develop process to provide oversight of e-Army activities, including e-Army 'way ahead' road map, and ensuring integration with joint, DoD and government e-Business/e-Government programs NLT Jul 03.
- Incorporate e-Army principles into Army strategies, policies, and publications (FY 04).
- In coordination with functional community/MACOM POCs, review plans for Government Paperwork Elimination Act (GPEA) compliance and integrate substantive elements into Army GPEA strategy and oversight program NLT 1 Jul 03.

- In coordination with the APD and AA, assist in the development of strategy to support transformation from 'forms management' to 'content management for forms data' NLT 1 Jun 03. Incorporate digital signature capability into strategy.
 - In coordination with G1 records management proponent, assist in the development/update of strategy that supports 'e-records' management NLT 1 Jun 03.
 - Identify e-Army opportunities and advise functional domain owners on e-Army process transformation and integration of multi-functional processes to achieve an automated end-to-end process state (FY03 and beyond).
 - Assist proponents in planning and executing e-Army activities (FY 03 and beyond).
 - In conjunction with the AAIC guidelines, incorporate operational, systems, and technical requirements of e-Army processes into AKEA, as necessary (FY 03 and beyond).
 - Provide the AKO common operating environment necessary to support secure, reliable, timely transactions in support of e-Army execution (FY 03 and beyond).
 - Coordinate the development of methodology to assess progress, impact, and results (increased productivity, cost savings, reduced cycle time) of operating in e-Army environment NLT 1 Dec 04.
 - Coordinate support and participation in e-Government and other external Army e-related programs (FY 03 and beyond). Integrate requirements into appropriate Army programs and activities.
- 2) Office of Administrative Assistant
- Develop strategy, with CIO/G-6 support, to achieve transform forms management to 'revolution to content management' for forms data, to include digital signature for transaction integrity, NLT 1 Jun 03.
- 3) G1
- As Records Management proponent, and with CIO/G-6 support, develop e-records strategy to update records management program consistent with the e-Army environment NLT 1 Jun 03.

4) MACOMs and Functional Proponents

- Integrate e-Army principles into organizational and functional transformation activities.
- Execute AKM guidance to 'webify and streamline' applications behind AKO, as directed in AKM Goal 4, NLT 1 Jun 04.
- Design interoperability with joint, DoD and interagency entities into all programs, systems, and processes as required to support the goal of streamlining processes to create seamless enterprise operations. Consider process integration requirements of the Financial Management Modernization Plan (FMMP) when planning functional process transformation (FY 03 and beyond).
- Evaluate the AWPS as the management decision support tool, as applicable to organizational and functional mission and as directed by the SecArmy in memo dated 18 Oct 01, subject: Army Workload and Performance Plan System Implementation. If unsuitable for mission needs, incorporate other management decision support tools into processes, ensuring that they adhere to e-Army principles. Develop plan to incorporate management decision support tools into operations NLT 1 Mar 04.
- In coordination with CIO/G-6 GPEA proponent, develop and submit plans for GPEA compliance within community NLT 1 Jul 03.

5) AMC, TRADOC, Office of the Surgeon General, and COE

- Working in conjunction with Army Publishing Directorate in the Office of the Administrative Assistant and the CIO/G-6, migrate current and future publications and forms to AKO and the Army Home Page by end of FY 03, per letter dated 28 Aug 02, subject: Migration of Army-wide Publications and Forms to the Army Knowledge On-line Portal and the Army Home Page.

6) Point of Contact

- CIO/G-6 EIO and EIP

2.3.2. Transform Processes to Achieve the AKE

a. Desired End State

Enterprise-wide and cross-functional E2E processes that improve decision making by assuring relevant and timely information and ease of access to the knowledge-base.

b. Actions

Enhance the commander's situational understanding of the CROP by merging operational, logistics, finance, human resource, medical, and maintenance applications to provide up-to-the-minute, enterprise-wide analytical and collaborative decision support through an automated system linked into common databases. Enterprise and E2E processes provide consistency, reduce learning cycle, reduce life cycle support requirements (over current systems) and necessitate data standardization.

Functional proponents will lead the process transformation within their knowledge domain to embed AKM into their operations and streamline procedures to create enterprise-wide functional processes. Development of IT-enabled processes is the primary means to achieve the objective of creating the AKE. Proponents will identify opportunities to integrate processes, systems, and services with other domain owners to achieve the move to E2E enterprise processes. In performing responsibilities of the Clinger-Cohen Act, the CIO/G-6 is in a unique position to identify opportunities for cross- and multi-functional E2E processes and has the responsibility to assist those knowledge domain owners with leveraging technology to optimize the efficiencies and effectiveness expected of E2E process transformation.

Several activities support the achievement of process transformation:

- Assess processes against a 'process readiness' profile to determine applicability to future operations, state of migration, and enterprise architecture implications.
- Apply Knowledge Process Reengineering to integrate AKM into the operational functions of the Army. This includes the education programs conducted by the CIO/G-6 to establish a baseline of AKM understanding among the Army staff, the functional communities, and the operational Army.
- Establish data standardization as foundation for enterprise process transformation and the e-Army environment.

- 'Streamline and webify' applications and move Army processes to Army Knowledge Online (AKO), creating the killer application for land power dominance by integrating AKO fully into all operational activities.
- Identify processes that are applicable for use across the DoD and/or Army enterprise to the BIC at the DoD and Army levels.
- Synchronize ERP implementations within the Army, identify opportunities for E2E process development, and align Army processes with requirements at the DoD level, particularly the Financial Management Modernization Program (FMMP), through Army ERP integration.
- Integrate multiple processes and functions (via Enterprise Resource Planning and other enterprise systems) to streamline and enhance the effectiveness of support to warfighter operations and achieving the Objective Force's goal of 'foxhole to factory' continuum of operations.
- Incorporate enterprise and E2E processes in the AKEA operational architecture.

c. Specific Responsibilities:

1) CIO/G-6:

- Establish a customer relationship management function to embed knowledge management expertise in key functional areas on the Army Staff.
 - Educate Army Staff on the fundamentals of knowledge management. Train and embed knowledge management expertise in key functional areas NLT 1 Jul 03.
 - Develop and provide a KM Action Planning Course to assist Army functional communities in developing the in-house expertise to use knowledge process re-engineering to transform their processes. Develop and field baseline course NLT 1 Oct 03.
- Provide AKO policy and guidance, as described within AKM Goal 4, to facilitate the transition to e-enabled processes (FY 03 and beyond).
- Develop plan to determine definitive data owners and maintenance/accessibility standards for key data elements necessary to support transformed enterprise processes and the e-Army environment in conjunction with AAIC timelines NLT 1 Jun 03.

- Develop, test, and institute a methodology for a Knowledge Process Reengineering capability to assist communities in transforming processes consistent with achievement of the knowledge-based force. Integrate training on Knowledge Process Reengineering (KPR) methodology into KM Action Planning Course NLT 1 Oct 03.
- Develop methodology for 'process readiness profile' self-assessment tool and metrics to assess progress and effect of process transformation activities NLT 1 Jun 04.
- Identify opportunities to integrate cross- and multi-functional processes to create E2E enterprise processes. Coordinate with process proponents to achieve E2E goal (FY 03 and beyond).
- Provide assistance through proven methodologies and best practices to support stand-up of Operational View architecture CoP NLT 1 Jan 04.
- Ensure integration of multiple ERP systems into AKEA; Managing data standardization efforts to support ERP implementations; provide assistance to leverage technology and develop strategies to build enterprise and cross-functional E2E processes to achieve the vision of 'foxhole to factory' support to the warfighter (FY 03 and beyond).

2) MACOM and Functional Proponents

- Develop streamlined processes that create enterprise-wide operational capability. Coordinate with CIO/G-6 and NETCOM/9th ASC on optimal use of technology to facilitate process transformation (FY 03 and beyond).
- Incorporate the concept of Knowledge Process Reengineering into process transformation activities to build to the vision of 'network-centric, knowledge-based force' by examining the knowledge flows at the point of decision to determine the optimal process NLT 1 Oct 03.
- Identify opportunities to integrate cross- and multi-functional processes to create E2E enterprise processes. Coordinate with other process proponents and CIO/G-6 to achieve E2E goal (FY 03 and beyond).
- Ensure process transformation plans are consistent with integration into approved DoD and/or Army enterprise processes, such as the

DoD FMMP, and ERPs such as Defense Integrated Military Human Resource Management System, Defense Civilian Personnel Systems, Logistics Modernization Program, etc.

- Obtain approval from OSD (Comptroller) for ERP development, as directed in DoD Memos, “Deployment of Financial Management Enterprise Resource Planning Systems”, dated 21 Aug 01, and “Defense Financial Management Modernization Program—System Initiatives”, dated 12 Oct 01 (FY 03 and beyond).
- NLT Jun 04, execute ‘streamline and webify’ guidance of AKO Memorandum #2. Eliminate or migrate processes and applications that are duplicative, extraneous or do not support enterprise process objectives, consistent with the applications streamlining guidance of AKM Goal 4.
- In conjunction with AAIC, identify functional/proponent enterprise and E2E processes to the AKEA (FY 03 and beyond).
- Identify business processes that are applicable across the DoD and/or Army enterprise to the BIC at the DoD and Army levels (FY 03 and beyond).
- Use ‘process readiness profile’ to assess status/effects of process transformation activities NLT 1 Jul 04.

3) Point of Contact

- CIO/G-6 EIO and EIP

3.0 GOAL 3 – MANAGE THE INFOSTRUCTURE AS AN ENTERPRISE TO ENHANCE CAPABILITIES AND EFFICIENCIES

A network-centric environment of reduced infostructure and less overhead cost will allow the Army to exchange information seamlessly with greater responsiveness and flexibility during deployments and other operations. Benefits of migrating to a network-centric environment allow the Objective Force to plug a device into the Army’s enterprise network, use a single sign-on capability, and gain access to universal data providing decision dominance over the enemy.

Additionally, AKM Goal 3 focuses on operating and managing the Army ‘s infostructure as an enterprise to enhance system capabilities through improved configuration management, security, and interoperability while achieving cost efficiencies by consolidating IT resources, centralizing network management, and developing enterprise support contracts.

Transforming today's fragmented, multi-level IT management environment into an efficient, network-centric knowledge-based enterprise is a journey. The following five missions depicted in Figure 2.3-1 address the new paradigms needed for enterprise management of the Army's infostructure.

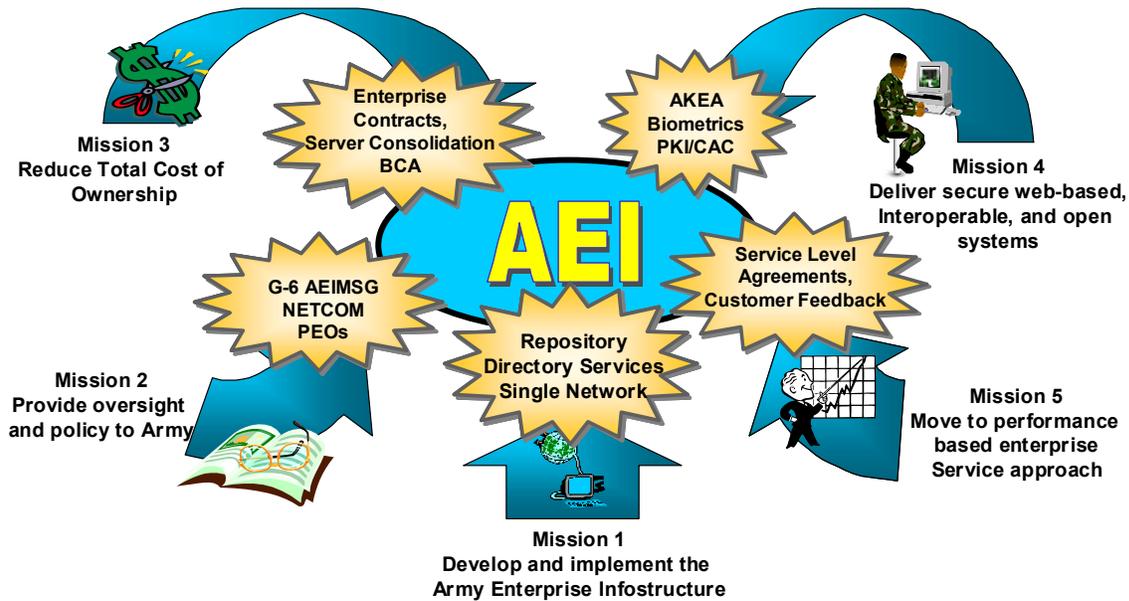


Figure 2.3-1 Transforming the Army Enterprise Infostructure

The significant actions incorporated within these five missions are presented as follows:

Mission One: Develop and Implement the Army Enterprise Infostructure

- Installation Bandwidth Modernization.
- Asset and Configuration Management.
- Implement Enterprise Directory services.
- Migration to Next Generation MS Operating System - Implement Active Directory.
- CONUS TNOSC Consolidation.
- Relocation of ANOSC to Fort Belvoir.
- Disaster Recovery and Continuity of Operations Planning.

Mission Two: Provide Oversight and Policy to Army

- AEI-Governance.
- Implement Enterprise Systems Management.
- AEI Systems Integration.
- Single DOIM Concept.
- Visual Information.
- Sub-Installation Support and Relationships.

Mission Three: Reduced Total Cost of Ownership

- Business Case Analysis.
- Acquisition of IT.
- Server Consolidation.
- Enterprise E-Mail and Web Server Strategy.
- Adjust Commercial Activities for Completed A-76 studies.

Mission Four: Deliver Secure Web-based Interoperable, and Open Systems

- Army Enterprise Networkiness Certification.
- Data Interoperability.
- Remote Services.
- Defend the Army Portion of the GIG by Implementing CAC and PKI.
- Defend the Army Portion of the GIG by Implementing a Cryptographic (CRYPTO) Modernization Program.
- Defend the Army Portion of the GIG by Integrating Biometric Technologies.

Mission Five: Move to Performance Based Enterprise Service Approach

- Baseline Services and Service Level Management.
- Implement an Enterprise Call Center.

3.1. MISSION ONE – DEVELOP AND IMPLEMENT THE ARMY ENTERPRISE INFOSTRUCTURE

3.1.1. Installation Bandwidth Modernization

a. Desired End State

Army installation portion of GIG provides foundation for network-centric transformation.

b. Actions

The Army has been modernizing the installation bandwidth on installations using the I3MP for both active and reserve components for several years. I3MP has been expanded beyond the main installation area to include training ranges, airfields, and motor pools. The I3MP implementation has been based on the Army's prioritized Installation Sequence List (ISL).

The I3MP needs to be expanded to include states and Army Reserve regions as "installations." This will allow all Army Reserve Regional Support Commands (RSC) and Army National Guard State Area Commands (STARAC) to be considered part of the ISL. These "installations" will be added to the ISL for bandwidth modernization NLT 1 Oct 03. Funding requirements for the "installations" will be included in the FY06-11 POM.

Installation bandwidth modernization must synchronize with the Installation Information Infostructure Architecture (I3A) of the AKEA.

Synchronization with GIG-BE is required in accordance with MID 905. GIG-BE plans must be forwarded to the DoD CIO NLT 30 Apr 03. This plan should synchronize the I3MP with the ninety most critical installation included in the "Global Information Grid Bandwidth Expansion Derived Requirements," dated 17 Dec 01. In addition, Army must work with DoD CIO to include the most critical Army (AC/RC) GIG-BE requirements.

Bandwidth expansion must be synchronized with the emerging Base Realignment and Closure (BRAC) lists.

c. Specific Responsibilities

1) CIO/G-6

- Develop a plan for expanded Bandwidth connectivity to bridge between installation and GIG at the designated locations worldwide. Forward plan to DoD CIO NLT 30 Apr 03. (completed)
- Synchronize ISL with emerging BRAC list.

- Expand installation bandwidth modernization to include states and reserve regions as “installations.” Include funding requirements for the “installations” in the FY06-11 POM.
 - Ensure synchronization between I3A and I3MP.
- 2) G3
- Expand installation bandwidth modernization to include states and reserve regions as “installations.” Include “installations” in the ISL for bandwidth modernization NLT 1 Oct 03.
- 3) Point of Contact
- CIO/G-6 IOM

3.1.2. Army Enterprise Infostructure - Repository

a. Desired End State

Army wide repository reflecting all IT assets.

b. Actions

A key element of managing the infostructure as an enterprise is establishing and maintaining of a comprehensive asset and configuration management repository. Intelligence and Security Command (INSCOM) Automated Systems Intelligence Database (ASID) has been nominated as a BIC initiative and has been approved by the ABIC for implementation. This Army Enterprise Infostructure-Repository (AEI-R) is expected to support multiple enterprise management processes, to include IT capital planning, architecture management, configuration management and control, Networkiness, and Enterprise Call Center user verification.

The Army will establish a centralized AEI-R capability tied to the AKO-SIPRNET (AKO-S) with a Theater Asset Repository (TAR) within each NETCOM/9th ASC Theater NOSC. NETCOM/9th ASC will operate and manage the AEI-R and the various TARs. The appropriate data steward will manage source data.

The implementation of the AEI-R will occur in four stages. The first stage will be to leverage the current INSCOM asset management application business processes as an interim enterprise asset management capability to initially perform capital planning and decision-making. The Enterprise Configuration Management (ECM) working group is developing requirements for an interim Army enterprise asset management/Infostructure repository capability. The target date for completion of the Interim AEI-R capability is 1 Apr 04.

The second stage of the AEI-R implementation will be an initial AEI-R accessible through the AKO-S. This initial AEI-R AKO-S capability will be based on the expanded requirements definition effort of Stage 1 and will be implemented between 1 Apr 04 and 1 Jan 05 based on this study and available funding.

The third stage will be to transfer current asset, configuration, and architecture repository activities to NETCOM/9th ASC and migrate the existing repositories into the AEI-R. NETCOM/9th ASC is not responsible for data content, products, or procedures. Data responsibility and management will remain the responsibility of the functional proponent or executive architect.

This state of AEI-R implementation will be the fielding of a TAR to each of the NETCOM/9th ASC TNOSCs and linking that TAR to the objective AEI-R via a Secret and Below Initiative (SAB). This stage will be completed by 1 Jan 05 based on available funding.

The fourth and last stage will be to implement the required third party tools to facilitate automated data population of the AEI-R. This stage will be completed by 1 Oct 05 based on available funding.

c. Specific Responsibilities

1) CIO/G-6

- Designate NETCOM/9th ASC as the Functional Proponent for the AEI-R.
- Provide necessary resources to implement the AEI-R capability.

2) ASA(ALT) PEO EIS

- Serve as Material Developer for the AEI-R capability.
- Develop the necessary system views (SV1 – SV7) of the AEI-R architecture.

3) MACOMs and Functional Proponents

- Implement MACOM or Functional Proponent asset management capabilities as necessary.
- Link MACOM or Functional Proponent asset management capabilities into the AEI-R.
- Transfer the resources (personnel and funding) associated with current asset, configuration, and architecture repository activities to NETCOM/9th ASC.

4) TRADOC

- Coordinate and review the Operational Views of the AEI-R architecture.

5) NETCOM/9th ASC

- Serve as Functional Proponent for the AEI-R.
- Work with MACOMs and Functional Proponents to transfer the resources (personnel and funding) associated with current asset, configuration, and architecture repository activities.
- Lead development of the requirements definition of the AEI-R system.
- Develop the necessary operational views (OV1 – OV5) of the AEI-R architecture.
- Review and approve the necessary system views (SV1 – SV7) developed by the PEO EIS.

6) DOIM

- Update information within the AEI-R and TAR as those capabilities are fielded.
- Provide support as part of the NETCOM/9th ASC requirements definition effort.

7) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC ESTA Governance and NETOPS Directorate

3.1.3. Implement Enterprise Directory Services

a. Desired End State

A global directory service to access information and people; anywhere, anytime.

b. Actions

The Army will implement an EDS to function as the integrated meta-directory for all Army users. The EDS will be the designated data source of Army data to the

DoD Global Directory System (GDS). It will integrate, as a minimum, the source data from the Army's implementations of:

- Active Directory.
- Defense Messaging System – Army (DMS-A).
- PKI.
- AKO Directory.
- Domain Name System (DNS).
- Telephone Directory Services.
- Other functional programs (Army Human Resources System (AHRM), Defense Finance and Accounting System (DFAS), etc.).

The EDS architecture will be developed by NETCOM/9th ASC in coordination with the US Army Signal Center (SIGCEN) NLT 1 Aug 03. PEO EIS will develop the detailed integration and implementation plan. PEO EIS, in coordination with PEO C3T, will implement the EDS across the Army in support of both deployed and sustaining base environments. All directory-related efforts and programs within the Army will be coordinated with NETCOM/9th ASC and implemented through PEO EIS to ensure integration and compatibility with the EDS concept. MACOMs, Functional Proponents, and Program Managers will identify resources associated with directory-related efforts to the CIO/G-6 for leveraging into an enterprise directory solution.

To become a network-centric force built around the concepts of Knowledge Management requires the Army to have access to information and people whenever and wherever they are. This implies an extensive and robust enterprise-wide directory service that is up-to-date and, to a large degree, automatically populated as the result of other actions or activities. This directory service must support Army users' deployed, fixed, and transitory environments and provide input to the DoD Global Directory Service (GDS). The Army Enterprise Infostructure Directory Service will:

- Provide a globally accessible directory service offering secure high data availability and supporting multiple standards based access protocols that will serve as the foundation for the digital infostructure in support of the Objective Force.
- Serve as a directory for various information types (e.g., white pages, applications, and services).

- Allow users to locate resources quickly and efficiently—achieving directory “dial-tone.”

Enterprise directory services are the centerpiece and critical component in next generation infostructure architectural design. An enterprise directory service consolidates disparate data repositories into a unified logical view of the entire organization. This provides users with unprecedented power with the ability to locate and view (this assumes the user has adequate permissions and the access control lists allow viewing rights) information about any resource in the Army. Resources could be phone and email addresses for people or groups, but could easily be applications or devices.

An enterprise directory moves the Army closer to realizing a single sign-on capability in which users present their credentials once, and applications consult the directory for configuration and permission level relieving the user from remembering and entering multiple passwords. Smart card implementation (Common Access Card (CAC)) is greatly facilitated by the establishment of an enterprise directory. An enterprise directory is the natural choice for storing and locating certificate and certificate related material (Certificate Revocation Lists).

Applications will be streamlined and speed of development will increase as a single repository of user, group and application information becomes available. Directory services is an enabler for single point of administration in which one change could re-configure all routers in a group vice configuring all 1000 routers individually. Global Combat Service Support –Army (GCSS-A) is an example of this approach in which the application does not use an application specific database, but relies on the Active Directory to store user related and application configuration information. The directory is the optimal repository for user preference and configuration data enabling a consistent desktop independent of user location.

Implementing an Army enterprise directory could be an enabler for bandwidth allocation by using the Quality of Service (QoS) features and allocating bandwidth based on application, user, group affiliation or a combination of both. This could provide relief to base camps and stations requiring greater bandwidth for mission critical applications.

The benefits of an enterprise directory service do not come without a price in the form of extensive up-front engineering to develop requirements, enterprise architectures, and distributed test plan documents. Once implemented, enterprise directory services represent a potential for tremendous savings in the out years in reduced application development, system administration, and lost efficiency costs.

c. Specific Responsibilities

1) CIO/G-6

- Ensure integration of the EDS architecture with AKEA.
- Secure funding required for EDS specific infostructure implementation and operations.
- Designate NETCOM/9th ASC as the EDS integrator.

2) ASA(ALT) PEO EIS

- Responsible for system design, development, acquisition, integration, testing, fielding, training, and transition to O&M the EDS in coordination with NETCOM/9th ASC. Tasks to be accomplished in coordination with CIO/G-6 and NETCOM/9th ASC.
- Implement all directory service capabilities in accordance with NETCOM/9th ASC guidance to ensure it contributes to the implementation of the EDS.

3) NETCOM/9th ASC

- Develop EDS architecture in coordination with the SIGCEN NLT 1 Aug 03.
- Operate and manage the EDS.
- Coordinate implementation of all directory service capabilities within the Army.
- Ensure operational and maintenance funding for EDS capabilities is identified in POM submissions.
- Assist DOIM in problem resolution.

4) DOIM

- Operate the existing LAN and NT infostructure.
- Perform system admin functions as delegated for the EDS.

5) Point of Contact

- CIO/G-6 IOM

- NETCOM/9th ASC ESTA

3.1.4. Migration to Next Generation Desktop Operating System – Implementing Active Directory

a. Desired End State

Have a continuous process of technology refreshment to support migration to the next generation desktop capability.

b. Actions

To effectively use the capabilities associated with Windows 2000 (WIN2K) (or later network operating systems (NOS)) and Active Directory, in an enterprise-wide approach with centrally operated and managed domain structures and naming conventions, the Army must migrate to another NOS environment. The current Army infostructure is heavily dependent upon Microsoft NT NOS. It is recognized that Microsoft will soon discontinue support for the NT NOS. While there are several options available to the Army, the vision is that a significant portion of the Army will choose to migrate to a Microsoft WIN2K or later level NOS with its attendant Active Directory (AD) support structure.

The Army will implement a limited-forest AD infostructure to support the migration of local and organizational LAN operations from Windows NT to WIN2K or later. The Army AD environment will be centrally managed with limited decentralized operations under strict configuration control of NETCOM/9th ASC. The AD forest configuration will change as time goes on as more knowledge is gained and AD becomes an integral part of the Army EDS. As an initial starting point, the AD forest configuration will consist of the following enterprise forests.

- CONUS
- Europe
- Pacific
- Korea
- Army National Guard
- Army Reserve
- Corp of Engineers
- MEDCOM
- Application Forest

MEDCOM will be the first large-scale Army implementation of AD. This is motivated by the need to migrate to Exchange 2000 to enable further email consolidation and reduce Total Cost Ownership (TCO). As part of the migration to single authority operation and management, NETCOM/9th ASC will operate the MEDCOM AD Forest root.

A common schema will apply to all the forests, and a meta-directory service will support exchange of information between forests. Special purpose forests may be authorized for systems that have no need to interact with other forests or have an urgent need before the geographical forests are established.

NETCOM/9th ASC will initially establish an AD backbone, fielded by ASA (ALT) PEO EIS, consisting of the root domain controllers for each of the forests, and the meta-directory service. The AD hierarchy will then be built out as resources permit. NETCOM/9th ASC will operate and manage the root domain controllers and the meta-directory service.

The tenants currently responsible for operations and funding of networks will identify the resources expended in support of those networks for FY03, the budgeted resources for FY04, and the resources contained in the POM for FY05 – FY11. The DOIM will assume operational control of the existing LAN and infostructure NLT 1 Oct 03 with the organization currently responsible for resourcing LAN operations transferring those resources to the DOIM upon assumption of control.

Tenants will transfer to the DOIM the necessary resources or equivalent dollars to continue operations of the current infostructure domain controllers (primary and back-up). NETCOM/9th ASC will publish a detailed AD migration plan NLT 1 Apr 03.

c. Specific Responsibilities

1) CIO/G-6

- Review and approve AD policy recommendations.
- Provide necessary resources for basic Army AD infostructure.

2) ASA(ALT) PEO EIS

- Manage cost, schedule, performance and supportability for designated AD implementations in coordination with NETCOM/9th ASC.
- Provide oversight and coordination for Army AD Implementations in coordination with NETCOM/9th ASC.

- Develop implementing instructions for AD migration.
 - Review, in conjunction with NETCOM/9th ASC, AD implementations at installations worldwide
 - Provide oversight and coordination for Army AD implementations.
 - Acquire AD backbone.
- 3) MACOM and Functional Proponents
- Transfer resources to IMA for DOIM operations of infostructure NLT 1 Oct 03.
 - Only those with approved forests will implement AD, based on approved architecture.
- 4) IMA
- Work with MACOMs and Functional Proponents to transfer resources to IMA for DOIM operations of infostructure NLT 1 Oct 03.
- 5) NETCOM/9th ASC
- Review and approve any additional AD forest implementations.
 - Provide recommendations to CIO/G-6 on AD implementation and operations within the Army.
 - Manage all domain controllers.
 - Operate all Army AD Forest roots and maintain configuration control of all Army AD implementations.
 - Manage funding for on-going infostructure operations and migrated AD operations through RCIOs to DOIMs.
 - Publish a detailed AD migration plan NLT 1 Jul 03.
 - Support AD implementations within their region as required.
- 6) DOIM
- Assume operational control of the existing LAN infostructure except in instances where SLA specify differently NLT 1 Oct 03.

7) Point of Contact

- CIO/G-6 IOM Directorate

3.1.5. CONUS TNOSC Consolidation

a. Desired End State

Centralized CONUS Theater NOSC operations in support of the AEI.

b. Actions

Under the approved NETOPS CONOPS, NETCOM/9th ASC will develop a NOSC consolidation plan to ensure continuity of operations and provide the best operational support to Army commands/customers.

It is envisioned the C-TNOSC will perform core Enterprise Services Management (ESM) functions on a regional and "unique/functional" basis and provide critical COOP and the infostructure to enable consolidation/elimination of functional NOSCs. Additional CONUS TNOSC facilities will not be built from scratch. NETCOM/9th ASC will develop the criteria for evaluating and selecting one or more additional CONUS TNOSCs facility locations. Criteria, alternatives and recommendations will be presented to the CIO/G-6 for decision NLT 1 Jul 03. A schedule for transition to the desired end state will be published NLT 1 Aug 03. Transition will begin NLT 1 Oct 03.

Upon establishment of one or more additional CONUS TNOSC facilities, and in conjunction with the AKEA development, existing MACOM/Functional NOSCs will be examined for decommissioning or retention as subordinate Regional NOSCs or NOCs under NETCOM/9th ASC Technical Control. Resources from decommissioned NOSCs will be reinvested into the Enterprise efforts.

c. Specific Responsibilities

1) CIO/G-6

- Approve and publish the transition plan NLT 1 Aug 03.
- Provide NOSC decommissioning guidance and policy.

2) NETCOM/9th ASC

- Submit criteria, alternatives and recommendations to the CIO/G-6 for decision NLT 1 Jul 03.
- Assume responsibility for all NOSC operations upon initiation of the consolidation plan.

- Conduct Site Surveys of existing non-NETCOM/9th ASC NOSCs.
 - Identify all resources required to support additional C-TNOSC.
 - Develop C-TNOSC ESM functional and technical requirements
 - Develop a C-TNOSC Business Case Analysis.
 - Develop C-TNOSC CONOPS for multiple facility operations.
 - Publish a CONUS NOSC consolidation plan.
 - Consolidate the list of all available NOC resources supporting each network and determine best solution for capitalization and reallocation.
 - Develop a C-TNOSC COOP Plan in accordance with enterprise COOP plans addressed in paragraph 3.1.7.
 - Develop a functional matrix allocating roles and responsibilities across the C-TNOSC facilities.
 - Operate and manage the C-TNOSC facilities.
 - Assist with the collection of the NOSC asset data.
- 3) MACOMs and Functional Proponents
- Provide to NETCOM/9th ASC a list of locations of the functional NOSCs and the functions that they perform NLT 1 Jun 03.
 - Provide to NETCOM/9th ASC a list of tools that are currently used by the functional NOSC NLT 1 Jun 03.
- 4) Points of Contact
- CIO/G-6 IOM
 - NETCOM/9th ASC ESTA Governance and NETOPS Directorate

3.1.6. Relocation Of ANOSC To Fort Belvoir

a. Desired End State

A single network and security management center that provides enhanced security and operations through CND and CNO in the Army's portion of the GIG.

b. Actions

Consolidate operations and maintenance of Army Networks by collocating the network management and network security operations of the AEI to meet DoD GIG operational network goals. This collocation will enable proactive CND and provide enhanced performance and availability to the warfighters on GIG.

Pending approval and successful AR 5-10 notification, NETCOM/9th ASC will collocate the ANOSC at Ft. Belvoir within the Information Dominance Center in the Nolan Building.

c. Specific Responsibilities

1) CIO/G-6

- Provide oversight to ANOSC consolidation.
- Ensure policy and governance reflect the transition.

2) NETCOM/9th ASC

- Create a Virtual CNO center with a one-stop shop for all queries on Network Operations, Computer Network Defense, Exploitation, and Attack (CND/CNE/CNA), in coordination with INSCOM.
- Publish operations guide for Virtual CNO.
- Provide ANOSC IOC NLT 1 Jun 03 and full operational capability NLT 1 Jan 04.

3) INSCOM

- Assist NETCOM/9th ASC to create a Virtual CNO center with a one-stop shop for all queries on CNO/CND/CNE/CNA.

4) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC G3

3.1.7. Disaster Recovery And Continuity Of Operations Planning

a. Desired End State

Uninterrupted AKE service for critical assets regardless of natural and man-made disasters.

b. Actions

The Army is moving to become a network-centric force built around the concepts and goals of the AKM initiative. As a result, Army information systems and access to Army data cannot be interrupted for any significant period. Therefore, the Army is committed to implementing an aggressive Continuity of Operations Plan (COOP) and Disaster Recovery (DR) capability. The vision is for all Army systems to have a COOP and a designated DR capability along with the associated statement of priority, DR performance metrics, and tested execution. NETCOM/9th ASC will provide as a core mission, the basic elements and services necessary to execute the system's COOP. However, the COOP is fundamentally a system or application proponent's responsibility. The system or application proponent must determine the priority and DR performance metrics acceptable based on a given system's mission criticality. Therefore, it is the functional proponent's mission to provide NETCOM/9th ASC with the necessary information and resources to successfully execute the DR program for each system or application in the Army.

NETCOM/9th ASC will develop and prioritize a DR capability to support all systems or applications under its operational control. Functional proponents will identify all systems or applications within their area of interest. They will define the DR priority and performance metrics necessary for each identified application.

NETCOM/9th ASC, in coordination with the various functional proponents, will develop a test execution process, schedule, and resources for all identified systems or applications under its operational control. Any system or application for which the functional proponent does not wish to have a test execution process defined will be terminated from the COOP process. The functional proponent will provide NETCOM/9th ASC the resources to test the COOP program for each system or application at least once each year. NETCOM/9th ASC will implement a DR Service Level Agreement with the appropriate functional proponent to document the COOP for that system or application.

The functional proponent will resource the execution of the DR program or provide justification to HQDA for DA to resource the necessary DR program. Failure to provide NETCOM/9th ASC the identified resources will constitute a decision by the functional proponent to terminate that particular system or application.

c. Specific Responsibilities

1) CIO/G-6

- Provide policy and oversight of COOP.

- Provide necessary resources to implement enterprise-wide COOP/DR capabilities.

2) ASA(ALT) PEOs

- Identify all systems or applications within their area of interest requiring a COOP.
- Define the DR priority and performance metrics necessary for each identified application.

3) MACOMs and Functional Proponents

- Identify all systems or applications requiring a COOP.
- Determine COOP criteria and DR performance metrics.
- Provide the resources to test and implement their COOP.

4) NETCOM/9th ASC.

- Identify all Army systems under NETCOM/9th ASC operational control requiring DR support.
- Develop an appropriate enterprise strategy to provide an efficient enterprise-wide DR support system.
- Develop and request HQDA approval and funding for the enterprise-wide DR capabilities.
- Report to CIO/G-6 as directed (e.g., DR asset management).
- Create DR processes tailored to a specific technology to optimize efficiency.
- Identify the critical functions that require continuous operations for the development of a DR capability to support all systems or applications under its operational control.
- Lead the development of COOP requirements and definition.
- Develop DR SLAs with the appropriate MACOM or Functional Proponent.
- Develop and execute COOP tests processes.

- Assist with the collection of the system identification data for each region.
- Provide status reports on COOP testing conducted within the region's DOIM facilities.

5) DOIM

- Design and execute an interim local COOP until the NETCOM/9th ASC DR capabilities are implemented.
- Propose new technology and services supporting DR.
- Ensure all existing installation assets and resources are identified and linked to the Army and organizational missions, processes, and tasks they support for DR.
- Provide any information and support any reconfiguration efforts required by the installation to support approved DR implementation plans.

6) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC ESTA Governance and NETOPS Directorate

3.2. MISSION TWO –PROVIDE OVERSIGHT AND POLICY TO THE ARMY

3.2.1. AEI Governance

a. Desired End State

A governance structure to manage and oversee implementation of Goal 3 initiatives for AEI.

b. Actions

The AEIMSG has been established to advise the Army CIO on all matters pertaining to Goal 3 of the AKM Strategic Plan. The Chair is the Chief of Information Infostructure Division. Members of the AEIMSG include representatives from HQDA, MACOMs, Guard, and Reserve. The AEIMSG will establish working groups to address specific technical issues.

Synchronization meetings will be held regularly to coordinate Goal 3 activities among the major players: CIO/G-6/IOM, NETCOM/9th ASC, PEO EIS, PEO C3T,

and AMC CECOM. These meetings at the COL/GS-15 level will parallel the General Officer AKM synchronization meetings among the same organizations.

A process will be established that involves the AEIMSG in developing and prioritizing AEI requirements. An initial set of AEI requirements were developed by the Requirements Integrated Process Team in Jan 02 and subsequently endorsed by the CIO EB in Feb 02. These requirements are being used to establish a baseline set of services to be provided across the Army enterprise as well as to identify new capabilities that need to be implemented. Technology refreshments will be driven by BCA.

c. Specific Responsibilities

1) CIO/G-6

- Chair the AEIMSG and establish working groups as required.
- Convene regular Goal 3 synchronization meetings with other major players.
- Establish a process for developing and prioritizing AEI requirements.

2) ASA(ALT) PEO EIS and PEO C3T

- Support AKM Goal 3 planning activities as the systems integrator.
- Participate in regular Goal 3 synchronization meetings.
- Participate in AEIMSG and working groups as required.

3) MACOMs and Functional Proponents.

- Participate in AEIMSG and working groups.

4) NETCOM/9th ASC

- Support AKM Goal 3 planning activities as the operational manager.
- Participate in regular Goal 3 synchronization meetings.
- Participate in AEIMSG and working groups as required.

5) Point of Contact

- CIO/G-6 IOM

3.2.2. Implement Enterprise Systems Management

a. Desired End State

Operate and manage the Army Infostructure as an Enterprise.

b. Actions

Army will adopt enterprise management processes and field the tools necessary to support those enterprise management processes in the most effective and efficient manner possible. The Army will implement an Enterprise Systems Management (ESM) capability that supports the Army environment in anticipation of fielding the Objective Force.

NETCOM/9th ASC is designated as the single authority to operate, manage, and defend the Army Enterprise Infostructure from end-to-end – from WAN to desktop, and from “mud” to “space”. The new NETCOM/9th ASC organization will need to be built up for its expanded role, from the former ASC, and the new NETCOM/9th ASC Regional Units staffed.

A concept of operations (CONOPS) for operations and management of the Army infostructure at the enterprise level (NETOPS) is being developed. NETOPS is the integration of Systems and Network Management (S&NM), Information Assurance (IA), and Information Dissemination Management (IDM). A key capability to be developed will be an Army Enterprise Network Common Operational Picture (NETCOP) that provides a top-level view of the status of the Army infostructure. Initially, this will be provided by feeds from existing component networks such as those supporting the Reserves, Guard, and Corps of Engineers.

Enterprise infostructure management concepts will need to be developed, to identify which functions will be performed at the global, theater, regional, and installation level. The number of Network Operations and Security Centers (NOSCs) required at each level will be studied. Through proactive event management and performance monitoring, a Service Level Management paradigm will be provided to Army infostructure users and warfighters. An enterprise missions and functions matrix is being developed to delineate detailed enterprise systems management requirements, responsibilities, phasing, and performance measures.

A technical Configuration Control Board will be established to manage configuration changes to the infostructure. A key concept will be the introduction of a networthiness process to review the designs and certify newly implemented systems before they are accepted into the infostructure.

NETCOM, as the Army's Functional Proponent for NETOPS, has the lead for developing the NETOPS components of the AKEA. In this role, NETCOM/9th ASC will develop the necessary architectural and requirements documentation to support the AKEA. NETCOM, in coordination with PEO EIS, PEO C3T, and TRADOC, will ensure the NETOPS architecture is implemented across the ONE Army.

NETCOM/9th ASC and the Army will leverage the results of the Military District of Washington (MDW) Proof of Concept (PoC) and the Ft Carson pilot to refine the Enterprise Management processes at the installation level in support of developing ESM requirements and the necessary operational views of the NETOPS architecture. The initial requirements and architectural views will be developed NLT 1 Jul 03.

While it would be easier if the Army were able to implement an ESM from a blank sheet, the reality is that the Army has invested heavily in various network and system management tools over the past ten years. This has resulted in a heterogeneous environment at all levels of the Army operational structure. Therefore, NETCOM/9th ASC will develop an ESM Migration Plan to move the Army into an interoperable, if not homogeneous, ESM environment. The initial version of the ESM Migration Plan will be developed NLT 1 Oct 03 and be based upon the initial requirements and architectural documents produced in 1 Jul 03.

c. Specific Responsibilities

1) CIO/G-6

- Provide architectural and policy guidance to ensure the NETOPS architecture supports the ONE Army and the Objective Force.
- Coordinate proposed Army NETOPS architecture and requirements with appropriate HQDA staff.
- Provide resources necessary to implement approved NETOPS architecture.

2) ASA(ALT) PEO EIS

- Serve as the AKM Goal 3 integrator.
- Oversee consolidation and modernization initiatives as prioritized by and in coordination with NETCOM/9th ASC.
- Perform horizontal integration of systems and systems components comprising AEI as prioritized by and in coordination with NETCOM/9th.

- Serve as Material Developer for the Army's ESM capabilities.
 - Support NETCOM/9th ASC in the development of NETOPS architectural products.
 - Manage cost, schedule, performance and supportability for assigned responsibilities.
 - Engineer, develop, acquire, and implement the Army's ESM capabilities in accordance with NETCOM/9th ASC requirements.
 - Support NETCOM/9th ASC in the development of ESM Migration/Implementation Plan in conjunction with NETCOM/9th ASC ESM architecture development.
- 3) ASA(ALT) PEO C3T
- Serve as material developer for ESM in the tactical environment.
- 4) NETCOM/9th ASC
- Functional Proponent for ONE Army NETOPS.
 - Publish NETOPS CONOPS.
 - Lead ONE Army NETOPS Architectural efforts.
 - Develop initial NETOPS requirements and architectural views NLT 1 Jul 03.
 - Develop in coordination with COIN functional proponents initial version of the ESM Migration Plan NLT 1 Oct 03.
 - Operate and manage the ONE Army ESM capability.
 - Establish Army Enterprise NETCOP.
- 5) AMC CECOM
- In coordination with G2 and NETCOM/9th ASC, provide acquisition life-cycle intelligence support to PEO EIS and C3T.
- 6) DOIM
- Provide feedback on ESM requirements.

- Implement interim local network and system management capabilities in accordance with Army policy and architecture.

7) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC ESTA Governance and NETOPS Directorate

3.2.3. AEI Systems Integration

a. Desired End State

The integration of the systems-of-systems components comprising the AEI.

b. Actions

The AEI is a system of systems with many components: wide area networks, base installation networks, email servers, web servers, other application servers, desktops, operating systems, directory services, security services including PKI/CAC, etc. Each of these components will be in a continuous state of change as technology changes and as the AEI evolves to the objective AKEA. The role of the AEI systems integrator is to ensure these systems of systems work together as a whole. For example PKI/CAC needs to work with Enterprise Directory Services and Active Directory, although they are each separate programs.

Sourcing strategy for the AEI integrator role is dependent upon core IT competencies that support the Army mission and need to be sourced internally. AKM objectives to be considered in determining the AEI integrator role include control, flexibility/risk, total cost of ownership, and investment funds required. The CIO EB approved the AEI acquisition strategy in May 2002, naming PEO EIS as the system integrator.

PEO EIS as the AEI systems integrator will oversee various consolidation and modernization efforts, ensure consistency with enterprise architecture and policies, and capture lessons learned. PEO EIS will utilize the capabilities of the Army core engineering assets, the organization of which is examined in a Part 1 task, augmented by contractor support.

c. Specific Responsibilities

1) CIO/G-6

- Provide policy and guidance to the AEI systems integrator.

- Review AEI implementation plans to ensure compliance with the enterprise architecture.
 - Secure resources for AEI systems integration.
- 2) ASA(ALT) PEO EIS
- Oversee consolidation and modernization initiatives.
 - Perform horizontal integration of systems of systems components comprising the AEI.
- 3) NETCOM/9th ASC
- Review AEI implementation plans to ensure consistency with NETOPS CONOPS.
- 4) Points of Contact
- CIO/G-6 IOM
 - PEO EIS.

3.2.4. Single DOIM Concept

a. Desired End State

A single DOIM on an installation will manage AEI assets.

b. Actions

AR 25-1, paragraph 3-9, mandates each garrison/location (or in some OCONUS theaters, and Installation Support Area) will have a single IM entity charged with the delivery of C4IM services to customers. This is called “the single DOIM concept”. Garrison commanders will implement the Single DOIM concept in accordance with AR 25-1 and Information Management Execution Plan Annex E dtd 1 Jul 02. HQDA will coordinate and document any resource transfers using the POM process.

The Information Management Execution Plan Phase I identified the requirement to implement the “single DOIM” concept by moving common user C4IM services, manpower assets and funding streams into the garrison single DOIM. DOIMs will identify those assets through the NETCOM/9th ASC RCIO to the IMA RD NLT 1 Oct 03. The Installation will consolidate common user services to the garrison DOIM Centralized Documentation (CENDOC) paragraphs NLT Jan-Apr 05 Management of Change (MOC) window. The IMA in coordination with NETCOM/9th ASC and the CIO/G-6 will coordinate the migration of identified

resources from the owning MACOM to the single DOIM on the Installation. IMA, with recommendations from NETCOM/9th ASC, will manage the Schedule 8 migrations of the resources.

As previously noted, certain COINs have achieved a high degree of centralized management and enterprise-level efficiency in C4IM service delivery, enabled by VPN transcending existing geographic and political boundaries. Those services are often provided to locations under single-DOIM control. Functional RCIOs will coordinate with IMA and NETCOM/9th ASC, as necessary, to ensure services are maintained at required levels within available funding.

ACSIM and CIO/G-6 have asked the AAA to conduct a review of Army garrisons to identify where multiple DOIMs exist and recommend solutions to the ACSIM, IMA, MACOMs, and CIO/G-6 for decision and resolution. The audit will also provide information on instances where the DOIM has not been made part of the Army garrison/facility structure and supporting rationale. Upon completion of the AAA audit, it is anticipated that common user services will be merged into the single DOIM concept, and resources transferred into the single DOIM.

Each Garrison/Army Site will have an identifiable DOIM who reports directly to the garrison commander for information services. DOIMs will be under the TECHCON of NETCOM/9th ASC RCIOs. The IMA in coordination with NETCOM/9th ASC will provide a basic blueprint for a standardized job description for the DOIM position. All garrison DOIMs will use this blueprint job description tailored to the local conditions as the basis for future standardization and delivery of services. The garrison commander in conjunction with the NETCOM/9th ASC RCIO will be the selecting official for all DOIMs. The consolidation of resources on each installation will be based on the AAA findings and be completed by 1 Oct 04.

c. Specific Responsibilities

1) CIO/G-6

- In coordination with ACSIM and supported MACOMs, develop and publish to Army garrisons standard procedures for identification of tenant DOIMs and procedures for transferring functions and resources to the garrison single DOIM, based on AAA analysis procedures. NLT 1 Oct 03.
- Establish DOIM responsibilities and provide input to incorporate into institution publications.
- Provide written approval to tenant and ACSIM for specific exemptions to policy.

- Work the issues raised by NETCOM/9th ASC RCIO and MACOMs to final resolution.

2) ACSIM and IMA

- In coordination with CIO/G-6 and supported MACOMs, develop and publish to Army garrisons standard procedures for identification of tenant DOIMs and procedures for transferring functions and resources to the garrison single DOIM, based on AAA analysis procedures. NLT 1 Oct 03.
- Work with tenants owning DOIMs and Information Management Officers (IMOs) to identify the workload, required manpower, physical assets and support dollars.
- In coordination with NETCOM/9th ASC provide standardized blueprint for job description for DOIM.
- Provide implementation guidance and assistance to enforce the single DOIM policy.
- Establish and maintain central repository of exemptions to single DOIM concept.

3) AAA

- Conduct a review of selected Army garrisons for compliance with the single DOIM concept.
- Provide recommends to the CIO/G-6 and ACSIM on what should be moved to the garrison DOIM and what should remain with the tenant.
- Provide a standard procedure for analyzing tenant DOIMs to determine which functions and resources should be performed by the tenant IMO and which by the garrison single DOIM.

4) NETCOM/9th ASC

- Assist the IMA in developing a standardized blueprint for a DOIM job description.
- In CONUS, serve as selecting official, with the garrison commander, for DOIMs and Intermediate Rater for DOIMs.

- Assist the IMA RD to move tenant DOIM functions and resources to the DOIM paragraphs in CENDOC.

5) Garrison Commander

- Serve as selecting official, with NETCOM/9th ASC RCIO, for DOIM and rates DOIM.
- Enforce the single DOIM concept.
- Place the tenant DOIMs under OPCON of the single installation DOIM.
- Coordinate Service Level Agreements with tenants Identify transfer of appropriate tenant DOIM functions and resources to the garrison DOIM.

6) DOIM

- Identify to the IMA RD through NETCOM/9th ASC RCIO and the garrison commander, the installation tenant DOIM assets and NLT 1 Oct 03.
- Support and host the AAA Team.

7) Points of Contact

- CIO/G-6 IOM
- IMA
- NETCOM/9th ASC ESTA/RCIO

3.2.5. Visual Information

a. Desired End State

Provide quality, installation-level Visual Information, Training Support Centers & Training Aids Devices Simulators and Simulations (TADSS) services to all customers.

b. Actions

The CIO/G-6, in coordination with the Army G3, the IMA, and NETCOM/9th ASC, will develop a plan for providing and managing installation VI services to include TADSS, by 31 Mar 04. The plan will provide implementation guidance and milestones, and will be based on:

- A review of current management, funding, and provisioning of installation-level VI services, including traditional VI functions (still and motion imagery, graphics, static displays, etc.), and training functions (TADSS, etc.).
- The linkages of each service the missions it supports.
- Explore opportunities to consolidate VI services at the installation, or regional level.

To avoid the potential for multiple mission/personnel transfers, installation-level VI activities will remain under the organization to which they are attached, until implementation of the approved plan.

c. Specific Responsibilities

1) CIO/G-6

- In coordination with the G3, IMA, and NETCOM/9th ASC, develop the VI management plan NLT 31 Mar 04.
- In accordance with GO #3, provide policy and oversight of VI.
- Lead the effort to develop the VI plan to optimize installation-level VI services.
- Provide interim guidance on the management of installation-level VI activities NLT 15 Jan 04.
- Amend Chapter 7, Visual Information, AR 25-1, after plan approval.
- Act as functional proponent for VI services.
- Execute necessary documentation to implement resource transfers outlined in the approved plan for the FY06 MOC window.
- Receive reports as required, from the IMA regions.

2) G3

- Act as the functional proponent for TADSS.
- Provide funding for installation TADSS requirements.
- Participate, along with CIO/G-6, the IMA, and NETCOM/9th ASC, in the development of the VI plan.

3) IMA

- Participate, along with CIO/G-6, the Army G3, and NETCOM/9th ASC, in the development of the VI plan.

4) NETCOM/9th ASC

- Execute CIO/G-6 VI programs and functions.
- Provide implementation guidance for Army policy to installation VI managers, as needed.
- As the VI manager for the IMA regional director:
 - Consolidate and forward VI reports from the installations within their respective region to CIO/G-6.
 - Forward installation VI UFRs, POM requirements, etc. to IMA.
 - Participate, along with CIO/G-6 , and the IMA, in the development of the VI plan mentioned above.

5) DOIM

- Identify spaces to be moved to the CENDOC TDA to align in accordance with the VI plan.
- Work with their Regional VI Manager to identify and resolve VI issues.
- Prepare reports in accordance with guidance and forward to Regional VI Manager.
- Execute VI program in accordance with AR 25-1 and DOD guidance ensuring delivery of baseline services on a non-reimbursable basis, and 'above baseline' as specified in the SLAs.

6) Points Of Contact

- CIO/G-6 IOM
- Army G3
- IMA
- NETCOM/9th ASC - ETSA

3.2.6. Sub-Installation Support And Relationships

a. Desired End State

Subordinate Installation relationships independent of regional boundaries where the business case justifies the alignment.

b. Actions

The IMA will conduct a review of all parent-subordinate relationships between installations and recommend continuance or modification. Determining factors will be personnel assets, operational design capabilities, and network efficiencies. This is to be a coordinated action between IMA and NETCOM/9th ASC for consistency as there are information management issues, which impact the final decision. DOIMs will provide input on subordinate installation to NETCOM/9th ASC NLT 1 Jan 03 (completed). NETCOM/9th ASC will forward input to the IMA NLT 1 Aug 03 for implementation on 1 Oct 03.

c. Specific Responsibilities

1) CIO/G-6

- Review for approval NETCOM/9th ASC recommendations.

2) IMA

- Review input for final determination on sub-installations NLT 1 Sep 03.
- Implement any changes resulting from decision NLT 1 Oct 03.

3) NETCOM/9th ASC

- Receive initial sub-installation information from DOIMs.
- Coordinate any budget/TDA implications with IMA.
- Provide recommendation to IMA.

4) DOIM

- Provide input to NETCOM/9th ASC on sub-installations Information Management functions, e.g. when/why/who/how the relationship was created; how many DOIM assets are on sub-installation; what functions they're performing; what (if any) functions the parent organization is performing for the sub-installation. (completed)

5) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC G8
- IMA

3.3. MISSION THREE – REDUCE TOTAL COST OF OWNERSHIP

3.3.1. Business Case Analysis

a. Desired End State

An Army-wide Business Case Analysis (BCA) encompassing multiple alternatives for server consolidation, email, active directory implementation, enterprise systems management and consideration of the various CNA and CNE arrayed against the implementation strategies and technical alternatives.

b. Actions

The objective is to develop an Army-wide BCA strategy. Initial BCA/Analysis of Alternatives (AoA) has focused on MDW and USAREUR 80th Area Support Group (ASG). This will be expanded to other AEI initiatives to provide data for performing Army-wide extrapolation in accordance with OMB Circulars A-94 and A-130. The effort will document the “as is” state, develop performance metrics, develop alternative approaches, and build a BCA and life cycle cost estimate. Alternative architectures will be considered for server consolidation, email, active directory implementation, and enterprise systems management. CONOPS alternatives will be considered for ANOSC and TNOSC management of servers and desktops. A qualitative comparison of alternatives will be made. The BCA will be expanded to include other AEI initiatives, so as to obtain a representative Army-wide sample. Changes in total cost of ownership and investment will be used to calculate Army-wide return on investment including indirect savings/cost avoidance. The BCA will determine implementation strategy among technical alternatives.

c. Specific Responsibilities

1) CIO/G-6

- Provide policy and guidance for the scope of BCA/AoA. Criteria will be defined for determining when implementation alternatives are selected based on BCA, and when broader architecture principles are involved that need to be considered as part of the enterprise architecture.

- Review architectural alternatives to be considered in BCA/AoA.
 - Secure resources for BCA/AoA.
- 2) ASA(ALT) PEO EIS
- Complete MDW BCA NLT 1 Oct 02.
 - Complete USAREUR BCA NLT 1 Jun 03.
 - Develop Army-wide BCA.
 - Make recommendations to CIO/G-6 per the BCA findings.
- 3) MACOMs and Functional Proponents
- Support BCA data collection efforts.
- 4) NETCOM/9th ASC
- Review architectural alternatives to be considered in BCA/AoA.
 - Develop threat analysis to support the BCA/AoA to ensure that such key issues as server consolidation, active directory implementation, and CNA and CNE are considered.
- 5) Points of Contact
- CIO/G-6 IOM
 - ASA(ALT) PEO EIS.

3.3.2. Acquisition of IT

a. Desired End State

Enterprise-wide contracts to achieve economies of scale.

b. Actions

In concert with Information Technology E-Commerce and Commercial Contracting Center (ITEC4), PEO EIS will establish contracts that provide hardware solutions and enterprise support services such as server consolidation, WAN/LAN/seat management, software, systems engineering and design, storage area networks, building cable installation, information assurance, and systems administration, help desk support, AD implementation, Defense Information Technology Security Certification and Accreditation Program (DITSCAP)

certification, business process reengineering, etc. NETCOM/9th ASC will support PEO EIS in identifying vendors and other providers with issues relating to foreign ownership, control, or influence (FOCI) to assist in the management of risk associated with the establishment of contracts.

Enterprise-wide contracts will be available through ITEC4. The CIO/G-6 in cooperation with ITEC4 will develop and establish the guidelines on the purchasing of IT items and services. It is the intent of the CIO/G-6 to mandate that all procurements of commercial IT products (not tactical) go through ITEC4. The CIO-G-6 will establish policy NLT 1 Oct 03. The Army Contracting Agency (ACA) will produce guidelines to all contracting agencies on the prohibition of purchasing IT items and services from other than ITEC4. ITEC4 guidelines will be published NLT 1 Oct 03. The NETCOM/9th ASC RCIO in concert with the DOIMs will identify potential areas of opportunity for regional or national contracts. DOIMs will architecturally approve purchases and process through the Directorate of Contracting (DOC) and ITEC4 all IT items and services for all customers and ensure appropriate property book accountability.

c. Specific Responsibilities

1) CIO/G-6

- Establish policy on use of ITEC4 NLT 1 Oct 03.
- Work with ACA to produce policy and guidance that all commercial IT procurements go through ITEC4.

2) ASA(ALT) PEO EIS

- Work with ACA to develop enterprise contracts under ITEC4.

3) ACA

- Produce ITEC4 guidelines NLT 1 Oct 03.
- Award enterprise contracts under ITEC4.
- Produce guidelines to all contracting agencies on the prohibition of purchasing IT items and services from other than ITEC4.
- Ensure publication and distribution of policy guidance on IT acquisition and provide any implementation guidance as required.

4) NETCOM/9th ASC

- Monitor IT purchases; consolidate reports, analyze and identify purchase trends for opportunities for regional and/or national contracts.
- Provide FOCI analysis to PEO EIS and ITEC4.
- Work with ACA/ITEC4 to establish regional/national contracts.

5) DOIM

- Develop relationship with local DOC.
- Ensure installation customers are aware of architectural approval process for the procurement of IT products and services.
- Be the installation architectural approval authority for IT purchases.
- Develop report of IT products and services and submit to the RCIO.

6) Point of Contact

- CIO/G-6 Acquisition Cell

3.3.3. Server Consolidation

a. Desired End State

Consolidated servers at the installation or region with improved security and service levels and reduced overall IT costs and footprint.

b. Actions

AKM Implementing Instructions #2 for Goal 3 instructs the Army community to reduce the number of servers on their posts, camps, and stations by 30 percent (from the September 01 baseline) NLT 1 Oct 03: The end-state goal is to reduce the number of servers by 50-60 percent, similar to what industry has achieved through their server consolidations. Consolidation at the installation level will facilitate and enable future migrations to a regional strategy, given available bandwidth and facilities. When submitting requirements, DOIMs may also include funding requests for common user communications and computing routers, distribution hubs, and garrison fixed station Video Teleconferencing (VTC) facilities.

RCIOs working with DOIMs will initiate plans for consolidating email, web, file, domain controller, print, and application servers on their posts, camps, and

stations. The DOIMs on each post will consolidate servers for Army tenants residing on the post to a minimum number of server cluster locations. : **No activities or servers are excluded from server consolidation except deployable assets.** Any exceptions to the AKM guidance memorandum are reserved for SECARMY approval. Status of server consolidations will be reported to senior Army leadership on a quarterly basis through the CIO EB and the Strategic Readiness System.

While some activities may preclude server consolidation, as noted below, all activities will support server consolidation in accordance with the SECARMY AKM guidance memorandum and CIO/G-6 implementing instructions. The CIO/G-6 recognizes server consolidation is a formidable task. The DOIMs should first focus on what can be easily achieved in the near term (email, web, file, print servers to include sustaining base application servers) and document any non-participating activities.

There are activities receiving processing support from centralized locations, such as the IG, USAR, and NGB, that the DOIM is not responsible for consolidating. In addition, there may be standalone servers required to support deployed forces. Even though medical, research and development, intelligence, and investigative activities are sensitive in nature, funded by other Defense/Federal Agencies, or support joint programs, these activities will be considered as candidates for area or theater consolidation and for integrated support centers. These activities will consolidate and operate their applications under the oversight of the DOIM. Their unclassified common user services, where not consolidated on a regional or Army wide basis, will be provided by the DOIM to support phased migration to enterprise service management and global directory services.

The DOIMs are responsible for baselining and reporting in a server consolidation plan on all unclassified Army server assets for all Army tenants (to include other HQDA/MACOM/PEO tenants) residing on the installation. Garrison tenants receiving processing services from another location should be reported by the entity responsible for providing those services and noted (with supporting rationale) as non-participating tenants in the server plan for their resident installation (e.g., NGB, USAR, IG, United States Army Corps of Engineers (USACE), United States Army Accessions Command (USAAC)). Quarterly status reporting of server consolidations is the responsibility of the DOIM. If the DOIM has negotiated an agreement with a tenant to establish a separate server farm on the installation, under the oversight of the DOIM, it is still the responsibility of the DOIM to baseline and report status of these server farm assets.

Army activities not residing on an installation or under the direct support of a DOIM will submit plans and quarterly reports on their server consolidation (e.g., Personnel Command (PERSCOM), USACE, USAAC, RDAISA, SMDC, USAR,

NGB). HQDA functional proponents/MACOMs should report their respective activities not residing on an installation or under the direct support of a DOIM. Functional processing centers and sites should be separately reported. OCONUS commands will report server consolidation plans by their Area of Responsibility (AOR) or ASG, as these commands are assigned in geographic regions.

The intent is to consolidate users on common processing platforms where feasible and economical, not just co-locate servers. The DOIM may designate other server farm locations to accommodate floor space limitations. DOIMS should consider continuity of operations, network access, and facility improvements (e.g., back-up power, heating, ventilation, and air conditioning, storage) required to support server consolidation for enhanced system availability and reliability. It is also the Army's intent that all servers and associated system administration personnel will be relocated and consolidated to facilities specified by the DOIM.

The process for transferring system administrators to the garrison DOIM is still under development. The first step, however, is the DOIMs will need to begin documenting resources required to support operations as tenant servers are consolidated into their facilities. This documentation will then become the foundation for resource transfers and investment analyses. In the interim, similar to the HQDA Information Management Center (IMCEN) support agreements, full-time system administrators should be placed under operational control of the DOIMs upon signature of the tenant SLAs. Once TDA changes are approved, action can be taken to officially transfer the authorized spaces and associated funding. If personnel are not available to transfer, then the DOIM must be reimbursed for services and the funding identified for future transfer.

The CIO/G-6 will develop the format for submitting requirements for future POM builds and spend plans during the year of execution. DOIMs will submit their requirements for server consolidation through their garrison commander and RD to the CIO/G-6 by the end of the first fiscal year quarter for review and prioritization. The RD will coordinate DOIM requirements with their NETCOM/9th ASC RCIO prior to forwarding requirements to the CIO/G-6. NETCOM/9th ASC, in coordination with PEO EIS and AMC CECOM Information Systems Engineering Command (ISEC), will conduct a technical and cost evaluation of the requirements and recommend to the CIO/G-6 which requirements should be resourced based on mission criticality, implementation strategy, and more importantly, return on investment. A different format will be developed for submitting POM input but the same requirements process flow will apply. When submitting requirements, DOIMs may also include other funding requests for common user communications and computing upgrades needed for the server farm(s), garrison backbone and connectivity to the DISN (e.g., data switches, routers, distribution hubs), Private Branch Exchange (PBX) switches, and garrison fixed station VTC facilities. MACOMs will submit to the CIO/G-6 their

requirements for POM years and spend plans for the year of execution, which support end user connectivity to the garrison backbone.

To assist the DOIMs, PEO EIS will establish a core team to coordinate, integrate, and engineer DOIM plans for server consolidation. In addition, PEO EIS will be publishing implementing guidelines, naming conventions, design templates, and "to be" business processes for enterprise service management. A number of initiatives are being conducted to determine the optimum approaches to server consolidation and enterprise systems management, supported by BCA. These related activities are described in the following paragraphs:

- The MDW initiative is transitioning Army tenants to PKI, Windows 2000, Active Directory, and consolidating email services into centralized Exchange 2000. Phase 1 of the transition is to move 1000 MDW users at Fort Belvoir to the AD and Enterprise Management infostructure, managed by NETCOM/9th ASC. Phase 2 will focus on the remaining MDW Army users at Fort Belvoir, Fort Myer, Fort McNair, Fort Meade, Fort A.P. Hill, and Fort Hamilton. MDW will include implementation of an Enterprise Management Solution (ANOSC, TNOSC, Network Security Center (NSC), NOC) that allows NETCOM/9th ASC to perform its mission as the single authority to operate and manage the Army's infostructure down to the server level. A single 1-800 Army Help Desk solution will be provided. Use of PKI/CAC will be demonstrated for signing/encrypting email. A BCA will be conducted to select an optimal architecture among several alternatives for server consolidation and enterprise management. Server reduction is projected at 80%.
- In the USAREUR initiative, IT services are defined within five categories: server management, end-user services, help desk, local network, and wide area network. The initial server consolidation was at HQ USAREUR in Heidelberg. A task order request for IT services to support server consolidation has been awarded for the 80th ASG, with options to extend to the rest of Europe. The initial scope is the 80th ASG with options to extend to the rest of Europe. Work includes baselining, developing target configuration options, conducting analysis of alternatives, designing and implementing the consolidation and preparing SLAs.
- The Commanding General 7th Infantry Division, Fort Carson, initiated a plan for server consolidation. Data center upgrades and consolidated common services (email, file and applications) were implemented in FY00. Centralized data storage architecture and enterprise backup system were deployed in FY01. Collapsing NT domain controllers and WIN2K desktop migration was implemented in FY02. Web server consolidation started in FY02. Enterprise Systems Management is planned for FY03.

- There will be a centralization of all HQDA IT elements under HQDA DOIM IMCEN control. Desktop support services will be consolidated under IMCEN. The desktop services transition will involve a managed transfer of personnel, contracts, and funds associated with delivery of desktop services from HQDA organizations to IMCEN. SLA will be established and full desktop services life cycle support of the HQDA organization will be assumed by IMCEN. HQDA agencies will complete the transition in FY 03. HQDA server consolidation will follow the consolidation of IT services, with a projected 70 percent reduction in servers.

c. Specific Responsibilities

1) CIO/G-6

- Provide policy and establish reporting requirements to measure progress in server consolidation.
- Provide program oversight for all server consolidation initiatives.
- Approve consolidation strategy.

2) ASA(ALT) PEO EIS

- Manage and integrate the MDW and other server consolidation initiatives, leading to enterprise-wide server consolidation strategy.
- Coordinate, integrate, and engineer (if necessary) DOIM server consolidation.
- Produce documentation on AD implementation guidelines, naming conventions, design templates, and lessons learned.
- Analyze all ongoing Army ESM initiatives to determine optimum solution.
- In coordination with NETCOM/9th ASC, develop an overarching Application Consolidation Strategy to include engineering/cost analysis that will:
 - Identify target applications for consolidation at a Enterprise level, Regional level, or Installation level.
 - Identify target environments for consolidation; e.g. Army locations, DISA Megacenters, and commercial locations.
 - Determine if Army should procure its own enterprise services

(e.g., email, web hosting, etc) or procure these services from DISA or commercial sources based on Service Level Agreements.

- Identify non-core services that could be contracted with industry.
- Outline a pilot/first implementation that tests/proves consolidation strategy prior to fielding enterprise-wide.

3) NETCOM/9th ASC

- Develop a consolidation strategy for CIO/G-6 approval.
- Ensure that server consolidation plans, ESM, AD implementation, and regional consolidation design are consistent with NETOPS CONOPS to include regionalized consolidation of email, file, print, and web servers; migration to WIN2K/AD and Exchange 2000; and enterprise management.
 - Perform enterprise operations and management.
- Develop, in conjunction with PEO EIS, an overarching Application Consolidation Strategy to include engineering/cost analysis that will:
 - Identify target applications for consolidation at a Enterprise level, Regional level, or Installation level.
 - Identify target environments for consolidation; e.g. Army locations, DISA Megacenters, and commercial locations.
 - Determine if Army should procure its own enterprise services (e.g., email, web hosting, etc) or procure these services from DISA or commercial sources based on Service Level Agreements.
 - Identify non-core services that could be contracted with industry.
 - Outline a pilot/first implementation that tests/proves consolidation strategy prior to fielding enterprise-wide.
- Report quarterly on server consolidation progress.
- Review DOIM plans for server consolidation.

4) DOIMs

- Initiate plans for server consolidation.
- Execute server consolidation and implement ESM.
- Report quarterly on server consolidation progress using web based automated tools provided.

5) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC ESTA

3.3.4. Enterprise Email and Web Server Strategy

a. Desired End State

All Army using web based mail, anywhere, anytime.

b. Actions

The AEI end-state objective is for applications to be web enabled, thereby greatly simplifying desktop configuration management. This includes email applications. At present, the web-enabled email available on AKO has less functionality than client-server based email.

NETCOM/9th ASC will assess web-based mail emerging technologies and make a determination based on business and technical cases, what is appropriate for AKO.

Concurrently, DOIMs will initially consolidate servers at the installation level using current software with planned migration to AD and a regional consolidation architecture. NETCOM/9th ASC will develop AKO portal email capability to support non-LAN based users.

The following diagram illustrates this phased approach moving from the current distributed server environment to the full implementation of the single AKO Portal email and associated portal services. See Figure 2.3-2.

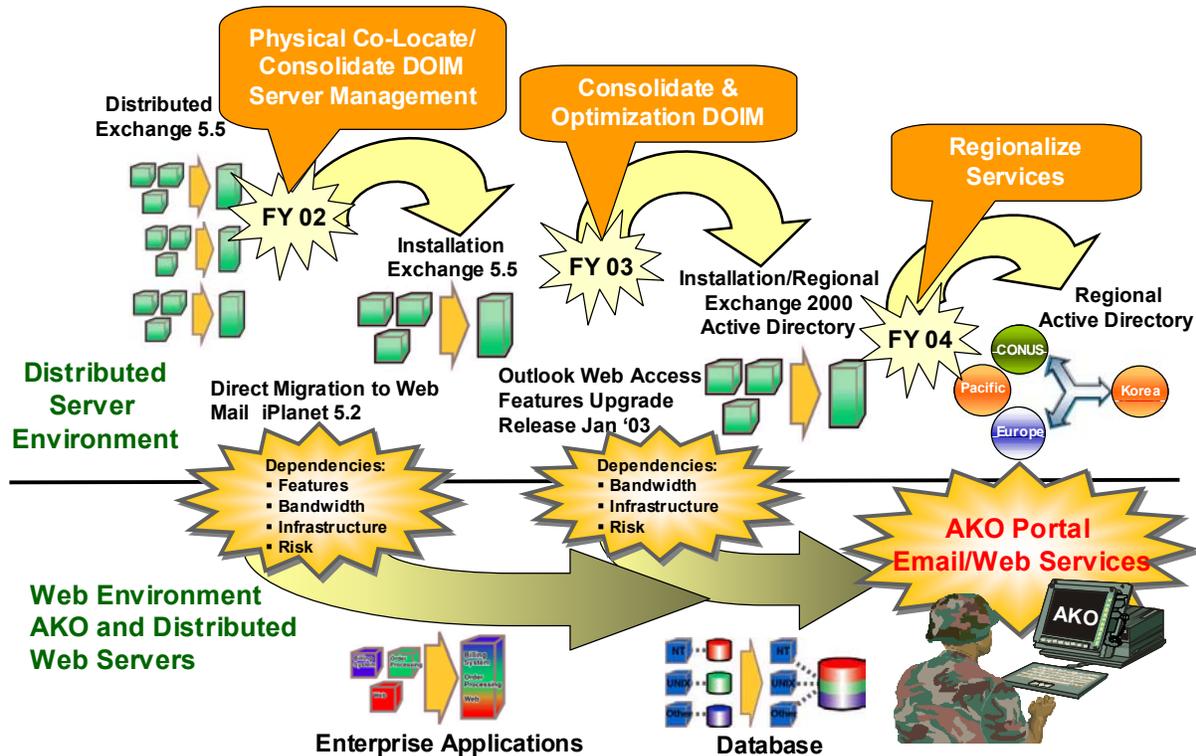


Figure 2.3-2 Enterprise Email and Web Services Strategy

c. Specific Responsibilities

1) CIO/G-6

- Integrate web-based email recommendations into enterprise architecture.

2) NETCOM/9th ASC

- Develop email capability through AKO portal to support non-LAN based users.
- Assess web-based mail emerging technologies and determine selection based on business and technical cases.

3) Point of Contact

- CIO/G-6 IOM

- NETCOM/9th ASC CTO

3.3.5. Commercial Activities for Completed A-76 Studies

a. Desired End State

Adjust commercial activities (CA) for completed A-76 studies to standardize common user services.

b. Actions

The ACSIM and IMA with the CIO/G-6 and NETCOM/9th ASC will conduct a post competition assessment that will be used to develop standard services. The Objective Force requirements of the future army combat doctrine as it impacts base operations (BASOPS) and power projection must be integrated into this study.

IMA and NETCOM/9th ASC will form a team(s) to review all DOIMs that have been competed in accordance with OMB Circular A-76, for compliance with the established CIO/G-6 and ACSIM standards and service levels. Those DOIMs that do not conform to the CIO/G-6 and ACSIM standards will be adjusted to the standard using existing legal and contracting authorities. After reviewing for conformity a decision will be made to continue the studies or pursue another methodology such as strategic sourcing, direct conversion, outsourcing, existing contracts and other centralized contracts. Assessments are to be completed NLT 1 Oct 04.

For those studies involving DOIMs that have not been concluded by award IMA and NETCOM/9th ASC will review, with the garrison commander, to insure that the acquisition and force structure strategy is in compliance with the Single DOIM concept and CIO/G-6 and ACSIM standards. A list of impacted garrisons will be provided by the ACSIM and a rapid survey (less than 30 days) will be conducted to assess the total scope of the issue. Recommendations will be made based on the survey.

c. Specific Responsibilities

1) CIO/G-6

- Align the DOIM Organizational Design Strategy to the Army's outsourcing strategy.
- Support the Army outsourcing program.
- Act as subject matter expert to the ACSIM for outsourcing studies involving C4IM.

- Approve C4IM outsourcing strategy.
 - Approve the adjustment strategy.
- 2) ACSIM
- Define an outsourcing strategy.
- 3) IMA
- Form a team(s) to visit each installation and assess the road ahead requirements to bring the DOIM structure in line with the baseline service strategy.
 - Develop and recommend a plan for course(s) of action in accordance with legal, outsourcing goals, and acquisition regulations.
- 4) NETCOM/9th ASC
- Review regional recommendations for best methodology to meet NETCOM/9th ASC standard services.
 - Act as subject matter expert to the IMA for outsourcing studies involving C4IM.
- 5) DOIM
- Provide to RCIO the potential scope of the task on their installation.
 - Provide to RCIO outsourcing information, including where in the process the DOIM currently stands.
 - If completed CA process, gather performance data to include job analysis, performance standards, identification of performance indicators, and acceptable levels of performance.
 - Identify lessons learned.
 - Identify variations between what is currently performed and what is required in baseline services.
- 6) Points of Contact
- CIO/G-6 IOM
 - IMA

- NETCOM/9th ASC ESTA/RCIO

3.4. MISSION FOUR – DELIVER SECURE WEB-BASED, INTEROPERABLE, AND OPEN SYSTEMS

3.4.1. Army Enterprise Networkiness Certification

a. Desired End State

All automated information systems (AIS) connected to the AEI-T are assessed for risk to the network, networkiness, and compliance with AKEA.

b. Actions

The Army Networkiness Certification will be done for all AIS. The Army will synchronize existing processes (such as POM, DITSCAP, Command, Control, Communications, and Computers Intelligence Support Plan (C4ISP), etc) and issue two certificates – a CON and a CTO. The CON ensures all AIS are documented and validated for meeting supportability, security, compatibility, integration, manageability and interoperability requirements. The CTO validates, from a location-centric view, that the resulting infostructure can support the system, that there is no negative impact to existing systems, that it does not introduce any security vulnerability, and that it can be managed and maintained from a life cycle perspective. The CIO/G-6 will issue the CON and NETCOM/9th ASC will issue the CTO, with notification by both to the CIO EB. The CIO/G-6 and NETCOM/9th ASC will develop the CON and CTO evaluation criteria, in concert. The policy memorandum implementing Networkiness Certification will be issued prior to 1 Jun 03.

For this program a change is a deviation on a baseline system that:

- Impacts any infrastructure requirement that varies bandwidth and spectrum support requirements.
- Affects how planned necessary lifecycle resources have been provided.
- Introduces new technology to an existing system.
- Alters the dependencies and interface requirements between systems.

The requester must submit a request for Networkiness through the appropriate chain of command to the CIO/G-6. The CIO/G-6 will record the request, perform a document review, and staff for assessment. NETCOM/9th ASC will perform technical assessment for CON and start the CTO assessment. Figure 2.3-3 is a high level Networkiness Certification process flowchart and depicts the interrelationship of major documents and the key contributors. The Army's

Networthiness Certification process incorporates and demonstrates the completeness of guidance, formats, and procedures such as the AKEA, C4ISP, the DITSCAP/System Security Authorization Agreement (SSAA), and existing developmental and test reports. If there are questions about the package, the CIO/G-6 will work with the requesters to find appropriate answers.

The complexity and scope of the proposed AIS or change will determine the time required for Networthiness Certification. This will be based upon potential risk and availability of information in the evaluation categories, as shown in Figure 2.3-4.

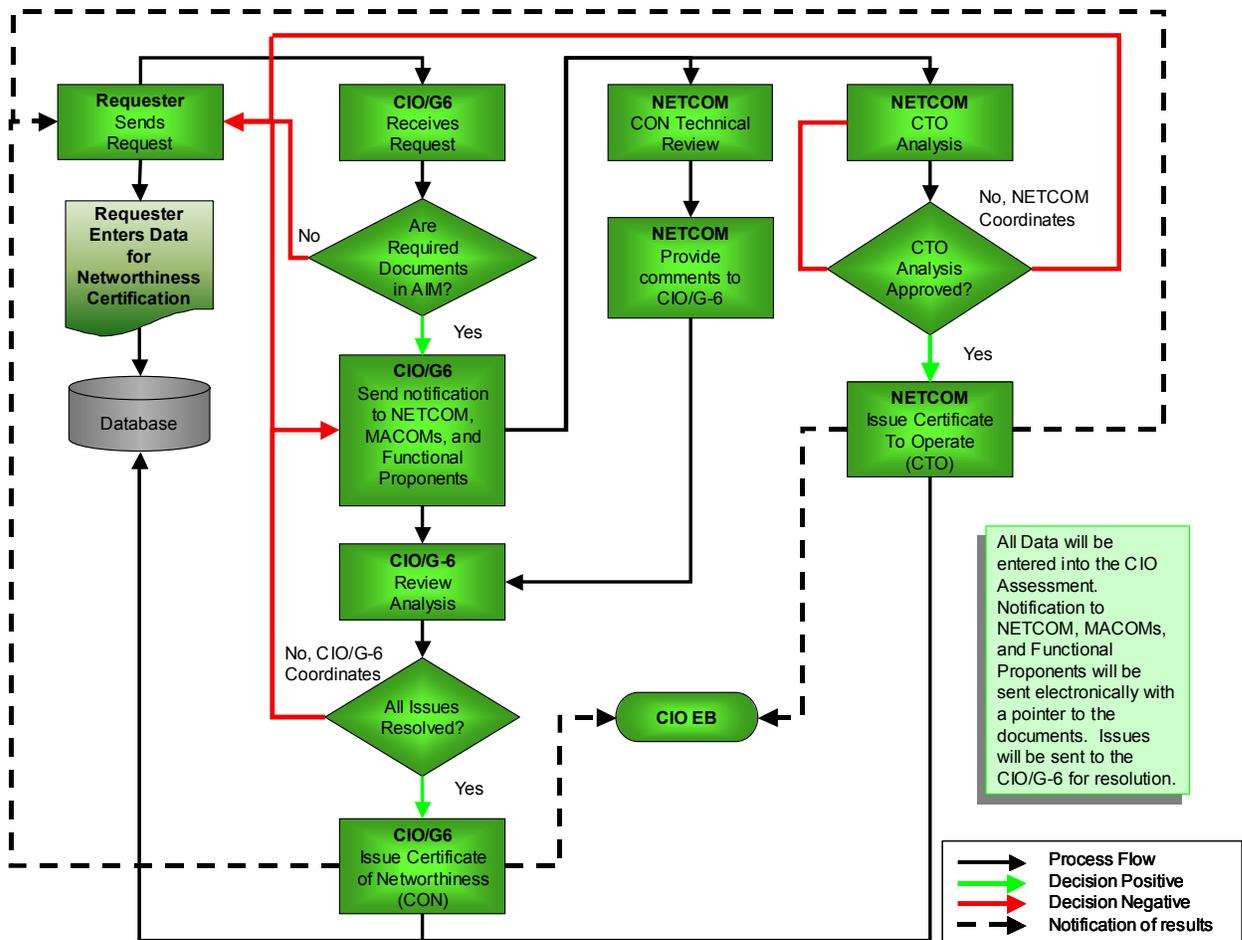


Figure 2.3-3 Networthiness Flow Diagram



Figure 2.3-4 Depth of Assessment

The process will assess the AIS to ensure that it will:

- Be supported by the infostructure.
- Not cause harm to existing systems or capabilities using the Army infostructure.
- Be operated and managed within the resources provided or available.
- Not cause security vulnerability within the Army infostructure.

c. Specific Responsibilities

1) CIO/G-6

- Develop, staff, and promulgate the Army Networkiness Certification program NLT 1 Oct 03.
- Synchronize tracking of requests for Networkiness Certification with related POM, DITSCAP, C4ISP actions and other processes as required.
- Coordinate and manage Networkiness Certification staffing and distribution.
- Work with requesters to resolve Networkiness Certification issues.

- Provide Networthiness Certification status to the CIO EB.
- Serve as the Certification Authority for Networthiness and issue CON.
- Oversee and sanction NETCOM/9th ASC in the development, coordination, and implementation of procedures for issuance of CTOs.
- Monitor, review, and assess the progression of related processes in accordance with the Interim Defense Acquisition Guidebook, October 30, 2002 (formerly the DoD 5000.2-R, dated April 5, 2002), NLT 1 Sep 04.
- Review and recommend revision of C4ISP, DITSCAP/SSAA, and CIO Assessment to synchronize with Networthiness Certification policy NLT 1 Sep 04.

2) IMA

- Provide guidance and program management on all installation-specific matters relating to Networthiness.
- Review the CON and provides recommendations to the CIO/G-6.

3) ASA(ALT) PEOs

- Oversee AIS research, development, tests, evaluations, and acquisition.
- Coordinate C4ISP milestones with the CIO/G-6.
- Incorporate recommendations for Networthiness Certification into the final C4ISP review.
- Ensure PEO and Program Managers (PM):
 - Follow the Networthiness Certification program.
 - Submit requests for Networthiness Certification for PEO-developed AIS and AIS components.
 - Provide resources for integrated test and evaluation activities associated with the issuing of a CON and CTO for new systems.
 - Review the CON and provide recommendations to the CIO/G-6.

4) MACOMs and Functional Proponents

- Comply with the Networkiness Certification program.
- Submit Networkiness Certification requests for requester-developed AIS to CIO/G-6.
- After 1 Sep 03, provide resources for test and evaluation activities associated with the issuing of a CON and CTO for the legacy AIS undergoing networkiness evaluation
- Review the CON and provide recommendations to the CIO/G-6.
- Assist the CIO/G-6, as requested.

5) NETCOM/9th ASC

- Review the Networkiness Certification requests and provide CON recommendations to the CIO/G-6 .
- Develop, coordinate, and implement procedures for issuance of CTOs NLT 1 Sep 03.
- Manage the CTO process and serve as the certification authority for and issue the Army CTO.
- Maintain configuration management over Networkiness implementation guidance and associated networkiness criteria.
- Coordinate with DOIMs to ensure tenants have initiated the Networkiness process and work with DOIMs on CTO issues.

6) DOIM

- Validate the existence of a CON and CTO for systems prior to connection to the local backbone.
- Submit local applications to the Networkiness process during development stages of the project.
- Ensure all changes have been processed in accordance with NETOPS CONOPS and the Army Networkiness process.
- Document and forward implementation issues or performance problems to RCIO.

7) Points of Contact

- CIO/G-6 IOE
- NETCOM/9th ASC ESTA Governance and NETOPS Directorate

3.4.2. Data Interoperability

a. Desired End State

Attain integrated, virtual, distributed '*One Database*' for the Army, able to access data anywhere, anytime, whenever needed, input information only once, reuse many times, and post before processing.

b. Actions

The concept behind the Army Knowledge Enterprise (AKE) Information Management (IM) Architecture Reference Model (see Figure 2.3-4) is that just as a house has an architecture and requires many different components to make it complete (e.g., plumbing, wiring, carpentry, etc.), to achieve data interoperability also requires an architecture. The Information Management Architecture Reference Model consists of three policy bands, four data standards blocks, and three layers of a shared data environment. The binding policy is similar to the cement that holds the bricks or blocks together, which keeps them from falling apart and failing to support the superstructure.

Army Knowledge Enterprise IM Architecture Reference Model

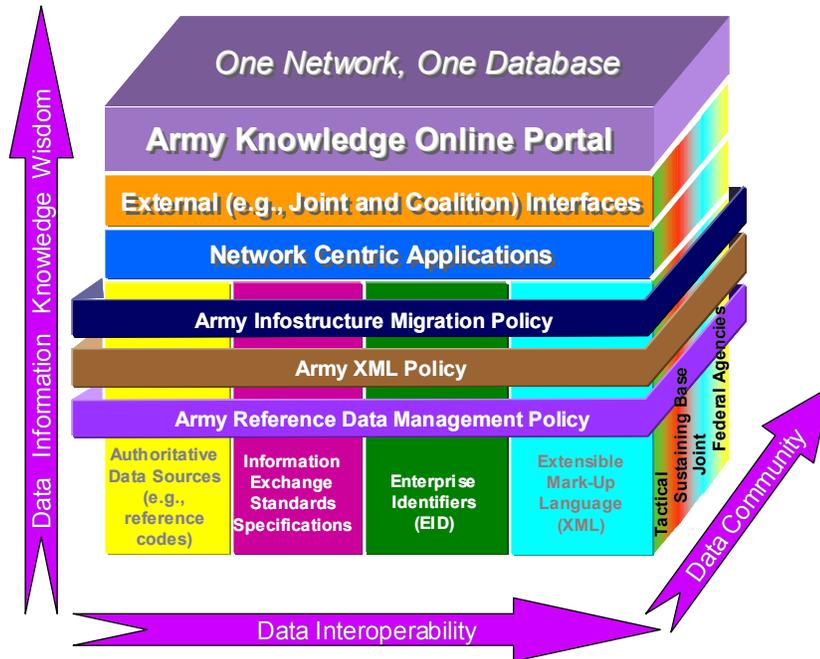


Figure 2.3-4. Four Components of the Army Data Standards Strategy in Relation to Network-Centric Applications and Desired End State

Binding policy for the Enterprise Information Management (EIM) Blocks: Army Reference Data Management, Army eXtensible Markup Language (XML), and Army Infostructure Migration. Enterprise Information Management includes policy for creating and adopting enterprise identifiers and information exchange standards specifications. EIM policies ensure that the requisite governance, support, resources, and tools are provided across the Army Enterprise, such that data are structured, documented, and managed to support information exchange within and across all commands, and among data producers and consumers within the Total Army environment.

Block 1: Authoritative Data Sources (ADS). An ADS provides a common data structure in module form that can be used to provide common domains of data values to different databases. An ADS provides the link between the logical model and the physical implementation. ADSs ensure interoperability between databases, reducing the need for translation. ADSs also contribute to easier and less costly maintenance of the database, and add to the testability of the database.

Block 2: Information Exchange Standards Specifications (IESS). An IESS is a narrowly scoped data model to facilitate data exchange and interoperability between communities of interest (COIs). IESSs are smaller, more manageable data models. COIs can develop their own COI data model for their communities and use their IESS as the common basis and translation mechanism between them. Unlike individual Application Programming Interface (API) calls that need to be modified to exchange the same data between several different systems, using an IESS provides for one common translation mechanism that everyone builds to.

Block 3: Globally Unique Enterprise Identifiers (EID). An enterprise identifier guarantees a key that is unique enterprise-wide. The use of Enterprise IDs will ensure exact record-matching between heterogeneous databases even when the databases were designed independently. Establishing EIDs as the standard identifiers across the Army and DoD will improve battlespace resolution for Joint Task Force (JTF) commanders. EIDS will allow a horizontal interoperability (across Services) that does not currently exist.

Block 4: Extensible Markup Language (XML). XML is the proposed universal format for structured documents and data on the Web. It is intended to describe data, not to drive the way it is displayed by any given application. XML tags can be used to identify and display data/documents on divergent platforms in the way that best fits the platform's abilities and limitations. XML tags need to be based on standardized data for maximum reuse.

Upper Layers: Shared Data Environment (SDE). A shared data environment presumes a "Functioning System" is in place with a distribution infrastructure supporting information producers and consumers. This distribution infrastructure includes (1) Network-centric Applications; (2) External (e.g., Joint and Coalition) Interfaces; and (3) the Army Knowledge Online Portal. Operational data services require that interfaces be sustained. Overall performance may be related to four key performance parameters (KPPs): awareness, access, delivery, and services. Overall performance must be evaluated, with feedback to organization or installation operators, and to command functional proponents as appropriate.

- Continue support for data standards by enforcing the use of (1) vetted Authoritative Data Sources (ADSs) for all reference data needed for information exchange, (2) globally unique Enterprise Identifiers for key management within databases, (3) scoped, Community of Interest (COI)-driven Information Exchange Standards Specifications (IESSs), and (4) XML based information exchanges among all data stores, particularly, those targeted to support next-generation Network-Centric solutions.
- Develop policies and procedures for all four areas of the Army data standards strategy (i.e., ADS, EID, IESS and XML).

- Collect and maintain data resources developed in support of the Army data standards strategy and provide for their ready access via the Army Knowledge Portal.
- Establish pertinent working groups in each of the four areas of the Army data standards strategy.
- Assign via the Component Functional Data Administrator (CFDAd) appropriate responsibilities within the COIs or domains, (i.e., Operations & Plans, C3, Intelligence, Requirements & Programs, Manpower & Personnel, Readiness, Training, Logistics, Finance, Transportation, Medical, Acquisition, Legal, Installations, & Quality of Life/Morale, Welfare, and Recreation (MWR)).
- Coordinate Army data standards initiatives with those of Network Operations, Communications, Computing, and Enterprise.
- Ensure system managers implement data interoperability, as described in this section, in accordance with AR 25-1, the Software Blocking Policy and the Unit Set Field directive.

c. Specific Responsibilities

1) CIO/G-6

- Promulgate policies and procedures for all four areas of the Army data standards strategy.
- Oversee compliance with the Army Knowledge Enterprise Architecture and relevant architecture guidance documents.
- Oversee compliance with the JTA-A and DoD Metadata Repository requirements.
- Represent Army position on the four areas of the Army data standards strategy at Federal, DoD and Inter-Service level.

2) ASA(ALT) PEOs

- Ensure materiel developers comply with Army and DoD data standards requirements by developing a Program Data Administration Strategic Plan and a Program Data Performance Plan.
- Input Metadata into the DoD Metadata Repository NLT Sep 03.

3) MACOMs and Functional Proponents

- Identify functional data standards producers to carry out data management and standard actions for their respective organizations and serve as liaisons between functional experts and technical personnel.
- Work with the appropriate Resource Sponsors to identify funding requirements in support of data producers, for their functional area.
- Review the data structure of assigned data standards in the AKO at each milestone and at 5-year increments after system deployment.
- Input Metadata into the DoD Metadata Repository NLT Sep 03.

4) Point of Contact

- CIO/G-6 IOE

3.4.3. Remote Services

a. Desired End State

Consistent level of remote services to individuals to enable successfully performance of assigned mission within the protected Army intranet.

b. Actions

As the Army increasingly relies on individuals not located within an installation or Army facility boundary (e.g., ARNG, USAR, Army Recruiters, ROTC personnel, persons on travel, telecommuters), the need to provide quality remote access to the AEI has increased. In addition to remote dial-up services, this remote service calls for protected access across the Internet to the AEI through the AKO portal, thus extending the Army's defensive IT perimeter out to individuals where they are, and not just within an Army facility or installation.

The CIO/G-6 will rewrite the IM portions of AR 5-9 and work with the ACSIM to organize and facilitate the new Army remote IT services construct NLT 30 Jun 03. The rewrite will define all IT Remote Access and telecommuting service requirements to include but not be limited to: MACOMs, Accessions Command, Corps of Engineer, USAR, and ARNG requirements.

NETCOM/9th ASC will develop a common user remote access plan to include dial-in and protected access to the AEI via the Internet NLT 30 Jun 03 and be published in conjunction with the CIO/G-6 rewrite of portions of AR 5-9. NETCOM/9th ASC will develop a Remote Access Migration Plan (RAMP) for all

existing dial-up access points within the Army into the common-user access architecture NLT 1 Oct 03 with the migration to be complete NLT 30 Sep 06.

DOIMs, MACOMs and Functional Proponents that currently have dial-up access to portions of the Army infostructure or Army systems will identify all dial-up access points to NETCOM/9th ASC NLT 1 Jul 03 to ensure the functional requirements for remote access are fully accounted for in the RAMP.

c. Specific Responsibilities

1) CIO/G-6

- Establish policy for the remote services portion of the Army SLM program.
- Establish Integrated Process Teams(s) of Remote Service users to participate in the rewrite the IM portions of AR-5-9 to organize and facilitate the new Army remote IT services construct.

2) ACSIM

- Fund remote services portion of the C4IM baseline services.
- Review and incorporate the new Army remote IT services construct into AR 5-9.

3) NETCOM/9th ASC

- Develop a common user remote access plan to include dial-in and protected access to the AEI via the Internet.
- Develop, operate and manage the Army remote service management solution, within available resources, in conjunction with CIO/G-6.
- Manage and update the Army SLM program and process to reflect the addition of remote services.
- Develop and implement a regional C4IM mechanism for measuring the cost directly attributable to the customer to provide a given remote service.

4) MACOMs and Functional Proponents

- Identify all dial-up access points to NETCOM/9th ASC NLT 1 Jul 03

5) DOIM

- Develop and implement a garrison C4IM mechanism for measuring the cost directly attributable to the customer to provide a given remote service.
- Identify all dial-up access points to NETCOM/9th ASC NLT 1 Jul 03

6) Point of Contact

- CIO/G-6 IOM Division

3.4.4. CAC and PKI

a. Desired End State

Integrate the DoD PKI and CAC infostructure into all levels of the AEI and AKEA.

b. Actions

The Army Enterprise PKI refers to the architecture, organization, techniques, practices, and procedures that support the DoD CAC and PKI Implementation policy. PKI refers to the framework and services that provide for the generation, production, distribution, publication, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. The end-user token for individuals will be the CAC. The CAC will contain an integrated circuit chip (ICC) with a cryptographic coprocessor. The Army Enterprise PKI and CAC are enabling technologies that support the Army defense-in-depth security strategy. The PKI and CAC programs introduce enabling information assurance technologies that provide data protection for IT resources through strong authentication, non-repudiation, data confidentiality, and data integrity. The CAC/Smart Card readers that will be implemented as part of the AKEA will provide authentication of users to the AEI and AKO Enterprise portal. These technologies will also provide digital signatures and email encryption capabilities. PK-enabling of business applications and private web servers are critical components of the PKI program as they provide for the required security services in support of daily business operations. Mission Category 1 Applications and private web servers are required to be PK-enabled by 30 Sep 02 in accordance with OSD and DA guidance. Security services may include authentication, non-repudiation, and encryption (in-transit and in-storage). PK-enabling applications also involves the integration with application access controls to provide role-based access to business application information. As the DoD Biometrics Architecture is implemented, some biometric technologies (e.g., fingerprints) may be incorporated into the Army CAC. This coupling will provide additional assurance for identification and authentication (I&A) where required (e.g., for highly sensitive system or facility access). There are challenges that must be

addressed for this goal to succeed and the specific challenges will be addressed in the planning and coordination phases.

c. Specific Responsibilities

1) CIO/G-6

- Provide policy and oversight of PKI/CAC initiatives.
- Coordinate proposed Army PKI/CAC policies with appropriate HQDA staff.
- Prioritize applications for PK Enabling.
- Proponent for CAC/PKI initiatives.

2) ASA(ALT) PEOs and PM Secure Electronic Transactions – Devices (PM SET-D)

- Coordinate CAC/PKI fielding and training with DEERS/RAPIDS installation.
- Develop a phased implementation/fielding schedule that starts deploying CAC reader hardware in last QTR FY01 and continues until its completion date in last QTR FY03.
- Disseminate schedules, procedures, and responsibilities for fielding at each location.
- Implement directives.

3) MACOMs and Functional Proponents

- Disseminate schedules, procedures, and responsibilities for fielding at each location.
- Implement directives.

4) IMA

- Disseminate schedules, procedures, and responsibilities for fielding at each location.
- Implement directives.

5) NETCOM/9th ASC

- Develop policy for PKI/CAC initiatives.
- Monitor emerging and evolving threats to PKI/CAC.
- Acquire resources necessary to implement approved PKI/CAC policies and resulting security implementations, (i.e. encrypted email, digitally signed email).
- Implement approved PKI/CAC policies based upon allocated funding.
- Implement PKI/CAC in accordance with The Public Key Infostructure Implementation Plan for the Department of Defense, version 3.1, 18 Dec 2000.
- Ensure, in coordination with MACOMS, PEO, and DOIMS, that by the end of FY03, every soldier, selected reserve component personnel, civilian employee and onsite contractor in DA will have a CAC.

6) DOIMs/Tactical Units

- Implement directives.
- Provide feedback to NETCOM/9th ASC and PM-SET-D on CAC/PKI security initiatives.
- Implement local security capabilities in accordance with Army policy and posture.

7) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC ESTA Advanced Technology Integration Group and IA Division

3.4.5. Cryptographic (CRYPTO) Modernization Program

a. Desired End State

Crypto/Computer Security (COMSEC) technologies leveraged to provide multifunctional protection to the network-centric enterprise.

b. Actions

Implement the COMSEC modernization program throughout the Army. The DoD crypto inventory is 30 years old, technologically obsolete, rapidly losing its effectiveness to secure information links, and logistically unsupportable. The Army has 1.2 million crypto items that comprise over 40% of the DoD inventory. These stovepipe components operate point-to-point and are incapable of supporting the new network-centric AKEA architecture. The crypto modernization initiative leverages the latest technological advances to produce multi-functional components to replace a family of equipment. These components will employ a modular, programmable, and re-configurable design that facilitates future software and component upgrades. Many of these new technologies will require new methods of key delivery and management and the National Security Agency (NSA) Key Management Infrastructure (KMI) is integral to the success of the Army crypto modernization implementation.

An ASD(C3I) Memorandum, signed by Arthur Money, dated 23 February 2001 directed the following actions:

“The DoD must put into place a cohesive department wide initiative which includes the necessary fiscal and implementation planning for upgrades, replacements, and future cryptographic products to ensure our security posture does not continue to erode...”

The minimum capabilities that will be incorporated in the modular, programmable, multi-functional Crypto/COMSEC components include the following:

- Programmable, downloadable NSA approved Crypto/COMSEC algorithms.
- Embeddable (whenever possible).
- Scalable components (software components must be upgradeable).
- EKMS and KMI compliant.
- Network-centric.
- Interoperable with Legacy Components.

c. Specific Responsibilities

1) CIO/G-6

- Provide policy and oversight of Army Crypto/COMSEC and KMI modernization efforts.

2) G8

- Provide programmatic management and execution oversight.

3) ASA(ALT) PEO

- Develop a process that will ensure Crypto/COMSEC modernization efforts are linked to major programs and initiatives (WIN-T, Joint Tactical Radio System (JTRS), KMI, & FCS) and are in concert with Joint Cryptographic Modernization Capstone Requirement Document NLT 1 Dec 03.
- Implement Crypto/COMSEC modernization directives.
- Embed security features into all new material development and acquisitions.

4) AMC CECOM (CSLA) and RDECOM (CERDEC)

- Develop COMSEC equipment shortage and supportability lists NLT 1 Dec 03.
- Prepare fielding plans and coordinate fielding plans with ASC Ft Gordon, NLT 1 Dec 04.
- Prepare transition plans and coordinate transition plans with ASC Ft Gordon NLT 1 Dec 04.
- Coordinate with NSA to ensure all Army Crypto acquisitions receive NSA Crypto Certification and Approval.
- AMC RDECOM will conduct technical reviews, new technology concept exploration, and proof of concept testing as required in support of Crypto/COMSEC modernization.

5) TRADOC SIGCEN

- Develop Army COMSEC operational requirements documentation NLT 1 Dec 03.

6) MACOMs and Functional Proponents

- Implement Crypto/COMSEC modernization directives.

7) NETCOM/9th ASC

- Integrate crypto modernization into policy and plans.
- Ensure AKEA implemented crypto technologies are interoperable with external interfaces to DoD Agencies and other Services as required.
- Coordinate with CSLA to provide implementation directives.

8) IMA

- Implement Crypto/COMSEC modernization directives.

9) DOIM/Tactical Units

- Implement Crypto/COMSEC modernization directives.

10) Points of Contact

- CIO/G-6 BMO
- NETCOM/9th ASC ESTA IA Division

3.4.6. Biometric Technologies

- a. Biometric technology integrated into AEI to protect the enterprise.

Integrate Biometric Technology in the Army Enterprise Infostructure and for high and medium assurance applications.

- b. Actions

Biometrics will be used, in conjunction with other I&A technologies, to provide increased levels of assurance. Biometrics are an empowering technology that ensures the right person with the right privileges is provided timely access to secure systems and facilities in support of warfighter dominance.

The Army is the executive agent for the DoD Biometrics Management Office (DoD BMO). The BMO will lead, consolidate, and coordinate the development, adoption, and institutionalization of biometric technologies in combatant commands, services, and agencies to enhance Joint Service interoperability and warfighter operational effectiveness. (The integration of Biometric technologies

into the AEI where strong I&A are required will support this mission. Biometrics is one of the I&A supporting architecture components of the Army defense in depth strategy that will provide information superiority and protect the Army portion of the GIG by protecting vital information.

c. Specific Responsibilities

1) CIO/G-6

- Provide policy and oversight.
- Provide Budget planning and support.
- Capture, analyze, and document Army Biometrics requirements.
- Provide Army Biometrics requirements to TRADOC for incorporation into MNSs and ORDs.
- Ensure that the Army Biometrics program is coordinated with other DoD Agencies, Services, and non-DoD agencies to address interoperability issues as part of program planning and development.
- Manage the DoD Biometrics program and insure that the acquisition of biometrics technologies and supporting infostructure components by the PEO supports the DoD requirements.

2) G3

- Direct TRADOC to incorporate Biometrics I&A requirements in Army systems' MNS and ORDs NLT 1 Dec 03.

3) ASA(ALT) PEO EIS

- Execute the acquisition of biometrics technologies and supporting infostructure components.
- Develop Biometrics Integration Plans NLT 1 Oct 04.
- Develop Biometrics Fielding plans NLT 1 Oct 04.
- Complete initial fielding of test biometrics devices NLT 1 Mar 04.
- Complete full operational biometrics capability NLT 1 Mar 05.

4) ASA(ALT) PEOs

- Implement directives.

5) IMA

- Implement directives.

6) TRADOC

- Incorporate Biometrics I&A requirements in Army systems MNS, and ORDs at the direction of the G3 NLT 1 Dec 03.

7) MACOMs and Functional Proponents

- Implement directives.

8) NETCOM/9th ASC

- Ensure the Army Biometrics architecture and technologies are incorporated and compatible with the AKEA NETOPS architecture.
- Provide implementation directives.
- Monitor emerging and evolving threats to biometrics.

9) DOIM/Tactical Units

- Implement directives.
- Manage, support, and maintain biometric devices and systems where implemented in the AKEA (ongoing).

10) Points of Contact

- CIO/G-6 BMO
- NETCOM/9th SC ESTA IA Division

3.5. MISSION FIVE – MOVE TO PERFORMANCE-BASED ENTERPRISE SERVICE APPROACH

3.5.1. Baseline Services and Service Level Management

a. Desired End State

The Army centrally funds, manages, and provides a core base level of service as identified by the CIO/G-6 and validated by the ACSIM and manages processes to provide unique mission or above baseline support on a reimbursable basis.

b. Actions

A consistent base level of infostructure services will be provided to all authorized Army users at the least cost feasible within Army operational constraints. An objective set of baseline services, with performance metrics, will be defined, based on approved AEI requirements. Five service areas are included: communications systems and systems support (including voice and data networks); visual information processes (including graphic art and imagery); document management (records management); information assurance (including communications security and computer security); and automation (data services and applications including email). However, Records Management is transitioning to the garrison AG as described in Part 2, paragraph 1.2. The objective is to have the DOIM responsible for the delivery of these services, within performance metrics, to the installation. Periodic surveys will be used to measure customer satisfaction with delivery of services.

NETCOM/9th ASC will analyze current services provided relative to the objective baseline, together with their costs and funding streams. NETCOM/9th ASC will develop a Service Level Management (SLM) plan to address the transition to standard baseline services, their costs, and the required realignment of funding streams.

SLM is the disciplined, proactive methodology and procedures used to ensure that adequate levels of service are delivered to all C4IM users in accordance with Army priorities at an acceptable cost. Service levels typically are defined end-to-end from a customer perspective in terms of the availability, responsiveness, integrity, and security delivered to the users of the service. NETCOM/9th ASC will create an automated service management environment to measure and report service delivery. By maintaining a core-funded baseline, the Army will implement a modified industry best practice SLM approach, where commercial industry typically implements a totally reimbursable concept.

Baseline service is the methodology under which standard services will be provided. This methodology is rooted in the tenet that every customer requires a consistent, funded level of base services to perform the standard range of Army

missions. This methodology also supports the IMA leadership intent to: eliminate the migration of installation support dollars; achieve regional efficiencies; and provide consistent and equitable services via standards. The CIO/G-6 and NETCOM/9th ASC, in coordination with IMA and the DOIMs, will develop common C4IM service requirements, identify baseline services, establish baseline service delivery levels, and coordinate baseline service delivery funding requirements with the ACSIM, and other Army business lines. Commanders will determine the correct mix of IT services and other mission requirements against their available mission resources and request above baseline service delivery on a reimbursable basis. Both parties will negotiate SLA for enhanced service requirements above the established service delivery baseline.

NETCOM/9th ASC will develop and implement an Army performance based SLM program for common C4IM services. Detailed information will be published in the AEI SLM program implementing instructions NLT 1 Jun 03.

NETCOM/9th ASC will submit recommended baseline service implementation and fulfillment plan to the AEIMSG for validation and to the Army CIO EB for approval. Until a common level of C4IM baseline services can be achieved technically and financially, the Army may establish multiple baselines driven by existing technical capabilities and available funding. It is neither the intention of the CIO/G-6 nor NETCOM/9th ASC to diminish existing service levels during the transformation to a service-based management approach.

NETCOM/9th ASC will monitor, measure, manage, and report performance for all baseline and above services on an AKO knowledge center. The SLM web site, developed NETCOM/9th ASC and accessed on AKO, will provide access to:

- Army baseline service level information.
- Army baseline service level performance reports.
- Customer and business line SLA information for above baseline services.
- Customer and business line SLA performance reports for above baseline services.

c. Specific Responsibilities

1) CIO/G-6

- Establish policy for the Army SLM program.
- Identify the baseline services.
- Provide Baseline Service Implementation to AEIMSG for validation.

- Provide Baseline Service Implementation to CIO EB for approval.
- 2) ACSIM
- Fund the C4IM baseline services.
- 3) IMA
- Manage distribution of funds for the C4IM baseline services.
 - Develop and manage Enterprise Regional Activity Based Costing and Management models.
- 4) NETCOM/9th ASC
- Develop and maintain the SLM web site on AKO portal.
 - Develop the Army baseline service implementation plan and submit the service baseline to the AEIMSG for validation and the Army CIO Executive Board for approval.
 - In conjunction with DOIMs, define the operational requirements for the DOIM Budget.
 - Manage and update the Army SLM program and process.
 - Review/update C4IM service requirements based on available resources, enhanced customer expectations, service performance. Develop data analyses of the enterprise baseline services, unique enterprise SLA extensions to baseline service costs, and track cost of business management, to include the incremental cost of doing ABC/M.
 - Identify new technology and services requiring SLM.
 - Approve regional extensions to SLAs.
 - Periodically review/update regional SLA extensions to baseline service levels.
 - Coordinate service performance measurement for regional baseline services and unique regional SLA extensions to baseline service levels.
 - Negotiate and sign unique SLA extensions to baseline services that have an enterprise impact or cross regional boundaries.

- Monitor/review service performance measurement for enterprise baseline services and SLA extensions to baseline service levels.
 - Approve unique garrison SLA extensions to baseline service levels.
 - Recommend improvements to the Army SLM program to achieve agreement on established baseline service levels and SLA extensions to baseline service levels and monitoring of an optimal level of C4IM service, at a justifiable cost.
 - Develop baseline and reimbursable cost reporting guidance. Identify and track the Army reimbursement policy for enterprise SLAs.
 - Identify service requirements; negotiate and sign SLAs with other Federal Government service providers, e.g., DISA.
 - Negotiate enterprise service provider to service provider SLAs, e.g., local direct contracting, Army-wide touch labor, 1-800-Army AKM.
- 5) Garrison Commander
- Ensure resource transfers for server consolidation are provided to the DOIM.
- 6) DOIM
- Manage the garrison SLM Program.
 - Negotiate and sign SLA with tenant customer s for services above the baseline.
 - Provide input into the garrison ABC/M model as a C4IM mechanism for measuring the costs directly attributable to the customer to provide a given service. Provide to NETCOM/9th ASC RCIOs the ABC/M data for inclusion into the Enterprise and Regional ABC/M model for data analyses. Track cost of business management.
 - Develop and implement a garrison C4IM mechanism for measuring the cost directly attributable to the customer to provide a given service.
 - Propose changes to C4IM service requirements based on available resources, enhanced customer expectations, service performance, and a periodic financial analysis of service levels and costs.

- Propose new technology and services requiring SLM.
- Coordinate garrison extensions to baseline service levels.
- Periodically review/update garrison SLAs extensions to baseline service levels.
- Monitor/coordinate service performance measurement for garrison baseline services and unique garrison SLA extensions to baseline service levels.
- Recommend improvements to the Army Service Management system to achieve agreement on established baseline service levels and SLA extensions to baseline service levels and monitoring of an optimal level of C4IM service, at a justifiable cost. Provide reports to RCIO, as required.
- Prepare Unfunded Requirements (UFR)/POM documentation, etc, as appropriate to upgrade/maintain the infostructure.
- Document resources required to support consolidated server operations.
- Provide resource documentation for resource transfers and investment analyses.
- Accept full-time system administrators under operational control upon signature of the tenant SLAs.
- Accept manpower in accordance with TDA changes or funding if no manpower.

7) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC ESTA SLM

3.5.2. Enterprise Support Center

a. Desired End State

A tightly integrated support center providing support to the customers.

b. Actions

An Enterprise Support Center (ESC) which provides help desk support, diagnostics, and resolution for all C4IM-related issues and coalesces the ESC, the TNOSCs, PEO, MACOM, functional proponents, industry partners, and the local support dispatch center to form a tightly integrated web of support to the customer (see Figure 2.3-4).

NETCOM/9th ASC will establish an ESC, to accept trouble calls from users across the entire AEI. Empowered by technology, the ESC may be formed from de-centralized Help Desks from the AEI players (Installations, Army Reserve, Army National Guard, et al), or it may be formed as a new in-house activity, or out-sourced, or any combination of the above. Regardless of its structure, the ESC will serve as a central receiving point, tracking and reporting, and diagnostic center for all AEI issues. Trouble tickets from the user will be received in and logged into a database tracking system. Once diagnosed, the trouble ticket will be transferred to one or more of the ESC partners for resolution, customer feedback and interface, and documentation as illustrated in Figure 2.3-5, CALL Flow Diagram.

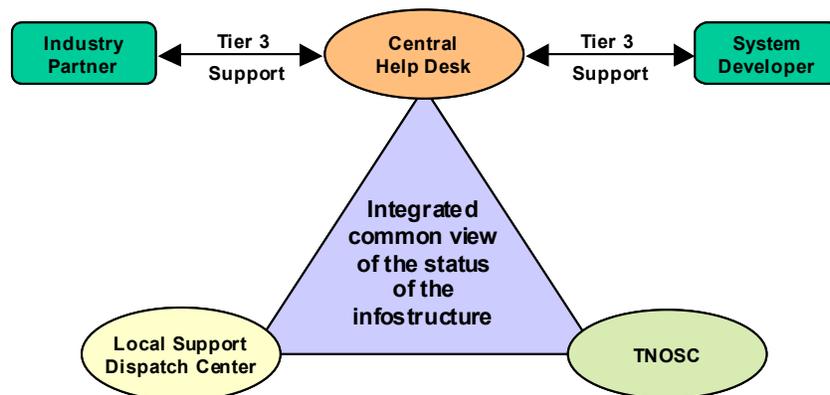


Figure 2.3-4. Enterprise Support Center

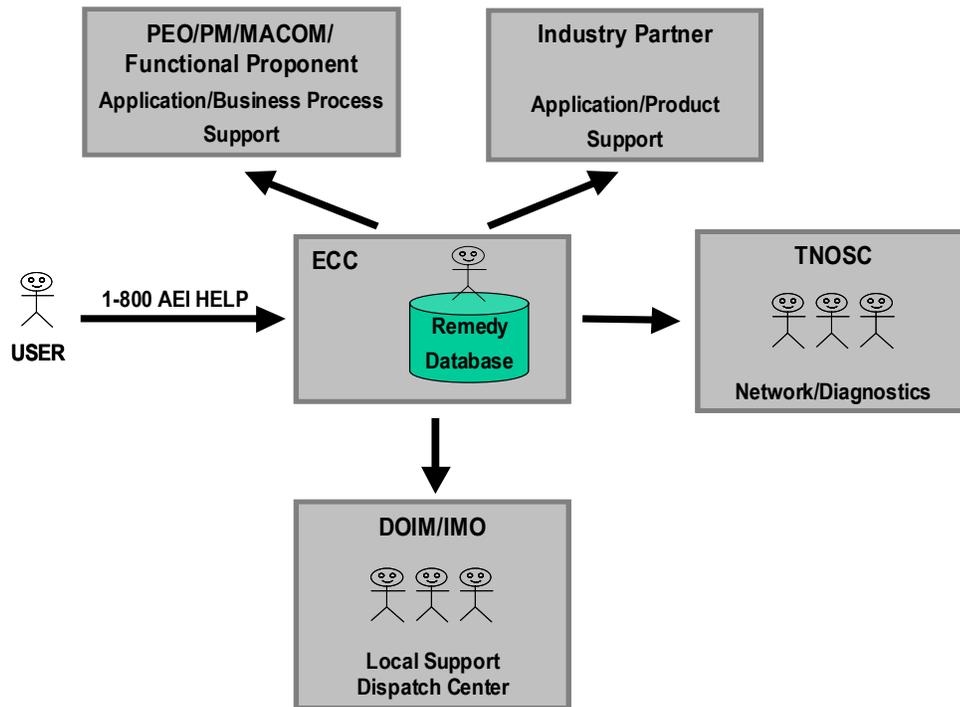


Figure 2.3-5. CALL Flow Diagram

To implement this ESC, NETCOM/9th ASC will leverage the MDW PoC demonstration of a pseudo ESC to develop an ESC architecture and supporting workflow processes. NLT 1 Jun 03, NETCOM/9th ASC will develop an ESC Concept Plan and initial architecture (OV1 – OV3). These initial ESC architecture views will be incorporated into the overall NETOPS architecture required in support of the AKEA effort described in Part 1, paragraph 2.0 of this plan. In addition, NETCOM/9th ASC will develop ESC functional requirements for use by PEO EIS in implementing this capability for the Army NLT 1 Jul 03.

c. Specific Responsibilities

1) CIO/G-6

- Publish policy for centralized tracking and resolution of all AEI trouble tickets.
- Ensure resources are available for implementation of the ESC concept.

2) ASA(ALT) PEO EIS

- Implement ESC concept and functional requirements as defined by NETCOM/9th ASC NLT 1 Aug 03.

3) NETCOM/9th ASC

- Establish an ESC, empowered with appropriate tools and processes, for reception, tracking, reporting, diagnostics, and escalation of all AEI trouble tickets.
- Develop ESC Concept Plan NLT 1 Jun 03.
- Develop operational views (OV1 – OV3) for ESC NLT 1 Jun 03.
- Develop ESC functional requirements NLT 1 Oct 03.
- Monitor ESC trouble ticket reporting to identify trouble trends, and identify systemic solutions.

4) DOIM

- Staff and operate local support dispatch center (Help Desk) to provide customer relation and feedback, and touch labor problem resolution.

5) Tenant IMO

- Staff and operate application-specific support cells (Tier III Help Desk) to provide application problem resolution, and business process assistance.

6) Points of Contact

- CIO/G-6 IOM
- NETCOM/9th ASC ESTA Governance & NETOPS Directorate

4.0 GOAL 4 – INSTITUTIONALIZE ARMY KNOWLEDGE ONLINE

In order to effectively use AKO, Army leaders and AKO customers need to be informed of current/planned AKO capabilities and how these capabilities can support accomplishment of their mission and functions. With an understanding of current and planned AKO capabilities Army leaders will be able to leverage those capabilities to achieve mission success.

AKO will be institutionalized when there is Army-wide routine utilization of AKO capabilities to optimize accomplishment of the Army's many varied missions and functions. This section outlines the actions required to move the Army toward this goal and to realize the potential value of AKO Portal.

4.1. SCALE AKO AND AKO-S

a. Desired End State

99.99% reliable; "big enough, fast enough, and available."

b. Actions

Institutionalization of the AKO portal will occur when its capabilities are utilized to the maximum practical extent possible to achieve a majority of Army end-to-end missions and functions. This requires that AKO capabilities be first understood and then integrated by Army leaders and their functionals into their organization's routine and ad-hoc operations.

- Understand the Capabilities AKO Offers
- Develop and implement a continuous operation capability.
- Be informed of current/planned AKO capabilities and how they support accomplishment of missions and functions.
- Manage AKO Usage within their Functional Domain.

c. Specific Responsibilities

1) All Army Organizations

- Identify organization personnel that are required to have an AKO/AKO-S (FY03 – 4th Quarter).

2) NETCOM/9th ASC

- Implement a continuous operation (COOP/Disaster Recovery Site) NLT 1 Oct 03.
- Implement AKO functional requirements identified and endorsed by the AKO CCB NLT 1 Oct 03.
- Implement a Configuration Management Lab NLT 1 Oct 05.
- Implement a Separate Systems Development and Operations Environment NLT 1 Oct 05.

3) Point of Contact

- NETCOM/9th ASC/CTO

4.2. LEVERAGE AKO

a. Desired End State

Functionals maximum use of the Enterprise portal for mission success.

b. Actions

Establish methods to engage the Functionals: CIO AKM Task Force Concept, the AKO Configuration Control Board (CCB), the annual Army Knowledge Symposium, and targeted partnering agreements between the CIO and functional domains.

c. Specific Responsibilities

1) CIO/G-6

- Establish and manage an AKM Task Force to assess and govern AKM initiatives across the Enterprise NLT 1 Oct 03.
- Plan, coordinate and host the Army Knowledge Symposium NLT 1 Oct 03.
- Plan, coordinate and host the AKO CCB, quarterly NLT 1 Oct 03.
- Develop partnerships with the Functionals and the tactical agencies and assist them in migrating current systems to AKO, while simultaneously re-engineering their business process to take advantage of IT/AKM principles NLT 1 Oct 03.

2) MACOMs and Functional Proponents

- Identify and present functional requirements to the AKO CCB for vetting and approval NLT 1 Oct 03.

3) Point of Contact

- CIO/G-6 EIK

4.3. SELF-SERVICE CENTER FOR NETWORKED KNOWLEDGE MANAGEMENT

a. Desired End State

Leverage Intellectual Capital to better organize, train, equip, and maintain the Objective Force.

b. Actions

Develop detailed comprehensive policies and guidelines that guide the daily operation of the Army's intranet/portal efforts.

Develop an AKO comprehensive style guide.

c. Specific Responsibilities

1) CIO/G-6

- Ensure the development of an AKO comprehensive style guide NLT 1 Oct 03.
- Develop detailed comprehensive portal policies and guidelines NLT 1 Oct 03.

2) NETCOM/9th ASC

- POM and manage the infrastructure to alleviate potential bandwidth shortcomings NLT 1 Oct 03.
- Assess and identify potential bandwidth bottlenecks NLT 1 Oct 03.
- Implement the AKO Style Guide NLT 1 Oct 04.

3) MACOMs and Functional Proponents

- Examine current processes in light of existing technologies and reengineer processes for the portal environment NLT 1 Oct 03.
- Adhere to the approved AKO templates and style guides NLT 1 Oct 04.

4) Point of Contact

- CIO/G-6 EIK

4.4. STRATEGIC READINESS SYSTEM (SRS) SCORECARD

a. Desired End State

Expand AKO capabilities to the Functional Domains through targeted efforts.

b. Actions

Explore new technologies to enhance the portal capability based on user requirements.

Expand existing capabilities and work-in-progress.

Reduce duplication.

c. Specific Responsibilities

1) CIO/G-6

- Facilitate the expansion of AKO capabilities to the functional domains through targeted efforts NLT 1 Oct 03.

2) MACOMs and Functional Proponents

- Identify and define specific requirements for functional groups and communities of practice, and build them into the implementation plans and the POM NLT 1 Oct 03.
- Validate incoming requirements against existing portal capabilities NLT 1 Oct 03.

3) NETCOM/9th ASC

- Publish portal baseline and capabilities NLT 1 Oct 03.

4) Point of Contact

- CIO/G-6 EIK

4.5. REQUIREMENT AND CONFIGURATION MANAGEMENT BUSINESS PROCESS

a. Desired End State

AKO capability driven by user requirements.

b. Actions

AKO functional and technical requirements drive AKO capability development and upgrades. Management of these potentially numerous and complex requirements is necessary to ensure their correct and complete implementation and ultimately to ensure AKO user needs are met. Key Requirements Management functions include:

- Outreach to all AKO users.
- Requirement Traceability.
- Requirement Implementation Verification.
- Requirement Quality Verification.
- Requirement Impact Analysis.
- AKO Development Oversight and Control.

An AKO requirements management plan will be developed and promulgated across the Army through the AKO CCB for all AKO functional requirements baselined by the AKO CCB. To ensure effectiveness of AKO requirements management it will be integrated with two other key management processes, AKO IT systems development and configuration management.

c. Specific Responsibilities

1) CIO/G-6

- Generate an AKM Requirements Management Plan NLT 1 Oct 03.
- Oversee implementation of the AKO requirements management plan to ensure all functional requirements baselined by the AKO CCB are fully implemented in appropriate functional plans and by AKO technical capabilities developed by NETCOM/9th ASC NLT 1 Oct 03.

2) NETCOM/9th ASC

- Perform technical requirements management to ensure functional requirements are implemented by technical requirements, designs, end products, test plans, and operation and maintenance documentation NLT 1 Oct 03.
- Incorporate technical requirements management into AKO development, configuration management NLT 1 Oct 03.

3) Point of Contact

- CIO/G-6 EIK

4.6. CONFIGURATION MANAGEMENT

a. Desired End State

A consolidated configuration management process for AKO capabilities.

b. Actions

Configuration Management ensures appropriate review, approval, security, and coordination of AKO configuration items during their development, deployment and maintenance. The quality of AKO configuration items and their interoperability will directly impact the quality of service provided to users. Management of AKO configuration items must be jointly performed by functional and technical organizations that share responsibility for planning and implementing AKO capabilities.

An integrated AKO CCB and NETCOM/9th ASC configuration management process will be developed and implemented to ensure AKO capabilities meet user expectations and needs as defined in the functional and technical baselines.

c. Specific Responsibilities

1) NETCOM/9th ASC

- Produce, maintain, and promulgate a NETCOM/9th ASC AKO Configuration Management Plan that supports the AKO Requirements Management process NLT 1 Oct 03.

2) Point of Contact

- NETCOM/9th ASC

4.7. INFORMATION RETRIEVAL AND KNOWLEDGE DISCOVERY

a. Desired End State

A refreshed and sustained enterprise and functional level taxonomy based on the Objective Force IDM requirements.

b. Actions.

Taxonomy is focused on cataloging, structuring, classifying and categorizing unstructured and structured content to support efficient and effective knowledge

information delivery and management to the warfighter/tactical staff elements. Taxonomy establishes vertical and horizontal relationships between content elements to facilitate finding content, analyzing it, organizing it, codifying it, identifying points of contact to communicate with, and content implementation (situational awareness, decisions, reports, messages, etc.).

An effective enterprise and functional community level taxonomy will be developed, baselined, implemented, and maintained for all AKO content and applications requiring precise, relevant information capture.

c. Specific Responsibilities

1) CIO/G-6

- Produce an Enterprise Information Delivery Model and strategic plan and submit it to the AKO CCB NLT 1 Oct 03.

2) NETCOM/9th ASC

- CTO identify, define, and implement taxonomy technical requirements NLT 1 Oct 03.
- Perform technical and cost analysis of the functional communities taxonomy requirements NLT 1 Oct 03.
- Implement and integrate taxonomy across the Enterprise NLT 1 Oct 04.

3) All Army Organizations

- Identify mission and functional domain related taxonomy requirements and provide this information to the AKO CCB for approval and implementation NLT 1 Oct 04.

4) Point of Contact

- CIO/G-6 EIK

4.8. CONTENT LIFECYCLE MANAGEMENT

a. Desired End State

Appropriate, accurate, and timely content on AKO.

b. Actions

AKO content includes information published on all Army-owned web sites reachable through the portal. Content Management ensures that only valid, appropriate, practical, and timely information is accessible via the AKO portal to the user community.

AKO content meets user expectations and needs for every Army mission and functional domain.

c. Specific Responsibilities

1) CIO/G-6

- Produce, maintain, baseline, and promulgate an AKO Content Management plan for the Functional Domains NLT 1 Oct 03.
- Oversee, through the AKO CCB, the management of content identification, development, and publishing via the AKO portal NLT 1 Oct 03.

2) All Army Organizations

- Comply with content management life cycle guidelines NLT 1 Oct 04.

3) Point of Contact

- CIO/G-6 EIK

4.9. DYNAMIC FEEDBACK MECHANISMS

a. Desired End State

Instantaneous feedback mechanisms and metrics.

b. Actions

Identify the portal baseline for measurement.

Report critical metrics and measures to the AKO functional communities.

Continue process improvements.

Develop feedback mechanisms for community and content managers so AKO customers can directly interface with content providers.

c. Specific Responsibilities

1) CIO/G-6

- Build feedback mechanisms into the content and requirement management process NLT 1 Oct 03.
- Establish and provide oversight of the AKO Metrics Working Group NLT 1 Oct 03.

2) NETCOM/9th ASC

- Ensure that feedback mechanisms and measures are in place to support the Enterprise and assist in determining strengths and weaknesses of the portal NLT 1 Oct 03.

3) Points of Contact

- CIO/G-6 EIK
- NETCOM/9th ASC/CTO

5.0 GOAL 5 – HARNESS HUMAN CAPITAL FOR THE KNOWLEDGE-BASED ORGANIZATION

5.1. THIRD WAVE AKE ORGANIZATIONAL DESIGN PLAN

a. Desired End State

Empowered workforce effectively blending military, civilian, and industry partners to support AKE and enabling the Army to optimize resourcing of non-core functions.

b. Actions

Create a flexible functional structure model for all levels, identifying core and non-core functions, which will blend the military, civilian and industry partners into a combined workforce. This structure will be in compliance with the Non-Core Competencies Working Group (NCCWG) and complement the Objective Force Units of Employment and Unit of Action force structure to create the Army C4IM organizational structure.

The CIO/G-6 will produce an AKE organizational design plan to meet SecArmy memorandum, subject: NCCWG and The Third Wave, 4 Oct 02 tasking. This plan will:

- Develop exemption requests in coordination with ASA for Manpower, Resources, and Accounting (M&RA) NLT 29 Nov 02. (Completed).
- Determine whether civilian and contractor non-core functions should be:
 - Privatized.
 - Divested.
 - Outsourced.
 - Transferred to another Federal Agency.
- Determine whether non-exempted military spaces should be:
 - Converted to civilian.
 - Contracted.
- Provide an implementation plan to enact decisions and provide to NCCWG NLT 17 Feb 03. (Completed).
- SECARMY approval of implementation plans NLT 22 Mar 03. (Completed).
- Implement the plan on approval.

This should to be a complementary study to the tactical force structure study and should also be tied to the objective force requirements.

c. Specific Responsibilities

1) CIO/G-6

- In accordance with GO #3 paragraph 12 (K) will develop and implement a C4IM human capital strategy and programs.
- Provide written exemptions as appropriate.
- Direct the plan.

2) MACOMs and Functional Proponents

- Assist CIO/G-6 with plan.

- 3) IMA
 - Assist CIO/G-6 with plan.
- 4) NETCOM/9th ASC
 - Assist CIO/G-6 with plan.
- 5) DOIM
 - Assist CIO/G-6 with plan.
- 6) Points of Contact
 - CIO/G-6 RI
 - NETCOM/9th ASC G8

5.2. HUMAN RESOURCES PLANNING

a. Desired End State

Recruit and retain a quality workforce and plan for succession to meet future requirements.

b. Actions

In accordance with GO #3 paragraph 12 (K), develop and implement a C4IM human capital strategy and programs. The strategy will include initiatives designed to enhance recruiting and retention of the C4IM workforce, mechanisms to monitor and ensure development of future IT Job Series, a blueprint for an enhanced intern program, and a mandate to investigate regulatory and/or legislative changes to improve the Army's ability to attract and retain world-class C4IM professionals. Initial Strategy will be presented to the CIO/G-6 for review NLT 1 Dec 03.

c. Specific Responsibilities

- 1) CIO/G-6
 - In accordance with GO #3 paragraph 12 (K) will develop and implement a C4IM human capital strategy and programs NLT 1 Dec 03.
 - Partner with the G1, General Counsel, and Office of Legislative Liaison to investigate making changes to C4IM workforce regulations and laws.

- Develop and maintain a portal on AKO to make Army an employer of choice for C4IM.

2) NETCOM/9th ASC

- In coordination with CIO/G-6, request funding for C4IM workforce initiatives (recruiting bonuses, retention allowances, etc.) through the POM process.
- Conduct periodic surveys across regions to determine if workplace flexibilities (compressed work schedules, telecommuting) are in place where appropriate and resourced to ensure continued effectiveness of the C4IM workforce.

3) MACOMs and Functional Proponents

- Conduct periodic surveys across regions to determine if workplace flexibilities (compressed work schedules, telecommuting) are in place where appropriate and resourced to ensure continued effectiveness of the C4IM workforce.
- Conduct periodic C4IM workforce readiness assessments to ensure that the workforce possesses the requisite skill sets to accomplish its mission. Ensure adequate funds are programmed and available for training and professional development.

4) DOIM

- Conduct periodic C4IM workforce readiness assessments to ensure that the workforce possesses the requisite skill sets to accomplish its mission. Ensure adequate funds are programmed and available for training and professional development.
- Will forward consolidated list of training requirements/long-term and short-term to the RCIO.

5) Point of Contact

- CIO/G-6 EIH

5.3. PROFESSIONALIZATION OF THE C4IM WORKFORCE

a. Desired End State

Knowledge workers are immersed in an environment that fosters lifelong learning.

b. Actions

The CIO/G-6 supports the President's Management Agenda and the tenets of Management Initiative Decision (MID) 905 through effective workforce planning, cutting-edge recruitment and retention initiatives, broad-based education and training, and cross-functional professional development opportunities. In conjunction with the G-1, the CIO/G-6 partners with Federal, Defense, Army, and private sector educational sources to provide Soldiers and DA Civilians with the technical and managerial C4IM education needed to Transform the Army to a network-centric, knowledge-based force.

The CIO/G-6 will develop and implement a comprehensive human resource development program for the C4IM workforce, leveraging existing institutional relationships and building new ones, to provide education, training, and professional development opportunities aligned to the Clinger-Cohen CIO competencies, Knowledge Management (KM) practices, project management, and the Office of Personnel Management (OPM) Executive Core Qualifications for leadership. The program will also include a summary of all applicable laws and regulations on training for military, civilian, and contractor personnel, and an estimated training budget. In addition, the program will be aligned with the DoD CIO's effort to examine and assess IT education and training requirements for personnel engaged in the management and oversight of IT projects and acquisitions, scheduled for release in July 2003. Initial Army plan will be presented to the CIO/G-6 NLT 1 Nov 03.

c. Specific Responsibilities

1) CIO/G-6

- In accordance with GO #3 paragraph 12 (K) will develop and implement a C4IM human capital strategy and programs.
- Seek funding for C4IM workforce development through the POM process.
- Develop an Army plan NLT 1 Nov 03, to align Army programs with DoD CIO Education and Training Plan.

2) NETCOM/9th ASC

- Promote centrally-funded education, training, and professional development opportunities to the C4IM workforce.
- Consolidate and prioritize applications for education, training, and professional development opportunities.

- Develop C4IM workforce performance measures for installations in each region.
- Forward to CIO/G-6 the consolidated list of training requirements, long-term and short-term, from the DOIMs and RCIOs.
- Analyze opportunities for possible on-site training.

3) DOIM

- Develop partnerships with local colleges, universities, trade schools, and other educational organizations to influence the development of a C4IM curriculum aligned to their organizational needs.
- Senior Leadership of DOIMs should be CIO certified from the National Defense University or comparable institution.
- In addition to formal training, will promote cross training opportunities.
- Will promote and support educational opportunities.

4) Point of Contact

- CIO/G-6 EIH

5.4. INSTITUTIONALIZE AKE IN ARMY SCHOOLHOUSES AND SENIOR LEVEL SCHOOLS

a. Desired End State

Every soldier and civilian of every component, new recruit through senior leader, knows how his or her functional discipline fits into the Army Knowledge Enterprise.

b. Actions

Ensure that Military Occupational Specialty (MOS)-producing schools and Army's senior service schools embrace the AKE concept and integrate it into their respective schools' curricula. Preliminary implementation strategy will be presented to the CIO/G-6 NLT 1 Aug 03.

c. Specific Responsibilities

1) CIO/G-6

- In conjunction with TRADOC and the G1, develop a strategy for integrating AKE into every Army school.
- Coordinate with TRADOC and the G1 to determine the order in which Army schools will have their curriculum revised to encompass the AKE.
- In conjunction with functionals, review Program of Instruction (POI) of all Army schools in their respective regions, to ensure full integration of AKE content.
- Coordinate with TRADOC and the G1 to set up Pilot Programs at Army schools in their respective regions.

2) Point of Contact

- CIO/G-6 EIH

5.5. UTILIZATION OF INFORMATION OPERATIONS ASSETS

a. Desired End State

ARNG and USAR Information Operations units train in CND and network reconnaissance capabilities in conjunction with NETCOM/9th ASC TNOSCs and the associated Computer Emergency Response Team (CERT) operations.

b. Actions

The USAR and ARNG will identify units with appropriate Information Operations and NETOPS capabilities to work with NETCOM/9th ASC and the NETCOM/9th ASC TNOSC facilities. These units will be under the Command and Control of the appropriate State Adjutant General or the USAR, but TECHCON to NETCOM/9th ASC for Information Assurance missions unless and until mobilized. In addition, the USAR and ARNG will designate a training coordination officer to ensure that designated units are trained in accordance with Program of Instruction (POI) developed by NETCOM. The ARNG and USAR will allocate or program sufficient resources to ensure this occurs starting Oct 03. NETCOM/9th ASC will identify a ARNG/USAR coordinating officer within each TNOSC facility in addition to the Reserve Coordination Officer within the NETCOM/9th ASC G3. Furthermore, it is expected that the designated ARNG and USAR units that cannot conduct weekend training with a TNOSC will coordinate their weekend training activities with their assigned TNOSC facility to ensure that their weekend

training supports the overall Army NETOPS mission to the maximum extent possible.

Each TSC will designate two operations officers to NETCOM/9th ASC to coordinate all training activities of the TSCs with special emphasis on utilization of TSC assets of NETCOM/9th ASC ANOSC and TNOSC operations.

Specified USAR and ARNG Information Operations units will receive hands-on training in CND and network reconnaissance capabilities in conjunction with NETCOM/9th ASC TNOSCs and associated CERT operations, beginning NLT than 1 Oct 03.

c. Specific Responsibilities

1) CIO/G-6

- Ensure training is in compliance with C4IM Human Capital strategy.

2) NETCOM/9th ASC

- Coordinate with USAR and ARNG to schedule training at the TNOSC and CERT.

3) USAR/ARNG

- Coordinate with NETCOM/9th ASC to schedule training at the TNOSC and CERT.
- Ensure that units sent to TNOSC and CERT have obtained level 3 systems administrator and CND training.

4) Points of Contact

- CIO/G-6 EIH
- NETCOM/9th ASC IA

Appendix A: Acronyms and General Abbreviations

AAA	Army Audit Agency
AAIC	Army Architecture Integration Cell
AARMS	Army Architecture Management System
AASA	Administrative Assistant to the Secretary of the Army
ABC/M	Activity Based Costing/Management
ABIC	Army Business Initiatives Council
ABO	Army Budget Office
AC	Active Component
ACA	Army Contracting Agency
ACE	Advanced Collaborative Environment
ACERT	Army Computer Emergency Response Team
ACSIM	Assistant Chief of Staff for Installation Management
AD	Active Directory
ADS	Authoritative Data Sources
AEI	Army Enterprise Infostructure
AEI-MF	AEI Mission and Functions
AEIMSG	AEI Management Steering Group
AEIOO	Army Enterprise Integration Oversight Office
AEI-R	AEI - Repository
AEI-T	AEI - Transport
AFM	Army Flow Model
AG	Adjutant General
AHRS	Army Human Resource Systems
AIS	Automated Information Systems
AITR	Army Information Technology Registry
AKE	Army Knowledge Enterprise
AKEA	Army Knowledge Enterprise Architecture
AKM	Army Knowledge Management
AKM WG	Army Knowledge Management Working Group
AKO	Army Knowledge Online
AKO-S	AKO - SIPRNET
AMC	Army Materiel Command (soon Logistics Command)
ANOSC	Army Network Operations and Security Center
AoA	Analysis of Alternatives
AOR	Area of Responsibility
APC	Army Processing Center
APD	Army Publishing Directorate
APGM	Army Program Guidance Memorandum
API	Individual Application Programming Interface
APIC	Architecture Processing Integration Center
APPG	Army Planning Priorities Guidance
AR	Army Regulation
ARIMS	Army Records Information Management System

ARNG	Army National Guard
ARSTAF	Army Staff
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
ASA(FM&C)	Assistant Secretary of the Army (Financial Management & Comptroller)
ASA(M&RA)	Assistant Secretary of the Army (Manpower & Reserve Affairs)
ASCC	Army Service Component Command
ASCP	Army Small Computer Program
ASD (AT&L)	Assistant Secretary of Defense (Acquisition, Technology & Logistics)
ASG	Area Support Group
ASID	Automated Systems Intelligence Database
ASPG	Army Strategic Planning Guidance
AUSA	Association of the United States Army
AWPS	Army Workload and Performance System
BASOPS	Base Operations
BCA	Business Case Analysis
BFC	Biometrics Fusion Center (DoD)
BIC	Business Initiatives Council (DoD)
BMO	Biometrics Management Office (DoD)
BP	Best Practices
BRAC	Base Realignment and Closures
BSC	Balanced Scorecard
C2	Command and Control
C3I	Command, Control, Communications and Intelligence
C4IM	Command, Control, Communications, Computers, and Information Management
C4ISP	Command, Control, Communications, Computers, and Intelligence Support Plan
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
C4/IT	Command, Control, Communications, Computers/Information Technology
CA	Commercial Activities
CAC	Common Access Card
CADM	Core Architecture Data Model
CCB	Configuration Control Board
CDA	Central Design Activities
CFDAdS	Component Functional Data Administrator
CECOM	Communications and Electronics Command (AMC)
CENDOC	Centralized Documentation
CERDEC	Communications Electronics Research and Development Engineering Center
CERT	Computer Emergency Response Team

CFSC	Community and Family Support Center
CIO	Chief Information Officer
CIO-EB	Chief Information Officer – Executive Board
CIO/G-6	Chief Information Officer/G-6
CKO	Chief Knowledge Officer
CMM	Capability Maturity Models
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COE	Corps of Engineers
COIs	Communities of Interest
COMSEC	Communication Security
CON	Certificate of Networthiness
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations Plan
CoP	Community of Practice
COP	Common Operational Picture
COTS	Commercial Off-The-Shelf
CP-34	Career Program – Information Technology/Management
CPIM	Capital Planning and Investment Management
CRD	Capstone Requirements Document
CROP	Common Relevant Operational Picture
CRYPTO	Cryptographic
CSA	Chief of Staff, Army
CSLA	Communications Security Logistics Activity
C-TNOSC	CONUS TNOSC
CTO	Certificate to Operate
CXO	Chief Integration Officer
DA	Department of the Army
DAS	Director of the Army Staff
DCTS	Defense Collaboration Tool Suite
DEPCOM	Army Deputy Commander, Army Forces
ARFOR	
DFAS	Defense Finance and Accounting Service
DGSA	DoD Goal Security Architecture
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITSCAP	Defense Information Technology Security Certification and Accreditation Program
DLS	Distance Learning System
DMS-A	Defense Messaging System – Army
DNS	Domain Name System
DOC	Directorate of Contracting

DoD	Department of Defense
DOIM	HQDA Directorate of Information Management
DR	Disaster Recovery
DTLOM-PF	Doctrine, Training, Leadership, Organizations, Material, Personnel and Facilities
DUSA	Deputy Under Secretary of the Army
DUSA-IA	Deputy Under Secretary of Army, International Affairs
E2E	End-to-End
e-Army	Electronic Army
EB	Executive Board
e-Business	Electronic Business
e-Commerce	Electronic Commerce
EA	Executive Agent
EAC	Echelon Above Corp
ECM	Enterprise Configuration Management
EDS	Enterprise Directory Service
EEFI	Essential Elements of Friendly Information
e-Gov	Electronic Government
EID	Enterprise Identifiers
EIM	Enterprise Information Management
EKMS	Electronic Key Management System
EOH	Executive Office Headquarters
ERP	Enterprise Resource Planning
ESC	Enterprise Support Center
ESE	Enterprise Systems Engineering
ESM	Enterprise Services Management
FCS	Future Combat Systems
FDU	Force Design Update
FEMA	Federal Emergency Management Agency
FBI	Federal Bureau of Investigations
FMMP	Financial Management Modernization Program
FOCI	Foreign Ownership, Control, or Influence
FOIA	Freedom of Information Act
FORSCOM	Forces Command
FPC	Functional Processing Centers
FY	Fiscal Year
GCSS-A	Global Combat Service Support –Army
GDS	Global Directory System
GIG	Global Information Grid
GIG-BE	Global Information Grid – Bandwidth Expansion
GISRA	Government Information Security Reform Act
GOSC	General Officer Steering Committee
GPEA	Government Paperwork Elimination Act
HLS	Homeland Security
HQDA	Headquarters, Department of the Army

HTML	Hyper Text Markup Language
HVAC	Heating, Ventilation and Air Conditioning
I2AA	Installation Information Assurance Architecture
I3A	Installation Information Infostructure Architecture
I3MP	Installation Information Infostructure Modernization Program
I&A	Identification and Authentication
IA	Information Assurance
ICC	Integrated Circuit Chip
ICT	Integrated Concept Team
IDM	Information Dissemination Management
IESS	Information Exchange Standards Specifications
IG	Inspector General
ITEC4	Information Technology E-Commerce and Commercial Contracting Center
ITSB	Integrated Theater Signal Battalion
IM	Information Management
IMA	Installation Management Agency
IMCEN	Information Management Center
IMIP	Information Management Implementation Plan
IMOs	Information Management Officers
INSCOM	Intelligence and Security Command
IO	Information Operations
IPT	Integrated Process Team
ISEC	Information Systems Engineering Command (CECOM, AMC)
ISL	Installation Sequence List
IT	Information Technology
ITSB	Integrated Theater Signal Battalion
ITEC4	Information Technology E-Commerce and Commercial Contracting Center
JAG	Judge Advocate General
JAGC	Judge Advocate General's Corps
JC4P	Joint Command, Control, Communications and Computer Package
JDP	Joint Development Project
JFCOM	Joint Forces Command
JIM	Joint, Inter-Agency, and Multi-National
JTA-A	Joint Technical Architecture - Army
JTF-CNO	Joint Task Force
JTIC	Joint Test Interoperability Command
JTRS	Joint Tactical Radio System
JV2020	Joint Vision 2020
KBO	Knowledge-Based Organization
KCC	Knowledge Collaboration Center
KM	Knowledge Management
KMI	Key Management Infrastructure

KPPs	Key Performance Parameters
KPR	Knowledge Process Reengineering
KSF	Key Success Factors
LAN	Local Area Network
LIWA	Land Information Warfare Activity
MACOM	Major Army Command
MDEP	Management Decision Package
MDW	Military District of Washington
MEDCOM	Medical Command
MID	Management Initiative Decision
MILDEP	Military Departments
MNS	Mission Needs Statement
MOC	Management of Change
MOS	Military Occupational Specialty
MOU	Memorandum of Understanding
MTMC	Military Traffic Management Command
MTOE	Modified Tables of Organization and Equipment
MWR	Morale, Welfare, and Recreation
NCCWG	Non-Core Competencies Working Group
NCES	Net-Centric Enterprise Services
NCIC	National Crime Information Center
NETCOM/9 th	Network Enterprise Technology Command/9 th Army Signal
ASC	Command
NETCOP	Network Common Operational Picture
NETOPS	Network Operations
NGB	National Guard Bureau
NI2	Networks and Information Integration
NIPRNET	Non-Classified Internet Protocol Router Network
NOCs	Network Operating Centers
NORTHCOM	Northern Command
NOS	Network Operating Systems
NOSC	Network Operations and Security Center
NSA	National Security Agency
NSS	National Security System
OA	Operational Architecture
OCAR	Office of the Chief, Army Reserve
OCONUS	Outside CONUS
OE	Operational Environment
OFTF	Objective Force Task Force
OI	Organizational Integrator
OMB	Office of Management and Budget
OMM	Official Mail Management
OPCON	Operational Control
OPM	Office of Personnel Management
OPSEC	Operational Security

ORDS	Operational Requirements Document
OSD	Office of the Secretary of Defense
PA&E	Program Analysis & Evaluation
PAO	Public Affairs Office
PBX	Private Branch Exchange
PC	Personal Computer
PEG	Program Evaluation Group
PEOs	Program Executive Officers
PEO C3T	Program Executive Office for Command, Control, Communications, and Tactical
PEO EIS	Program Executive Office, Enterprise Information Systems
PERSCOM	Personnel Command
PFB	Process Functional Board
PKE	Public Key Enabling
PKI	Public Key Infrastructure
PL	Public Law
PM	Program Manager
PM SET-D	PM Secure Electronic Transactions – Devices
PoC	Proof of Concept
POI	Program of Instruction
POM	Program Objective Memorandum
PPBES	Planning, Programming, Budgeting and Execution System
PROBE	Program Optimization & Budget Evaluation
QDR	Quadrennial Defense Review
QOS	Quality of Service
RAMP	Remote Access Migration Plan
RCERT	Regional Computer Emergency Response Team
RCIO	Regional Director/Regional CIO
RD	Regional Director
RDAISA	Research, Development, and Acquisition Information Systems Activity
RDECOM	Research and Development Engineering Command
RDF	Resource Description Format
RFI	Request For Information
ROI	Return on Investment
RSC	Regional Support Commands
S&NM	Systems and Network Management
SA	Systems Architecture
SAB	Secret and Below Initiative
SABERS	State Accounting Budgeting Expenditure and Reservation System
SATCOM	Satellite Communications
SDE	Shared Data Environment
SECARMY	Secretary of the Army
SIGCEN	Signal Center

SIPRNET	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SLM	Service Level Management
SMDC	Space Missile Defense Command
SME	Subject Matter Experts
SNM	Systems and Network Management
SRS	Strategic Readiness System
SSAA	System Security Authorization Agreement
SSO	Single Sign On
STARC	State Area Commands
STRATCOM	Strategic Command
SWA	Southwest Asia
TAA	Total Army Analysis
TADLP	The Army Distance Learning Program
TADSS	Training Aids, Devices, Simulators, and Simulations
TAG	The Adjutant General
TAP	The Army Plan
TAR	Theater Asset Repository
TCO	Total Cost of Ownership
TCP	Transformation Campaign Plan
TCS	Transformation Communications Systems
TDA	Table of Distribution and Allowances
TDY	Temporary Duty
TECHCON	Technical Control
TIN	Theater Installation and Networking Company
TIP	Theater Injection Point
TNOSC	Theater Network Operations and Security Centers
TOE	Table of Organization and Equipment
TRADOC	Training and Doctrine Command
TSC	Theater Signal Command
TSC-A	TSC-Army Study
TTSB V2	Theater Tactical Signal Battalion Version 2
TV-1s	Technical Views
UFR	Unfinanced Requirements
USAAC	United States Army Accessions Command
USACE	United States Army Corps of Engineers
USAFMSA	United States Army Force Management Support Agency
USAR	United States Army Reserve
USAREC	United States Army Recruiting Command
USAREUR	US Army Europe
USD	US Defense Comptroller
Comptroller	
USSTRATCOM	U.S. Strategic Command
VI	Visual Information
VPN	Virtual Private Network

VTC	Video Teleconference
WAN	Wide Area Network
WDC	Warrior Development Center
WIN2K	Windows 2000
WIN-T	Warrior Information Network - Tactical
WKN	Warrior Knowledge Network
XML	eXtensible Markup Language

Appendix B: Commonly Used Knowledge Management Terms

Activity: A process, function or task that occurs over time and has recognizable results. Activities combine to form business processes.

AKO-Linked. System is web enabled and linked through a page on AKO so that users can get to the system via the portal. This is the initial minimum standard that's should have been met NLT 31 July 2002.

AKO Single Sign On Enabled. System is AKO-linked and utilizes the AKO Directory Services for access authorization. A user who is logged on to the AKO portal will have access to the system without having to go through a separate system login. An interim goal will be to provide a separate system login prompt that uses the same AKO UserID/password, but this does not count as "AKO Single Sign On" status for reporting purposes.

Algorithm: A formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point. Algorithms can be expressed in any language, from a natural language like English to a programming language like Java.

Analysis: A process of manipulation and accessing data to turn data into knowledge.

Application: The system or problem to which a computer is applied. Reference is often made to an application as being of the computational type, wherein arithmetic computations predominate, or of the data processing type, wherein data handling operations predominate.

Applications Component: Use of software to perform specific tasks or functions, such as word processing, creation of spreadsheets, generation of graphics, facilitating electronic mail, or other processes relating to Army Knowledge Enterprise.

Army Common Operating Environment (ACOE): Provides the ubiquitous foundation for all Defense Information Infrastructure system architectures to enable operational realization of the Command, Control, Communications, Computers, and Intelligence for the Warrior vision. The ACOE enables rapid application integration, a point and click installation, and fast turnaround for the War-fighter. It provides reusable, architecturally consistent, integrated components called segments. The Contemporary Operating Environment provides a process for distributing engineering across the Army, supporting the construction of systems from components developed by disparate organizations.

Army Data Management: Establishes information about the set of data standards, business rules and data models required to govern the definition, production, storage, ownership and replication of data used in the Army. Army Data Management facilitates the dissemination and exchange of information among organizations and information systems throughout not only the Army by also Department of Defense and the Federal Government. It manages information requirements from data models and business rules down to data elements and data value levels of detail. It facilitates internal, joint and combined interoperability through the standardization and use of common data elements. Data management improves data quality and accuracy, and minimizes the cost of data production and data maintenance. It provides guidance for all data exchanges and will be used in Information Technology planning. Army Data Management implements the information standard portion of Joint Technical Architecture – Army (JTA-A).

An Army Enterprise: an action, activity, program or effort (for example, information technology) across the Army.

The Army Enterprise: The Army; including all combat, combat support, and business operations, missions, tasks and activities or functions across all components.

Army Enterprise Directory: A single location for applications and users to quickly find information—dramatically increased information sharing (locating), reduced cost in application development, and database and/or directory administration.

Army Enterprise Infostructure (AEI): The Army Enterprise Infostructure is the implementation of the Army's portion of the Global Information Grid (GIG-A) and will provide the Army the ability to deploy anywhere, anytime. The AEI supports the GIG framework and enables the Objective Force in its operational net-centric environment.

Army Information Technology Registry (AITR). The AITR is an online system, available through the AKO portal to track all Army Systems. Eventually, it will be become the single tool for all data calls related to these systems. AITR is available through the AKO portal within the CIO/G-6 Community on the “AKM” page.

Army Knowledge Centers: A central Web-based repository that stores, organizes, and shares individual expertise and organizational information, such as documents, databases, and workflow systems and best practices. Exponential power occurs when individuals and organizations use the knowledge center's collaboration and self-service capabilities to rapidly and accurately access and analyze enterprise information. World-class knowledge centers include those at Joint Forces Command, PEO C3S, and the Army JAG Corps.

Army Knowledge Enterprise (AKE): The AKE framework consists of an enterprise-level infostructure and knowledge-based capabilities. It extends, compliments and supplements the GIG components. It provides for the integration and the interoperability of functional processing, storing, and transporting information over a seamless infostructure allowing access to universal and secure Army knowledge.

Army Knowledge Enterprise Architecture (AKEA): The integrated IT blueprint for a network-centric, knowledge-based force with access to universal and secure Army knowledge across the enterprise, including every echelon from sustaining base to forward deployed forces as part of Joint, Multinational and Inter-agency operations. This includes the transport of the data from end to end, the storage of data, and the use of information technology to mine data to create new knowledge. AKEA includes the operational requirements for combat, combat support, and business/functional areas that drive knowledge requirements; the infostructure to ensure storage and transmission of the related data; and the protocols and standards to ensure that the systems and systems-of-systems can exchange data within the Army and between the Army and other Services, DoD, and other entities including coalition partners. The AKEA supports the use of IT to simulate some aspects of knowledge and to break down Domain and Component barriers for the transmission of sharing of knowledge. Development of the AKEA depends upon multiple organizations using a standard set of rules and procedures for data development, storage, and manipulation that will enable data sharing. AKEA also provides metrics for compliance to aid adherence to the standards and protocols laid down in the architectures. The AKEA concept replaces the Army Enterprise Architecture concept.

Army Knowledge Enterprise Concept: The AKE Concept enables the Army Knowledge Management (AKM) Vision to transform the Army into a network-centric, knowledge-based force. The AKM strategic goals focus the Global Information Grid components (i.e., applications, computing, communications, network operations, and information management) into the AKE components of infostructure and knowledge. The AKE infostructure component (Army Enterprise Infostructure – AEI) maps directly back to the GIG’s communications, enterprise common-user services, network operations, and information management components.

Army Knowledge Enterprise Construct: Graphic illustration of the AKE as developed from drivers to the AKM Strategy through implementation of the Army Knowledge Vision in the Objective Force.

Army Knowledge Management: The Army’s approach to knowledge management. AKM integrates and establishes a systematic approach to identifying, managing, and sharing enterprise-wide information assets.

Army Knowledge Online (AKO): The Army's Enterprise Portal. It serves as a single point of entry for Army Knowledge resources on the Army NIPRNET.

Army Knowledge Online-SIPRNET (AKO-S): Army's enterprise portal for knowledge classified at the secret level.

Army Operational Architecture: Describes tasks and activities, operational elements, and information flows required to accomplish or support an operation - whether the operation is a military or combat support function. Army Operational Architecture defines types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in detail sufficient to ascertain specific interoperability requirements. Operational Architecture defines the functional requirements that may lead to future systems development or process improvement efforts. It is a prerequisite to the other two architectural views: System Architecture and Technical Architecture.

Army System Architecture: Describes systems and their interconnections supporting war-fighting functions. The System Architecture enables or facilitates operational tasks and activities through the application of physical resources. It maps systems with their associated platforms, functions, and characteristics back to the operational architecture. The System Architecture identifies systems interfaces and defines the connectivity between systems. It is based upon and constrained by the Army Operational Architecture and JTA-A.

Artificial Intelligence: Computer hardware and software packages that try to emulate human intelligence in order to solve problems using reasoning and learning. There are various techniques such as expert systems that have historical roots in artificial intelligence.

Balanced Scorecard System: Method of measuring performance of a firm beyond the typical financial measures. Links corporate goals and direct performance measures in a blueprint specific to a firm, and is one method of measuring the impact of knowledge management.

Baseline: The current condition that exists in a situation. It is usually used to differentiate between a current and a future representation.

Benchmarking: The process of identifying, understanding, and adapting outstanding, or “best” practices from organizations anywhere in the world to help an organization improve its performance. Benchmarking is a tool to help an organization, unit or team improve its business or operational processes. Any business or operational process can be benchmarked. Benchmarking is a highly respected practice in the business world. It is an activity that looks outward to find best practice and high performance and then measures actual business or military operations against those outstanding strategies, tactics, techniques and procedures with a proven record of success elsewhere. It then provides, where feasible, “a way” for practical application of shared best practice across the organization. Internal benchmarking studies the practices and performance within The Army. External benchmarking determines the performance of other, preferably world-class, organizations, public or private. Two common forms of benchmarking are metric and process. “Metrics” give numerical standards against which an organization’s own processes can be compared. Metrics are usually determined via a detailed and carefully analyzed survey or interviews. Organizations are then able to identify shortcomings, prioritize action items, and then conduct follow-on studies to determine methods of improvement. Another form of benchmarking includes “process benchmarking,” generally higher-level and less numbers-intensive than metrics. These studies demonstrate how top performing units and teams accomplish the specific process in question. Such studies can take the form of research, surveys/interviews, and site visits. By identifying how others perform the same functional task or objective, leaders and leader teams gain insight and ideas they may not otherwise achieve. Such information affirms and supports quality decision-making. The benefits of process benchmarking are realized when leaders employ recommendations and embark on a change process -- making marked improvements in mission accomplishment, taking care of their personnel and reducing costs in time and money.

Best Practices: Business processes, strategies, and tactics, techniques and procedures (TTPs) employed by organizations, units, teams and individuals, particularly leaders and leader teams at all grades, and validated as especially effective by Army communities of practice, the lessons-learned program or proponents. Validated best practices are included in a common database with lessons learned in a form that best enables their consideration for inclusion in doctrine and training literature, and other authoritative knowledge products. The Army’s best practices include documented strategies and TTPs employed by other, highly admired organizations, including businesses. Best practices imported from the experience of organizations outside the Army have a proven record of success in providing competitive advantage to those who implemented them, and have passed review by Army communities, the lessons-learned program, or proponents as relevant to Army practice.

Biometrics: Biometrics are measurable physical characteristics or behavioral traits used to positively authenticate the identity of an individual (e.g. fingerprint, iris, face recognition).

Browser Based: A web-based application.

Business Case Analysis: A management planning and decision-making tool that is used to define alternative ways of doing business and the associated investment and operating costs, savings, payback period, and return on investment. The analysis includes the rationale and methodology for quantifying benefits and costs to include a discussion of critical success factors and risk assessment.

Business Domain: Those systems and information that allow the Army to function and operate on a daily basis. Information includes personnel, logistics, readiness, finance, health care, transportation, JAG, law enforcement, acquisition, and resource management. (As identified in Joint Technical Architecture-Army sub domains).

Business Intelligence (BI): A practice in which data is collected, analyzed, and provided to internal users to help them make informed business decisions. Statistical analysis, data mining, and online analytical processing (OLAP) are some of the tools that enable effective BI.

Business Objectives: Goals of the organization that can be measured in some quantitative way. (e.g. Decrease cost by 15%. Become the supplier with the lowest rate of returned products.)

Business Process Portal: Focuses on solving a particular business problem or manage a particular business function. Business process portals bring the right information to the right people at the right time to help them get their work done. A business process portal is a type of vertical portal.

Business Process Reengineering (BPR): A structured approach by all or part of an enterprise to improve the value of its products and services while reducing resource requirements. The transformation of a business process to achieve significant levels of improvement in one or more performance measures relating to fitness for purpose, quality, cycle time, and cost by using the techniques of streamlining and removing added activities and costs.

Collaboration: The use of technologies, especially those that utilize the Internet, to create a virtual environment to promote and support the exchange of knowledge at the right time and place to affect an action, solve a problem, and/or impact a better decision.

Collaborative Tools: Tools that enable sharing of knowledge across time and distance. These tools may enable both structured and free-flow sharing of knowledge and best practices. Transcripts of the use of these tools may be incorporated into a knowledge base for future use.

Command and Control (C2) Domain: Command and Control of Army warfighting, combat support, and combat services support activities to include: Air Defense, Maneuver, Combat Services Support (CSS), Intelligence, Fire Support, Common Relevant Operational Picture (CROP).

Command, Control, Communications, Computers and Information Management (C4IM): Enterprise wide Information Management of C4. Refers to integrated systems of doctrine, procedure, organizational structures, personnel, equipment, facilities, communications, and information management systems designed to support the Army's exercise of information management across the range of military operations.

Communications Component: Includes

Transport: End-to-end movement of data, information, and/or knowledge between users and producers through other intermediate Global Information Grid entities.

Communications Networks: Sets of products, concepts, and services that enables the connection of computer systems for the purpose of transmitting data and other forms (e.g., voice and video) among the systems. (AEAGD)

Communications Nodes: Nodes that are either internal to the communications network (e.g., routers, bridges, or repeaters) or located between the end device and the communications network to operate as a gateway. (AEAGD)

Communications Systems: Sets of assets (transmission media, switching nodes, interfaces, and control devices) that establish linkage between users and devices. (AEAGD)

Community: A body of people having common rights, privileges, or interests.

Community of Practice: A group of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis. All CoPs share three structural sub-elements: the domain, the community and the practice. The domain is the topic of the community – the shared domain creates a sense of accountability to a body of knowledge, and therefore to development of a practice. The community is the body of members, engaged of their own volition based on shared passion for the topic, who interact regularly on issues important to their domain. The practice is the specific knowledge the community acquires, creates, maintains, and shares from a common set of perspectives to respond to a common set of situations and to solve a common set of problems. The purpose of CoPs is to create, expand, and exchange knowledge, to develop individual capabilities, and to support the development of team and unit capabilities. They deepen passion, commitment, and identification with fellow practitioners and their respective, collective expertise. The community of practice is the dominant structure of a knowledge-based organization. It serves as the principal component of that organization’s knowledge system, affecting processes from innovation and learning activities, where knowledge is generated and transferred, to the operations and business activities, where knowledge is applied. Synonyms for community of practice include “knowledge network” and “learning community.”

Component: A logical grouping of technologically distinct C4/IT capabilities and related processes required to provide a service across the Army Knowledge Enterprise. Components act as “architecture glue” that binds the Domains at their points of interconnection.

Computer Network Defense (CND): Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, and destruction.

Computing Component: Use of computer technology to manipulate data, information, and/or knowledge into the desired form to support decision-making and other functions. Includes Regional and Global Computing and Personal and Local Computing sub-components.

Consilience: The fusion, creation and integration of knowledge through interdisciplinary, cross-functional, cross-domain or inter-organizational work.

Content: The data, information, and knowledge (including processes and procedures), which are important to the organization.

Content management: Technologies that allow the capture and management of explicit experience. It allows people to capture, codify, and organize experiences and ideas in central repositories. A more general term than data management, content management includes structured and unstructured data.

Content mapping: Identifying and organizing a high-level description of the meaning contained in a collection of electronic documents.

Core Competencies: The complex set of skills, knowledge, and resources that span the organization, yield a sustainable competitive advantage in the marketplace, and permeate the organization's culture. Core competencies evolve over time and are based on specific "know-how."

Core Rigidity: Opposite of core competency. Defining any core competency too narrowly may turn it into a core rigidity. Core rigidities are unquestioned assumptions about an organization's products, policies, or positioning, which lead to complacency and inhibit innovation.

Corporate Knowledge: The collective body of experience and understanding of an organization's processes for managing both planned and unplanned situations.

Corporate Knowledge Management: The process whereby knowledge seekers are linked with knowledge sources and knowledge is transferred.

Customer Capital: The value of an organization's relationships with the people with whom it does business, or the value of its [the company's] franchise, its ongoing relationships with the people or organizations to which it sells.

Customer Relationship Management (CRM): A collection of methodologies, software, and often Internet capabilities that enable an enterprise to better understand its customer and customer interaction through improved management of marketing campaigns, accounts, and sales, leading to improved customer satisfaction and maximized profits.

Data: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representation such as characters or analog quantities to which meaning is or might be assigned. (Joint Publication 1-02)

Database: A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications. A database is generally considered to be structured data. (Army Enterprise Architecture Guidance Document, Version 1.1, 23 December 1998)

Data Mining: A class of database applications that looks for hidden patterns in a group of data. Data mining software can help retail companies find customers with common interests. The term is commonly misused to describe software that presents data in new ways. True data mining software does not just change the presentation, but actually discovers unknown relationships among the data.

Data Warehousing: A collection of data designed to support management decision-making. Data warehouses contain a wide variety of data that present a coherent picture of business conditions at a single point in time. Development of a data warehouse includes development of systems to extract data from operating systems plus installation of a warehouse database system that provides managers flexible access to the data. Data warehousing generally refers to many different databases across an entire enterprise.

Decision Support Systems (DSS): Interactive computer-based systems intended to help decision makers utilize data and models to identify and solve problems and make decisions. The system must aid a decision-maker in solving unprogrammed, unstructured (or "semi-structured") problems. The system must possess an interactive query facility, with a query language that is easy to learn and use.

Defense-In-Depth. The citing of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations or the whole position by the enemy, and to allow the commander to maneuver the reserve. (Joint Publication 1-02)

Discontinuity of Knowledge: A phenomenon that occurs when experienced knowledge workers move from one position to another position (inside or outside an organization) without having adequate time or KM facilities to transfer their tacit knowledge to coworkers.

Domain: A logical grouping of prime system elements (PSEs) that have similar characteristics or serve similar functions providing a capability across the Army Knowledge Enterprise. A domain exists irrespective of echelon and irrespective of whether it is in the Legacy, Interim, or Objective Force.

Double-Knit Knowledge Organization: An organization in which the communities of practice that steward knowledge and the operational and business processes, executed by teams and units (units of action, units of employment, business units), are tightly interwoven. Practitioners themselves, in their dual roles as both community practitioners and operational team members, help link the capabilities of communities of practice to the knowledge requirements of leader teams and units. In some of the literature, the “double-knit” is referred to as a “learning lattice,” with the vertical axes of multifunctional teams intersecting with the horizontal axes of communities of practice. The “double knit” is an essential enabler for the learning and knowledge-based organization, making it possible for an organization to learn fully from its own experience and to leverage fully its own (and other’s) knowledge as it prepares for war, achieves situational awareness and understanding, makes timely decisions, and finishes decisively through superior performance. It supplies the human and knowledge component of the network-centric organization as the “double knit” of corporate intellect complements, and is tied together, by telecommunications and electronic collaboration tools.

eBusiness: Conducting business applications using various electronic technologies that are changing and improving the method and location for transactions and information exchange. eBusiness incorporates Knowledge Management (KM), Business Intelligence (BI), Electronic Commerce (EC), Electronic Collaboration Tools (ECT), Customer Relationship Management (CRM), and Supply Chain Management (SCM).

Electronic Collaboration Technology (ECT): The use of groupware tools online to encourage internal and external communication and cooperative work efforts concerning information, products and services.

Electronic Commerce (EC): The process of conducting transactions for goods, services, and associated information via an intranet, extranet or the Internet, typically using catalog/search, shopping carts, and transaction technologies.

Enterprise: The highest level in an organization; it includes all missions, tasks and activities or functions. (Army Enterprise Architecture Guidance Document, Version 1.1, 23 December 1998)

Enterprise Architecture: A strategic information asset base that defines the missions, the information necessary to perform the mission and the transitional process for implementing new technologies IAW changing needs of an enterprise.

Enterprise Management: The implementation and oversight of information technology resources and policies for the sustainment, operation, and defense of The Army Infostructure to support the missions and functions of The Army.

Enterprise Portal: A web site or service that offers a broad array of resources and services, such as e-mail, forums, search engines, on-line self-service applications, security, directory, profiling, taxonomy, application integration.

Enterprise-wide: An action, activity, program or effort such as a technology that is applicable across an entire organization such as the Army. For the Army, this means “factory to foxhole” and “mud to space.”

Entity: The representation of a set of real or abstract things (people, objects, places, events, ideas, combination of things, etc.) that are recognized as the same type because they share the same characteristics and can participate in the same relationships.

Epistemology: The study of the nature and foundations of knowledge.

Executive Information Systems (EIS): A computerized system intended to provide current and appropriate information to support executive decision making for managers using a networked workstation. The emphasis is on graphical displays and an easy to use interface that present information from the corporate database. They are tools to provide canned reports or briefing books to top-level executives. They offer strong reporting and drill-down capabilities. These tools must provide information in context to convert information to knowledge.

Executive Support Systems (ESS): An executive information system (EIS) that includes specific decision aiding and/or analysis capabilities.

Expert System: An artificial intelligence application that uses a knowledge base of human expertise for problem solving. Its success is based on the quality of the data and rules obtained from the human expert. Expert systems are an ideal way to convert both tacit and explicit knowledge into a form that is available to many users, a key process in knowledge management. The implementation of expert systems involves systematic and well-established procedures for representing the knowledge of experts, a process referred to as knowledge engineering. For many purposes, expert systems have advantages over human experts. These include increased availability, lower cost, greater reliability, increased confidence in decision-making ability, faster response, steadiness and completeness (in an emergency, expert systems can perform better and without emotional impediments), clear reasoning for a given answer, and more intelligent access to databases.

Explicit Knowledge: Formal knowledge that can be conveyed from one person to another in systematic ways such as documents, e-mail, multimedia, etc. Knowledge that is easily codified and conveyed to others.

Extensible Markup Language (XML): A specification developed by the World Wide Web Consortium (W3C) especially for web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and among organizations. These customized tags can provide functionality not available with HTML. For example, XML supports links that point to multiple documents, as opposed to HTML links, which can reference just one destination each.

Functional Domains: A domain is a logical grouping of prime systems elements that have similar characteristics or serve similar functions providing a capability across the army Knowledge Enterprise. A domain exists irrespective of echelon and irrespective of whether it is in the Legacy, Interim, or Objective Force.

Functional Processing Centers: Centers where MACOMs and Functional Proponents process raw data into useful information. Many such centers run functional unique processes.

Future Combat System: The networked system of systems that will serve as the core building block within all maneuver Unit of Action echelons to develop overmatching combat power, sustainability, agility, and versatility necessary for full spectrum military operations. It is comprised of a family of advanced, networked maneuver, maneuver-support and sustainment systems (space-, air- and ground-based) that will include manned and unmanned platforms. The FCS further includes suites of information technologies, reconnaissance, surveillance, and target acquisition (RSTA) networks, and battle command systems that will enable the tactical unit to operate at a level of synchronization heretofore unachievable. The largest FCS systems will be lighter than current mechanized systems with each element possessing common or multi-functional characteristics. FCS units must achieve all organizational characteristics in the Army Vision.

Global Information Grid (GIG): 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 war-fighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. (Joint Publication 1-02)

Governance: The act, process, or exercise of authority and control including the persons who make up a governing body to administer such actions.

Heuristic: A rule of thumb that involves or serves as an aid to learning, discovery, or problem solving by experimental and especially trial-and-error methods. Of or relating to exploratory problem-solving techniques that utilize self-educating techniques (as the evaluation of feedback) to improve performance.

Horizontal Portal: A portal, which pulls together several vertical portals and is standardized across an enterprise.

Human Capital: The capabilities of the individuals required to provide solutions to customers, and thus directly or indirectly to leaders and soldiers preparing for, or engaged in, full-spectrum operations. One of the three main components of intellectual capital (along with structural and customer or relationship capital), human capital is the source of innovation and transformation.

Hyper Text Markup Language (HTML): An authoring language used to create documents on the World Wide Web.

Implicit Knowledge: The sum or range of what has been perceived, discovered, or learned. Implicit Knowledge is contrasted with explicit knowledge.

Incentivize: Using awards or rewards to entice, lead, or otherwise encourage individuals, groups or organizations to do a certain thing.

Information: The meaning that a human assigns to data by means of the known conventions used in their representation. (JCS Pub 1)

Information Assurance: Information Operations (IO) 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 non reaction capabilities. (Joint Publication 1-02)

Information Architecture: The art and science of organizing information to help people effectively fulfill their information needs. Information architecture involves investigation, analysis, design and implementation.

Information Dissemination Management: A set of integrated applications, processes and services that provide the capability for producers and users to locate, retrieve, and send/receive information by the most effective and efficient means in a manner consistent with a commander's policy. Fundamental IDM services include information awareness, information access, information delivery, and IDM support.

Information Management Component: The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructure. Includes data administration, database administration, and records management.

Information Management Officer/Office (IMO) will be a designation given to a person or group of people coordinating C4IM requirements and/or execution with the supporting installation DOIM. An IMO is designated to support mission applications and associated databases. The IMO is the installation DOIM's primary interface with the supported organizations.

Infostructure: The information technology (computers, software, architecture, security, communications, programs and facilities) required to support the net-centric Army.

Infrastructure: The term is used with different contextual meanings. It most generally relates to and has a hardware orientation, but it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs.

Installation Information Infrastructure Architecture (I3A): Establishes an Army-wide Information Technology (IT) architectural design standard. The I3A is the source to fuel effective Army Knowledge Management necessary to support the Army Transformation Campaign Plan. I3A captures installation infostructure, synchronizes the implementation of automation programs, provides for analysis of operational force and sustaining base connectivity, and identifies costs associated with IT modernization. The I3A Configuration Control Board (CCB) manages I3A issues and tracks developments in IT technology, information assurance, enterprise systems management and automation information systems (AIS). The CCB, which oversees several working groups that address IT issues, meets quarterly. The Army I3A Repository is an on-line, password protected, database of existing and future installation infostructure maintained by the Fort Detrick Engineering Office, Information Systems Engineering Command. Under I3A, the Installation Information Infostructure Modernization Program (I3MP) implements installation IT data network upgrades. The Program Manager, Defense Data Network (PM DDN), U.S. Communications and Electronics Command (CECOM), Fort Monmouth administers the I3MP.

Intellectual Capital: The knowledge resulting from communications, collaboration, interpersonal relationships; ideas, patents and organizational processes; and tangible information resources such as databases, documents, lessons-learned systems, etc. Intellectual capital includes human capital, social capital and corporate capital that contribute to the growth of the organization. It can also be the knowledge and potential of employees, based on their education, experience, learned techniques, and best practices.

Intelligence, Surveillance, and Reconnaissance (ISR) Domain:

Intelligence is derived from collection, processing, integrating, analysis, evaluation, intercept of information received on the plans of allies and potential enemies through a variety of methods (electronic, investigative, human informants, etc.).

Surveillance is the systematic observation of space, surface or sub-surface through electronic or other means.

Reconnaissance is to obtain by visual observation or other detection methods of activities of enemy, meteorological, hydrographic, geographic areas.

Mission Areas include: Signals Intelligence, Human Intelligence, Counter Intelligence, Imagery, Measurements and Signatures, and Tactical Intelligence.

Interagency Coordination: Within the context of Department of Defense involvement, the coordination that occurs between elements of the Department of Defense and engaged U.S. Government agencies, non-governmental organizations, private voluntary organizations, and regional and international organizations for the purpose of accomplishing an objective.

Interface: The ability to connect two separate entities such as programs, devices, or programs to devices. For example, two devices that can transmit data between each other are said to interface with each other.

Internet: Worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange.

Interoperability: The ability of systems, units, or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together. (Joint Publication 1-02).

Intranet: A computer network that functions like the Internet, using Web browser software to access and process the information that employees need, but the information and Web pages are located on computers within the organization/enterprise. A firewall is usually used to block access from outside the Intranets. Intranets are private Web sites.

ISO 9000: Family of quality management and quality assurance standards adopted by ISO (International Organization for Standardization, founded 1947), an international consensus of over 110 countries. ISO 9000, first published in 1987, has been adopted as national standards in more than 80 countries.

Joint Technical Architecture - Army (JTA-A): A compilation of the standards, protocols, and technical specifications that enable Army systems to efficiently exchange information with other systems and take advantage of common system components. (Army Enterprise Architecture Guidance Document, Version 1.1, 23 December 1998).

Killer Application: A new information technology good or service that single-handedly rewrites the rules of an industry or set of industries. "Killer apps" establish an entirely new category and dominate it by being first. They are fundamentally disruptive and are killers in a double sense. They yield spectacular returns on investment and economic growth, yet destroy whole industries. They often change the rules of the game in sectors far from their point of origin or intended market, with disruptive implications for government, including the military, and society as a whole. The World Wide Web is a spectacular example of such an application, one that in turn has helped spawn the concept of network-centric and knowledge-based warfare. According to the leading strategist of e-learning, knowledge management itself an e-learning killer app. Focus on creation of killer apps, whether or not it succeeds in producing such an application, sets a high standard for transformational efforts, and encourages thinking about the context in which applications are set, including their second and third order effects.

Knowledge: "The fact or condition of knowing something with familiarity gained through experience or association." Knowledge is the richness of learning, insight and experience that is in people's heads (and some say in their bodies). Knowledge is the background that allows you to make the best decision or to perform a task – it is a platform for action. Knowledge can be in people's heads (tacit knowledge) or it can be written down or recorded (explicit knowledge). One can never capture the full richness of what's in people's heads. However, explicit knowledge can be a good catalyst for connecting people together, as it can be stored and searched. Captured knowledge can be of enormous value if easy to share, easy to read, easy to add to, if it provides a connection to others who know, and if it generates new insights and knowledge.

Knowledge Acquisition: The procedure in artificial intelligence of interacting with an external source, usually a domain expert, to find and organize knowledge for the purpose of transferring the knowledge to an expert system to solve problems.

Knowledge Asset: An organizational knowledge set or experience that is usable and re-deployable throughout an organization in a way that creates value. It represents accumulated critical knowledge pertaining to a specific topic that can be reused to improve organizational performance. Knowledge Assets usually include context, performance results, compelling stories, reusable artifacts and links to individuals and are linked to a community of practice, a group of individuals who are actively involved in an area of competence and who are willing to share that knowledge to improve individual and organizational performance.

Knowledge Base: A logical collection of information in a particular domain that has been formalized in the appropriate representation to perform reasoning. A dynamic knowledge base is used to store information relevant to solving a particular problem and varies from one problem-solving session to the next.

Knowledge-based Force: An organization whose processes, tools and technologies are focused on exploiting the enterprise's knowledge assets to achieve mission critical objectives.

Knowledge Discovery: A nontrivial process that gleans new, understandable, interesting, and potentially useful information from stored data. Knowledge discovery is a means of extending limited human capabilities by using computer capabilities to analyze large, often complex datasets in order to understand more information than could have been previously extracted using conventional means.

Knowledge Dominance: An imbalance in one's favor in the knowledge domain that provides decisive competitive advantage in transformation and preparation for, and planning and execution of, full-spectrum operations.

Knowledge Ecology: An inter-disciplinary field of theory and practice that provides tools and methods for freeing the human genius, individual and collective. It is the component of KM that focuses on human factors; the study of personal work habits, values, and organizational culture.

Knowledge Half-Life: The point at which the acquisition of new knowledge is more cost-effective and offers greater returns than the maintenance of existing knowledge.

Knowledge Management: An integrated, systematic approach to identifying, managing, and sharing all of an enterprise's information assets, including databases, documents, policies and procedures, as well as previously unarticulated expertise and experience resident in individual workers. Fundamentally, KM makes the collective information and experience of an enterprise available to the individual knowledge worker, who is responsible for using it wisely and for replenishing the stock. This ongoing cycle encourages a learning organization, stimulates collaboration, and empowers people to continually enhance the way they perform work.

Knowledge Map: An overview of all the knowledge that is vital to the attainment of strategic organizational goals. Creating a knowledge map focuses on identifying what knowledge we are hoping to share, with whom, and where that knowledge can be found. A knowledge map identifies domains that are the center of an organization's quest for knowledge. It then establishes knowledge links that glue together and strengthen related knowledge so that an organization can take advantage of its synergy. Finally, it defines knowledge segments as everything knowledge professionals and systems know about a specific subject that relates to achieving the organization's strategic and operational goals. Knowledge maps help prevent an accumulation of knowledge that exceeds or falls short of organizational needs. On the one hand, it helps prevent acquisition of knowledge for knowledge's sake. On the other, it focuses effort in filling in the white spaces. In the corporate role, knowledge maps sometimes serve as blueprints for corporate intranets. They may have a role to play in Army architectural and telecommunications efforts.

Knowledge Mapping: A process that provides a "picture" of the knowledge an organization needs to support business processes.

Learning Organization: An organization committed to continuous learning, both for individuals (in their personal development) and for the organization as a whole.

Legacy Systems: Existing information systems and/or databases that may or may not be migrated to a new system that uses newer technology for more efficient and effective delivery.

Lesson Learned: Validated knowledge and experience derived from observations and historical study of military training, exercises, and combat operations. Lessons learned are included in a common database with best practices in a form that best enables their consideration for inclusion in doctrine and training literature, and other authoritative knowledge products.

Liaison: A channel for communication between groups or individuals.

Link or Hyperlink: A connection between two pieces of information. A reference (link) from some point in one document to some point in another document or another place in the same document. A browser usually displays a hyperlink in some distinguishing way, e.g. in a different color, font or style. When the user activates the link (e.g. by clicking on it with the mouse) the browser will display the target of the link.

Metadata: Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata may include descriptive information about the context, quality and condition, or characteristics of data.

Mission Critical (MC) Information System. A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of war fighter operations or direct mission support of war fighter operations. (Note: a Component Head, a Combatant Commander or their designee should make the designation of mission critical.)

Mission Essential (ME) Information System. A system that meets the definition of "information system" in the Clinger-Cohen Act, that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: a Component Head, a Combatant Commander or their designee should make the designation of mission critical.)

Multinational Operations: A collective term to describe military actions conducted by forces of two or more nations usually undertaken within the structure of a coalition or alliance.

Network-centric: Refers to the use of networked technology to deliver information and data electronically.

Network Operations (NETOPS) Component: NETOPS is the organizational and procedural structure used to monitor, manage, and control the Army Infostructure by means of the Army Enterprise functions of Network Management (NM), Information Dissemination Management (IDM), and Information Assurance (IA).

Networthiness: A continual evaluation process that has two primary goals. First, all information systems assets within the AEI will be addressed to ensure that they utilize the network efficiently, securely, are architecturally compliant with the AKEA, meet interoperability standards, and do not interrupt or conflict with other AEI users. Second, the networthiness process ensures that the Army Enterprise Infostructure is used efficiently and can be visualized in order to support the reallocation of resources to support changing mission and threat environments.

Objective Force: The U.S. Army's future full spectrum force: organized, manned, equipped and trained to be more strategically responsive, deployable, agile, versatile, lethal, survivable and sustainable across the entire spectrum of military operations from Major Theater Wars through counter terrorism to Homeland Security. Objective Force units will conduct operational maneuver from strategic distances, creating diverse manifold dilemmas for adversaries by arriving at multiple points of entry, improved and unimproved. As necessary, Objective Force units conduct forcible entry, overwhelm aggressor anti-access capabilities, and rapidly impose their will on opponents. In this manner, Objective Force units arrive immediately capable of conducting simultaneous, distributed and continuous combined arms, air-ground operations, day and night in open, close, complex, and all other terrain conditions throughout the battlespace. Army units conducting joint and combined operations will see first, understand first, act first and finish decisively at the strategic, operational, and tactical levels of operation. The Objective Force is envisioned a skilled, knowledge-based force, exploiting the revolutionary potential of information superiority and networked sensors, shooters, supporters and decision makers.

Objective Force Task Force: The single, overarching, integrating activity with the Department of the Army that provides the direction, means, and impetus for the Objective Force. The task force facilitates the accelerated fielding of the Objective Force this decade by integrating and synchronizing warfighting capabilities and technologies and by providing assessments that focus Senior Army Leadership decision-making. The task force is the action agency for the Secretary of the Army and the Chief of Staff Army to synchronize all Objective Force efforts associated with the entire doctrine, training, leader development, organizational design, materiel, soldiers (DTLOMS) process. The task force charter is to favorably influence multiple parts of the Army, the Office of the Secretary of Defense, the Joint Chiefs of Staff, Congress and industry to ensure the Army achieves Objective Force capabilities this decade.

Ontology: Many definitions abound for ontology. Currently International Standards are being debated for ontologies and their development, implementation and sustainment within the portal and Semantic Web world. For the purposes of this strategic plan, ontology is defined as a collections of statements written in a language such as RDF that define the relations between concepts (for example, using taxonomy to define classes of objects and the relations among them) and specify logical rules for reasoning about them (inference rules). In the emerging Semantic Web, the killer application of the Objective Force, computers will "understand" the meaning of semantic data on a Web page by following links to specified ontologies.

Operational Architecture: A description (often graphical) of the operational elements, assigned tasks, and information flows required to accomplish or support a warfighting function. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges.

Organizational Knowledge: The combination of critical data, information, and knowledge with collective intellect that enables an organization to learn from experience, innovate, make a decision, create a solution, perform tasks, or change a position.

Performance Measure: An indicator that can be used to evaluate quality, cost, or cycle time characteristics of an activity or process usually against a target or standard value.

Portal: Software that provides access through a browser to a wide range of data stores – e-mail, data bases, analytical software, the Internet, billing and sales records, and other sources. A portal is different from other web pages in that a portal is customizable by the user as his needs and interests change.

Power Projection Domain: Enable a single, integrated network with redundancy provided through automated multi-mode, multi-path capabilities, which expand the commander's reach and ensure continuous connectivity from the installation to the combat arena.

Process: A systematic series of actions directed to some end.

Process Portal: Software that focuses the user of the portal to the explicit knowledge required to solve his/her particular problem, or deal with a particular situation or series of events. Changes implicit knowledge to explicit knowledge.

Push: In client/server applications, "pushing" is sending data to a client without the client requesting it. The World Wide Web is based on a pull technology where the client browser must request a web page before it is sent. Broadcast media, on the other hand, are push technologies because they send information out regardless of whether anyone is tuned in.

Repository: A mechanism for storing any information that has to do with the definition of a system at any point in its life cycle. Repository services would typically be provided for extensibility, recovery, integrity, naming standards and a wide variety of other management functions.

Resource: The forces, materiel, and other assets or capabilities apportioned or allocated to the commander of a unified or specified command. (Joint Publication 1-02)

Resource Description Format (RDF): RDF is a general blueprint for describing a Web site's metadata, or the information about the information on the site. It provides interoperability between applications that exchange machine-understandable information on the Web. RDF details information such as a site's sitemap, the dates of when updates were made, keywords that search engines look for and the Web page's intellectual property rights. Developed under the guidance of the World Wide Web Consortium, RDF was designed to allow developers to build search engines that relay on the metadata and to allow Internet users to share Web site information more readily. RDF relies on XML as an interchange syntax, creating an ontology system for the exchange of information on the Web.

Rules of Thumb: Shortcuts to solutions to new problems that resemble problems previously solved by experienced workers; heuristics.

Search & Deliver: Bringing knowledge to teams and communities through portals built on personalized cross-enterprise search and delivery technologies.

Search Engine: Software that helps a person find a piece of information. A public search engine such as Google or AltaVista uses programs that visit each web site on the Internet and copy each page into a database on its server. A user then asks the program to look through the database for a word the user enters. The programs that visit each site are called spiders or robots, and visiting each site is called crawling.

Signature Skill: An ability by which a person prefers to identify himself or herself professionally.

Social Capital: The intellectual capital resulting from communications, collaboration and interpersonal relationships. It includes human and virtual networks, relationships and the interactions across these networks built on those relationships.

Space Domain: The use of the medium of Space to provide U.S. Army warfighting capabilities including command, control, and communications and missile defense.

Space is a medium within which military activities shall be conducted to achieve U.S. national security objectives. The ability to access and utilize space is a vital national interest.

Space is a critical Enabler to the Objective force. AKEA enables horizontal integration of Space capabilities across all elements of combat power; AKEA serves as a compass for the Army Space Community as it conceives, develops and modernizes space support for the objective force; and AKEA supports the vertical integration the ground segment of Space Control.

Supply Chain Management (SCM): A practice in which business is conducted with a complete and integrated view of materials and information from the supplier's supplier, through the internal enterprise, to the customer's customer. Collaboration between these entities is a key enabler of effective supply chain management.

System: For the purpose of reporting to the Army Information Technology Registry, the terms "application" and "system" are used synonymously - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. In other words, the application of IT to solve a business or operational problem. System/Application owners will have to use judgment in how to report "systems of systems;" either as a single or separate entries.

Systems Administrator: An individual responsible for maintaining a multi-user computer system, including a local-area network (LAN), wide-area network (WAN), Telephone system, or voice-mail system. Responsible for the day-to-day operations and maintenance of the servers, operating systems, and supporting infostructure.

Systems Architecture: A description, including graphics, of systems and interconnections providing for or supporting warfighting functions. It defines the physical connection, location, and identification of key nodes, circuits, networks, and warfighting platforms and specifies system and component performance parameters. It is constructed to satisfy operational architecture (OA) requirements per standards defined in the technical architecture (TA). It shows how multiple systems within a subject area link and interoperate and may describe the internal construction or operations of particular systems.

System Owner. For the reporting purposes, the owner of a system or application is the MACOM or HQDA functional proponent responsible for the funding, fielding and maintenance of the system. In the case of these responsibilities being spread across several organizations, the funding organization is the owner unless all the organizations agree on a different owner. If a system is funded by multiple organizations, they must choose a single System Owner.

Tacit Knowledge: Personal knowledge that resides within an individual that relies on experiences, ideas, insights, values, and judgments. Knowledge that is resident within the mind, behavior, and perceptions of individuals. Knowledge developed and internalized by an individual over a long period of time incorporating so much accrued and embedded learning that its rules may be impossible to separate from how an individual acts.

Tactical Communications Domain: Collection of communications related requirements and systems from the STEP/TELEPORT to the foxhole.

Taxonomy: The logical, hierarchical classification of objects and relations among them. The result is the classification scheme for the knowledge accessible through a given system or interface. The scheme divides the knowledge into ordered groups or categories.

Team: A collection of individuals who are working together towards a common goal and who share a common, meaningful purpose.

Teamware: A category of software that enables colleagues, especially geographically dispersed colleagues, to collaborate on projects. Typically, teamware uses the Internet and the World Wide Web to facilitate communication among the team.

Technical Architecture: A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. It identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems on which engineering specifications are based, common building blocks are built, and product lines are developed.

The Army Enterprise Architecture: The overarching architecture for the entire Army Enterprise including the operational requirements for combat, combat support, and business/functional areas; the infostructure to ensure storage and transmission of the related data; and the protocols and standards to ensure that the systems and systems-of-systems can exchange data within the Army and between the Army and other Services, DoD, and other entities including coalition partners. Development of this architecture is dependent upon multiple organizations using a standard set of rules and procedures for data development, storage, and manipulation that will enable data sharing.

The Army Infostructure: The information technology (computers, software, architecture, security, communications, programs and facilities) required to support the network-centric Army.

Topic Area: A cross-functional grouping of business areas (grouping of processes). Examples of topic areas are finance, program management, administration, and research.

Training Domain: A process of instruction that follows the soldier from boot camp to retirement. Army training tools & architectures are changing to support the needs of the Objective Force. Training includes schoolhouses, independent study, on-the-job-training (OJT), field training and exercises, war gaming, assignments oriented training (AOT). Within the Army Knowledge Enterprise training can also be web-enabled training or it can use collaborative environments and distributed simulations. Army Knowledge On Line will be used as a portal for AOT. Soldiers receive common individual & collective training at various phases of their careers.

Units of Action: The tactical warfighting echelons of the Objective Force.

Units of Employment: The basis within the Objective Force of combined arms air-ground task forces. They resource and execute combat operations; designate objectives; coordinate with multi-service, interagency, multinational and non-governmental activities; and employ long range fires, aviation and sustainment. They also provide command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) and tactical direction to units of action.

Vertical Portal: A vertical portal is a portal that serves a specific community of interest. An organization may have several vertical portals, but will probably have only one horizontal portal.

Virtual: Indicates simulation technology that enables the user to cross boundaries and experience something without needing its physical presence, as virtual theme parks, virtual communities.

Virtual Team: A geographically dispersed team that brings together its members through modern communication and collaboration technology.

Web Browser: A software application used to locate and display web pages.

Web-Enable: System runs on a JTA-Army –compliant web browser without the need to preload any other software onto the client prior to first web access (software may be downloaded as part of the login).

Webify. This term encompasses both Web-enabling and AKO Linking. A fully webified system is both Web-Enabled and AKO-Linked.

Work Cell: A collection of roles in an organization that crosses functional barriers.

Workflow: A system whose elements are activities, related to one another by a trigger relation, and triggered by external events, which represent a business process starting with a commitment and ending with the termination of that commitment.

XML: Extensible Markup Language. XML is a subset of Standard Generalized Markup Language (SGML) that is used for putting structured data in a text file.