

2008-2015

ARMY CIO/G-6 CAMPAIGN PLAN



DELIVERING A JOINT NET-CENTRIC INFORMATION ENTERPRISE



SOLDIERS * FAMILIES * ARMY CIVILIANS

ARMY STRONG.



A MESSAGE TO OUR PARTNERS

FROM MR. VERNON M. BETTENCOURT, JR.



Vernon M. Bettencourt, Jr.
Acting Chief Information Officer, G-6

America's Army is continuing its transformation journey to remain the preeminent landpower on Earth; ready to meet and relevant to the challenges of a dangerous and complex 21st Century security environment. Our Vision is to deliver a joint Net-Centric information enterprise that enables Warfighter decision superiority.

Army is simultaneously improving its information infrastructure while re-engineering processes to improve the way we conduct and support war and keep the peace. We are transforming our infrastructure to better support mobile, modular forces at installations, depots, arsenals, off-installation Army activities, National Guard Joint Force Headquarters, and at Armories and United States Army Reserve Centers and facilities throughout the information network that connects them. We are doing this while maintaining our commitment to more efficiently support the varied demands of operational and institutional processes, and keeping a mission results focus ensuring that deployment requirements and global commitments of the security environment drive the transformation Army-wide.

We are also doing this in the face of ever-increasing threat to the LandWarNet and the IT-focused capabilities it provides. These threats have a significant scope and breadth. At the lower end of the threat spectrum are lone or small groups of amateurs using common hacker tools and techniques in an unsophisticated manner without significant support. At the high end are those threats associated with offensive Information Operations, especially computer network attacks (CNAs), using state-of-the art tools and covert techniques conducted in coordination with military operations. These high-end threats are assessed to be driven by the objective to deny the Army the advantage of a joint Net-Centric information enterprise and Warfighter decision superiority.

The Army CIO/G-6 Campaign Plan identifies the Vision, Mission, Goals, and Core Information Management/Information Technology (IM/IT) Capabilities that support the DoD, Joint and Army Strategic guidance. Additionally, transitional roadmaps for guiding our transformation in service to the warfighter are provided in a restricted appendix that can be accessed behind Army Knowledge Online-SIPRNet (AKO-S). The primary focus of this document is to outline the Army IM/IT strategy integrating the efforts of the CIO/G-6, the Direct Reporting Unit (DRU) NETCOM/9TH SC(A), the United States Army Signal Center and School at Fort Gordon as well as the Reserve Components in support of the Army Campaign Plan. The Army CIO/G-6 Campaign Plan is a long-term plan from the current time through 2015 that provides the Army with the strategic direction for IM/IT capability building in support of the Warfighter. The critical enabler for this plan is the prioritization of our resources for IM/IT investments against this strategy – a strategy that must be flexible, incorporating improved technology and leveraging process management and improvement whenever they benefit Army and can achieve Joint mission results. We are striving to become a service-based organization focused on providing world-class service to the Warfighter and those who support them. A culture of empowerment and stewardship should focus on the Soldier and the battlefield, even as we improve business processes. ★★★

TABLE OF CONTENTS

Introduction	4
Army Strategic Alignment.....	4
Enterprise Architecture	6
Army IM/IT Enterprise Architecture	6
LandWarNet Vision	7
Information Superiority	7
LandWarNet Core Capabilities	8
Army CIO/G-6 Core Competencies	8
Army CIO/G-6 Vision	9
Mission	9
Strategic Goals.....	9
Strategic Goal 1	10
Connect.....	11
Network Operations (NETOPS)	11
Strategic Goal 2	12
Data.....	13
Services	13
Applications	13
Governance/Standards	14
Strategic Goal 3	16
Identity	17
Strategic Goal 4	18
Applications	18
IT Portfolio Management Structure: Mission Areas and Domains.....	19
EIEMA Construct.....	19
Financial Resources Alignment	21
Strategic Goal 5	22
Human Resources Alignment.....	23
Strategic Goal 6	24
Implementation Strategy - CIO/G-6 500-Day Plan	24
Performance Reviews.....	24
Process Improvement	25
Strategic Communications.....	25
Program Executive Office, Enterprise Integration System (PEO EIS) Oversight	25
Army Chief Information Officer (CIO) Executive Board.....	27
Appendices	28
Take Aways	30

INTRODUCTION

Our Army faces an ever-changing and evolving enemy and we must be able to respond rapidly to defeat emerging threats. The current operating environment and projections of persistent conflict dictate the need to rapidly develop capabilities for both the current and future forces. Further, the rapid pace of Information Technology (IT) change will create opportunities necessitating transformation of our development and procurement process to exploit these opportunities and effectively integrate them into the force. This transformation must include the ways and means to identify and mitigate risks associated with procurement and acquisition in the global IT market space.

The Global Information Grid (GIG) is the Department of Defense’s approach to information and decision superiority – a key to the National Military Strategy for continued information dominance. This decision superiority is based on shared information across the Army and with Joint, Interagency, and Multi-National coalitions and allies. LandWarNet is the Army’s portion of the GIG and; therefore, key to Army’s decision superiority.

LandWarNet has been described as the Army’s Battle Command and GIG-derived, orders-based, capabilities focused system of systems, train as you fight, and enhanced orders process. LandWarNet enables information-based Joint, Interagency, multi-national, civil defense, Warfighting and support operations, regardless of Joint Operational Phase, operational urgency, or the battlespace circumstances of its authorized users.

Army Strategic Alignment

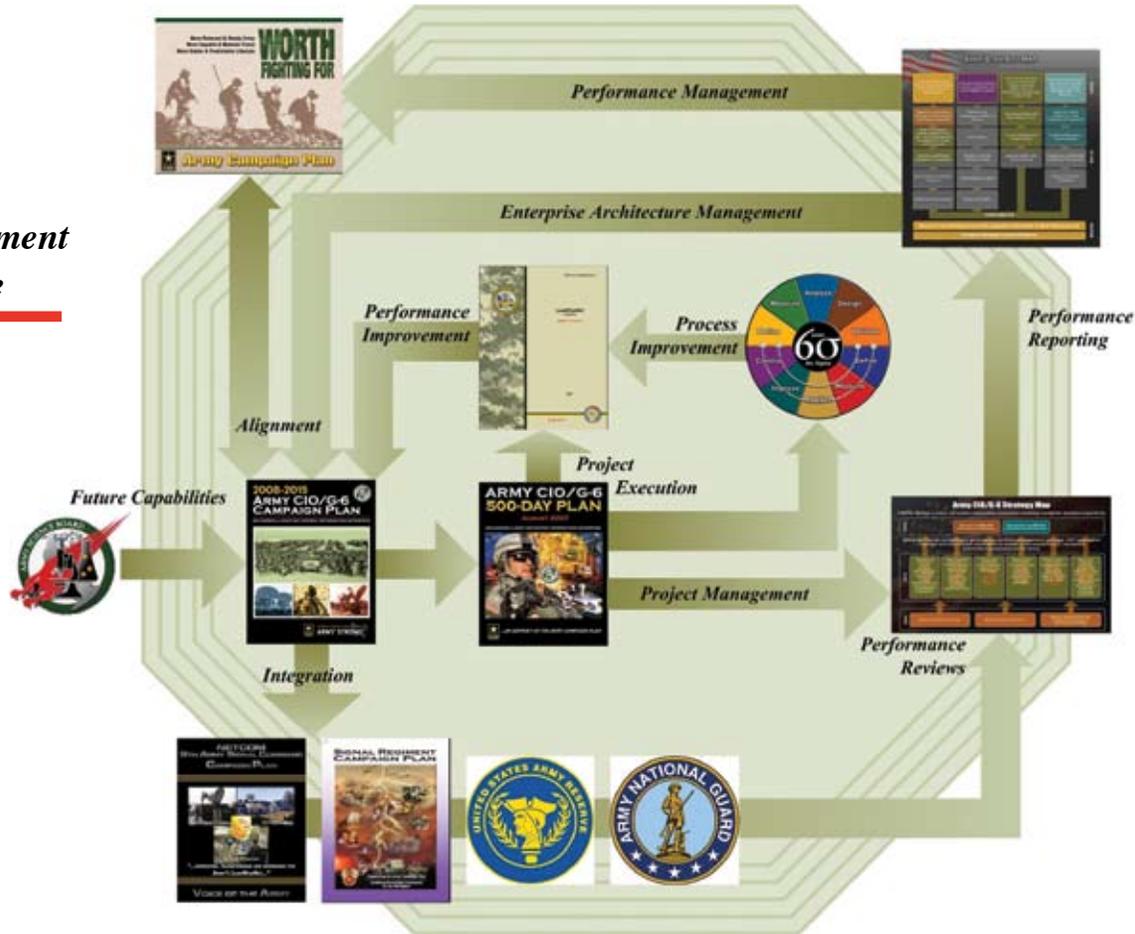


The IM/IT strategy as outlined in this document iterates the Army CIO/G-6 Vision, and Mission, six Strategic Goals and Core LandWarNet Capabilities that drive the Army’s long-term IM/IT strategy from 2008 through 2015. This Plan details the long-term specified and implied missions in the Army Campaign Plan, as well as OSD and Joint strategic guidance. The CIO/G-6 Vision, Mission and six Strategic Goals directly support the Secretary of the Army’s nineteen Strategic Initiatives and the seven Army Initiatives.

This Plan is intended to be the integrating instrument between the CIO/G-6, NETCOM/9TH SC(A), the Signal Center as well as the Army Reserve and the Army National Guard, providing the long-term direction for the Army’s IM/IT Strategy to support the Army.

The strategy management lifecycle begins with the alignment of the CIO/G-6 long-term vision in the CIO/G-6 Campaign Plan to the larger Army-wide specified and implied missions in the Army Campaign Plan and taking into consideration future capabilities and trends identified in the various Army Studies conducted by the Army Science Board and Rand Corporation on behalf of the Army. In addition, the Army CIO/G-6 works in collaboration with the DoD CIO to incorporate guidance in the QDR and Strategic Planning Guidance. From the long-term plan laid out in the CIO/G-6 Campaign Plan, the short-term implementation plan is developed and iterated in the CIO/G-6 500-Day Plan and the supporting plans of NETCOM/9TH SC(A), the Signal Center, and the Reserve Components. During performance reviews, the CIO/G-6 will monitor the implementation status and performance metrics of the various IM/IT initiatives projects and programs. The results of these performance reviews feed the Army's Strategic Management Systems allowing Army senior leaders to view the IM/IT performance in context with the rest of the Army's efforts to execute the Army Campaign Plan. In this way the effectiveness of the strategy can be evaluated and necessary course corrections in the form of changes to the strategy and process improvement efforts undertaken as needed. Completed projects result in process improvements that impact the way the LandWarNet operates, and result in need for new or revised strategies to affect change in the new operational situation completing the cycle of strategy development.

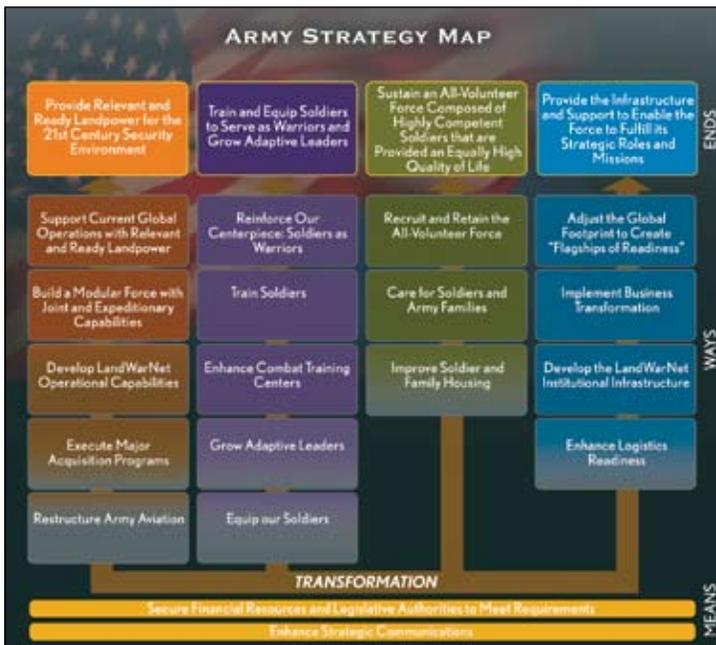
Strategy Management Lifecycle



The Army's portion of the Global Information Grid, the LandWarNet network, has many facets with multiple Army Staff elements responsible for the planning, designing, developing, training and operating. Integrating these efforts requires synchronization to provide a unified picture of how the various pieces fit together. Managing the strategy to accomplish this is a cyclical and iterative process.

The Army CIO/G-6 Campaign Plan serves as the unifying strategic umbrella for the multidimensional effort to develop, implement and operate the LandWarNet. Specific objectives related to LandWarNet training and operational efforts are documented in the following formal planning documents:

- NETCOM 9th Army Signal Command Campaign Plan, Version 2.0, 3 November 2006
- Signal Regiment Campaign Plan, March 2007



Enterprise Architecture

Enterprise Architecture is the principal driver in the process of aligning the Army’s strategic vision and goals with information technology by depicting the Army as it is today and as it is envisioned in the future.

The Army Enterprise Architecture can be defined as (1) a strategic information asset base, which defines the mission (connect and identity); (2) the information necessary to perform the mission (data); (3) the technologies necessary to perform the mission (services and applications); and (4) the transitional processes for implementing new technologies in response to changing mission needs (governance and standards) which includes (A) a baseline architecture (current force); (B) a target architecture (future force); and (C) a sequencing plan (roadmaps).

The Army Enterprise Architecture is the translation of the Army vision and strategy to enable effective enterprise transformation. The CIO/G-6 has established the Army Strategy Map, the Army’s strategic execution plan as iterated in the Army Posture Statement, as the authoritative framework for the Army Enterprise Architecture.

Whereas the Army Enterprise Architecture provides the “big picture” view across the Army Enterprise; Segment Architectures provide a more detailed and results-oriented view; they are a transition bridge establishing traceability between strategic goals and Information Technology solutions.

A Segment Architecture (1) is a detailed, results-oriented architecture and a transition plan for a segment of the enterprise; (2) comprises a series of work products describing baseline architecture, target architecture and a transition plan; (3) work products that document segment-level change drivers, describe baseline and target performance, business data, services, and technology architecture, and provide a roadmap to enhance business operations and achieve measurable performance improvements; and (4) has a segment transition plan which feeds the enterprise transition plan and should influence the enterprise investment portfolio.

Segment Architectures focus on major areas of the Enterprise (lines of business) to enable performing operations and customer service more efficiently and effectively. Solution Architectures define the delivering capabilities that enable operational outcomes by addressing gaps on which the segment (performance or services) relies. The end state for the Army’s architecture strategy is the full implementation of Services Oriented Architecture.

Army IM/IT Enterprise Architecture

The CIO/G-6 has established the Army CIO/G-6 Strategy Map as the authoritative framework for the Army IT Enterprise Architecture that supports the Army Enterprise Architecture. The CIO/G-6’s first and most significant means of developing LandWarNet will be accomplished through the development and enforcement of the Army Enterprise Architecture.

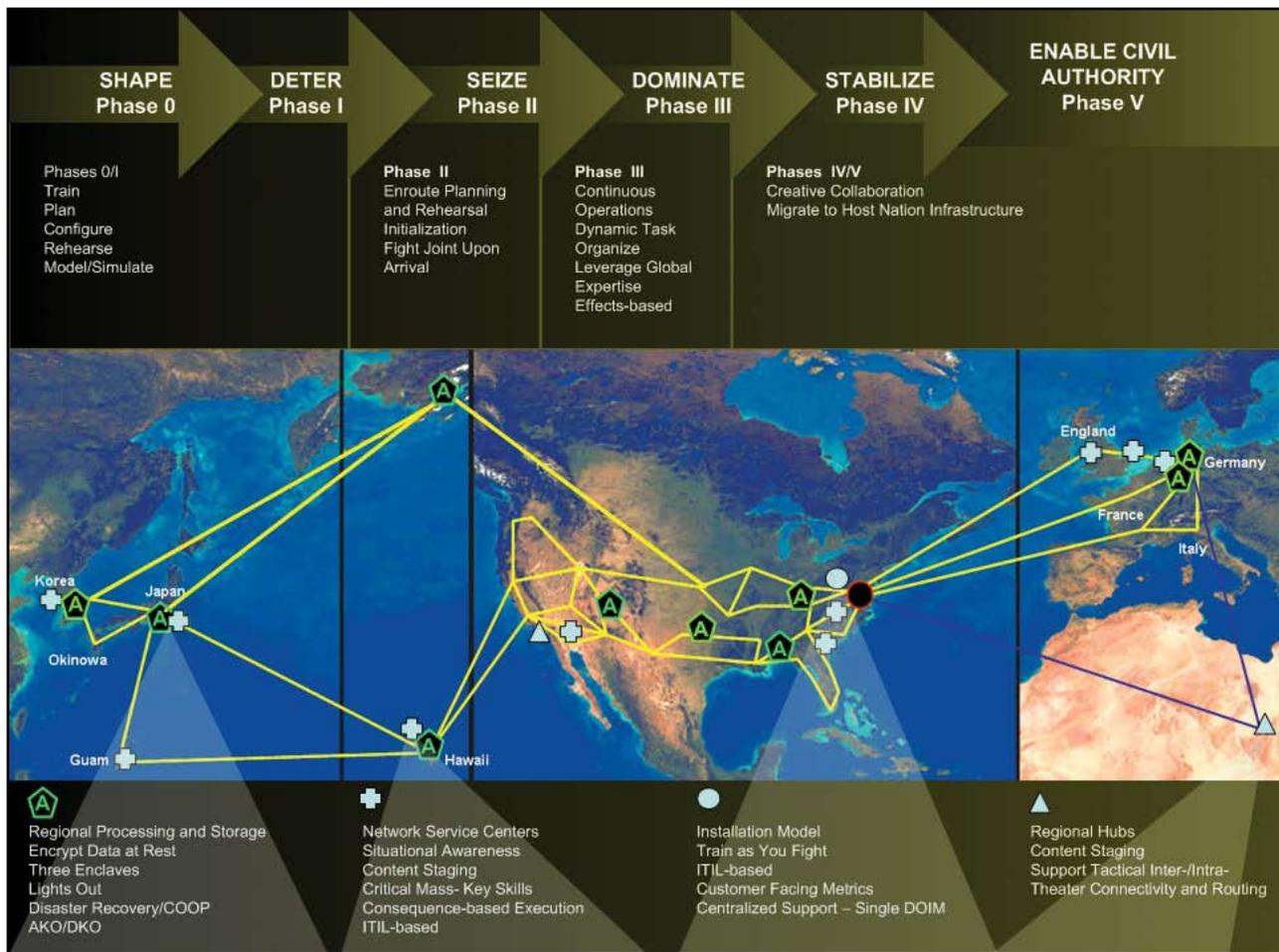


LANDWARNET VISION

The LandWarNet vision is to provide operational capabilities to the Warfighter during all six Joint Operational Phases (as illustrated below). To meet the Warfighters’ operational requirements the CIO/G-6 in collaboration with HQDA Staff, Army Commands, Army Service Component Commands, Direct Reporting Units, United States Army Reserve, and the Army National Guard will provide LandWarNet operational capabilities and LandWarNet institutional infrastructure in support of the Warfighter and the core business processes that support the Warfighter.

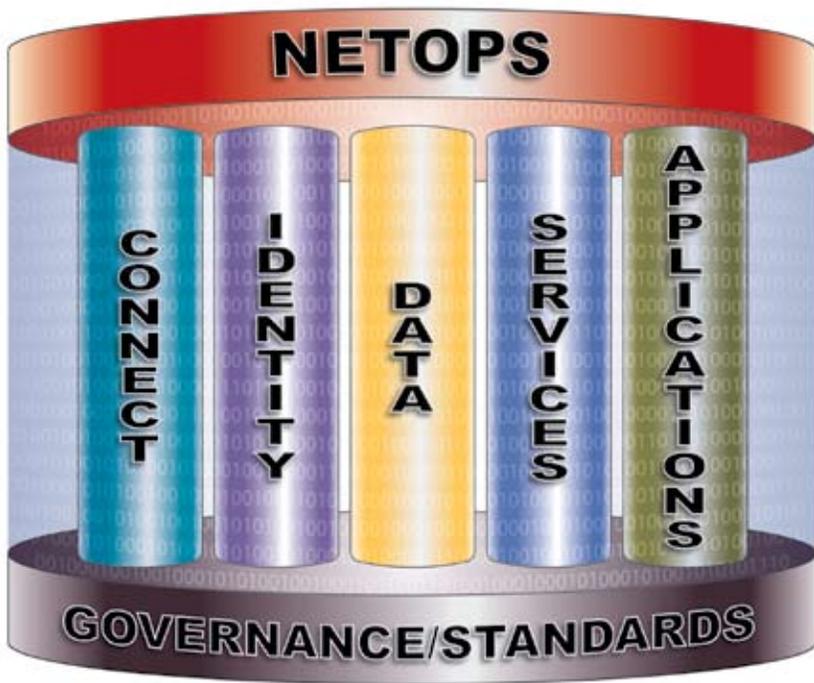
IM/IT Capability

Requirements for LandWarNet



Information Superiority

The Army has made significant strides in Information Assurance (IA) efforts to secure Cyberspace with expanded access to encryption software and robust identity management programs with two-factor authentication processes. Information Assurance will continue to be a priority and will be an element of the larger emerging mission of Cyberspace Operations. The Army, in synchronization with DoD and the Joint Staff, must aggressively address the new and emerging threats to our networks and information and develop capabilities that protect our interests in Cyberspace. Information Superiority will require greater reliance on all-source intelligence to define threats to LandWarNet capabilities and to work toward predictive analysis to enable scarce IA resources to be deployed at the right place at the right time. As Cyberspace is defined and operational missions emerge the Army will develop comprehensive plans and take aggressive actions to protect and defend our LandWarNet capabilities in collaboration with DoD in support of the DoD enterprise.



LandWarNet
Core Capabilities

The LandWarNet Core Capabilities depicted in the graphic at the left (Connect, Identity, Data, Services, Applications, NETOPS and Governance/Standards) provide the over-arching construct that will be used throughout this Campaign Plan. These core capabilities are the “Ways” that will enable achieving the LandWarNet Vision and the two “Ends” in the CIO/G-6 Strategy Map; Provide LandWarNet Operational Capabilities and LandWarNet Institutional Infrastructure. Each of the LandWarNet Core Capabilities will be discussed in detail in the subsequent sections of this document as the focus of our strategic goals.

Army CIO/G-6
Core Competencies

The Army CIO/G-6, in collaboration with the Deputy Under Secretary of the Army for Business Transformation (DUSA-BT), continues to implement business transformation changes to continuously improve the quality of support to our Army. The graphic at the right depicts the CIO/G-6 value stream or core competencies (Strategy, Policy, Architecture, Investment, Acquisition Oversight, Operations, and Governance and Compliance) that are the focus of our business transformation efforts. During the period covered by this plan the CIO/G-6 will transform from a primarily functionally based organization to a process-based organization and finally to a service-based organization. In this transformation the CIO/G-6 and the Signal Regiment will mature its service delivery from best effort to a quality of service model.



Army CIO/G-6 Vision, Mission & Goals

The next section of the CIO/G-6 Campaign Plan will lay out the Army CIO/G-6 Vision, Mission, and Goals to achieve the over-arching LandWarNet vision and provide the detailed ways and means to achieve the ends in the Army CIO/G-6 Strategy Map: LandWarNet Operational Capabilities and LandWarNet Institutional Capabilities. This will be achieved by building and improving the LandWarNet Core Capabilities.

ARMY CIO/G-6 VISION

In support of LandWarNet, the Army CIO/G-6 Vision is to: Deliver a joint Net-Centric information enterprise that enables Warfighter decision superiority.

MISSION

Provide architecture, governance, portfolio management, strategy, command, control, communications, computers and information technology (C4IT) acquisition oversight and operational capabilities to enable joint expeditionary Net-Centric information dominance for the Army.

STRATEGIC GOALS

The CIO/G-6 Vision and Mission are supported by six enduring Strategic Goals:

- [Strategic Goal 1](#): Develop and maintain a secure, seamless, interdependent LandWarNet network by leading development and enforcing the use of integrated enterprise architecture.
- [Strategic Goal 2](#): Lead enterprise integration to achieve decision superiority by transforming processes, applications, and data into net-centric capabilities across the Army.
- [Strategic Goal 3](#): Protect and defend the Army's systems, networks, and information.
- [Strategic Goal 4](#): Ensure Army information management and information technology investments maximize Joint and Army capabilities.
- [Strategic Goal 5](#): Develop the Army's information management and information technology knowledge and skills to support mission needs.
- [Strategic Goal 6](#): Deliver an integrated enterprise strategy that influences joint and Army use of information management and information technology in furthering the warfighting capabilities.



STRATEGIC GOAL 1

DEVELOP AND MAINTAIN A SECURE, SEAMLESS, INTERDEPENDENT LANDWARNET NETWORK BY LEADING DEVELOPMENT AND ENFORCING THE USE OF AN INTEGRATED ENTERPRISE ARCHITECTURE.

The Clinger Cohen Act mandates the Army CIO's responsibility to develop and enforce an Enterprise Architecture for the Army. The CIO/G-6 vision of LandWarNet is one virtual network with trusted interoperability between Combatant Commands (COCOMs), Army Service Component Commands (ASCCs), HQDA, and Reserve Components. Joint interoperability is mandated by DoD, and Presidential Decision Directive 12 (HSPD-12) requires information sharing between federal agencies. The Global Information Grid (GIG) is the transport layer for LandWarNet. Currently LandWarNet has two components; Institutional and Operational. The primary focus of the CIO/G-6 has been to ensure LandWarNet Operational Capabilities are delivered to Warfighters, this will remain the CIO/G-6's top priority, however, to achieve the CIO/G-6 vision of one virtual network that has end to end interoperability, the same focused effort must be applied by Army stakeholders in integrating the LandWarNet Institutional Network. This is critical in order to achieve support to Warfighters and those who support them during all Joint Operational Phases (Shape, Deter, Seize, Dominate, Stabilize, enable Civil Authority).

END STATE:

Although the full implementation of WIN-T is not scheduled until 2025, by 2015 today's disparate communications solutions that provide dedicated communications for specific communities/applications will be converging into a single integrating framework creating a network of networks to meet Future Combat Systems (FCS) Warfighter Battle Command requirements and the requirements of the institutional processes that support them. If the Army is to fully enable the FCS, we must begin now to implement these capabilities by spinning out information technologies that can be inserted into the Army today to provide our Warfighters with enhanced capabilities as soon as they are available. WIN-T will mandate the standards and protocols for applications and network hosts, to provide the most responsive and effective common services within a Services Oriented Architecture. WIN-T must be as mobile and agile as the warfighting maneuver forces. WIN-T will provide network access for the commander and leaders to utilize automated, collaborative decision support tools that enable the orders

process and provide commanders with the capability to train as they fight and to effectively plan, synchronize and virtually rehearse missions during all Joint Operational Phases. In the operational environment, WIN-T will achieve full On-The-Move capability within the Brigade Combat Team and Support Brigades down to the Battalion and Separate Company level including all sensors and munitions. LandWarNet will have achieved Everything over Internet Protocol (EoIP) by providing voice video and data to the Army utilizing Internet Protocol. In the Institutional environment within CONUS, LandWarNet will achieve Enterprise interoperability as envisioned. Today the Army has thirteen Active Directory (AD) forests in CONUS with no trusted relationships between these forests.

To achieve Army enterprise level interoperability the CIO/G-6 must work in collaboration with the Installation Management Command (IMCOM) to successfully implement the Single DOIM on Army Installations in order to attain a level of standardization to achieve interoperability between Army Commands and activities. Concurrently, the Army CIO/G-6 must work in collaboration with the United States Army Reserve and the National Guard to integrate Active and Reserve Components and achieve true enterprise network services as well as preserve the unique requirements of all stakeholders. By 2015, the Army will be operating its network services from Network Service Centers. Network services will mature from a best effort level of service to guaranteed levels of service to customers. Fixed based information infrastructure improvements will be accomplished across all Army installations and extended to United States Army Reserve and National Guard infrastructure to include the extension of SIPRNet services to Active and Reserve Component units down to Battalion and Separate Com-



STRATEGIC GOAL 1

pany level by 2015. An Enterprise level wireless capability will be deployed across the Army providing NSA approved, secure connectivity to LandWarNet.

By 2015 space-based, satellite capabilities will be augmented with Airborne layer capabilities to provide a minimum level of redundant capabilities required for assured levels of service to warfighters in operational theaters. Currently space-based capabilities are heavily reliant on commercial satellites (80%). By 2015, Army Enterprise Space-based capabilities will be expanded to include increased broadband and narrowband capabilities and less reliability of commercial-based satellites to achieve 50% commercial and 50% MILSATCOM.

Connect



Joins, or unites users, their platforms, their sensors, and their information in order to enable information exchange and global collaboration for Battle Command and Business Enterprise support to the Warfighter.

In the recent past, the primary focus and message of Army Communications has centered on developing the capability to “connect” by developing, expanding, upgrading, extending the network infrastructure and transforming the Signal Forces to support modularity. The Army’s accomplishments to provide the capability to connect via the network have been significant and successful: **Joint Network Node – Network (JNN-N)** – now the primary tactical communications network provider for the Army and referred to as Warrior Information Network – Tactical (WIN-T) Increment One; **Satellite Communications (SATCOM)** – combines a dual effort to expand the military constellation of satellites while at the same time expanding the spectrum of usable frequencies on the existing satellites in orbit; Fixed Regional Hub Nodes (FRHN) – in CONUS, Southwest Asia, Europe, and the Western Pacific provide world-wide support to satellite communications in support of deploying and deployed forces. The **Installation Information Infrastructure Modernization Program (I3MP)** is providing necessary infrastructure upgrades with the goal of making Army installations “Docking Stations” allowing Soldiers to train as they will fight with the same equipment and capabilities in garrison as they use during operational deployments. This support must be expanded to include the same capabilities to the Warfighter that are available in the deployed Theaters of Operation; for example,

the availability of SIPRNet to Battalion level in garrison. Plans for future advances to the network center on the **Warfighter Information Network – Tactical (WIN-T)** – the cornerstone tactical communications system that will establish a single, synchronized framework creating a “network of networks” by combining the disparate systems (MSE, TRI-TAC, JNN, BFTs, Trojan Spirit, etc.) into one, standardized architecture. Although some view the network in two segments; institutional (CONUS) and Operational (Deployed Theaters - OCONUS) the reality is that the Network must be end-to-end providing seamless support to the Warfighter during all six Joint operational phases and providing global reach for the business processes that are critical to support the Warfighter. The Networks Service Center which is enterprise focused and regionally based is the foundation for creating a Global Collaborative Environment and a strong network required to “connect.”

Network Operations (NETOPS)



LandWarNet core capabilities: Connect, Identity, Data, Services, and Applications are supported and protected by pervasive and rigorous Network Operations (NETOPS). The CIO/G-6 has the responsibility for conducting Network Operations within the Joint framework to enable assured information dominance and protected network-centric capabilities across the force. The CIO/G-6 provides management and oversight of this mission area. NETCOM/9TH SC(A), the CIO/G-6 Direct Reporting Unit (DRU) executes this operational mission for the Army. Specifically the following initiatives are executed by NETCOM/9TH SC(A):

- Enforce Unity of Command and achieve Unity of Effort across the Army Network-Centric Operational Environment (NCOE).
- NCOE situational awareness and Visualization for the LandWarNet to include JTF-GNO.
- Strengthen Network Security and Information Assurance (IA).
- Establish a Fully Functional Army Global Network Operations and Security Center (A-GNOSC) and supporting NOSCs capable of executing full spectrum of NETOPS.
- Ensure NETOPS is Pervasive across all layers of the Net-Centric Operational Environment (NCOE).

The NETCOM/9TH SC(A) Campaign Plan contains extensive strategic and tactical details about these initiatives.

STRATEGIC GOAL 2

LEAD ENTERPRISE INTEGRATION TO ACHIEVE DECISION SUPERIORITY BY TRANSFORMING PROCESSES, APPLICATIONS, AND DATA INTO NET-CENTRIC CAPABILITIES ACROSS THE ARMY.

While the Network is one of the critical enablers and past efforts have been clearly focused on enhancing this capability, the Army must balance those efforts with the critical mission of enabling information exchanges. Building a Network Service Center with a Joint, Interagency, Multi-national and Coalition



Global Collaborative Environment requires the synchronization and implementation of the DoD, Joint, and Army data strategies. These data strategies are visualized with the Army's effort of implementing Area Processing Centers and meets the Army's goal to make data visible, accessible, understandable, trusted, interoperable responsive to user needs and institutionalized. Successful information sharing requires a major cultural shift within the Army and DoD. There is a mind-set that information requires "ownership;" this mind-set needs to shift to a culture that has a mind-set of "stewardship." The most leading edge information technologies, transformed processes and policies will not lead to the achievement of this goal without Army stakeholders, and customers embracing stewardship. One of the Army's primary service delivery successes and key to access to information management services is the Army Knowledge Online (AKO) portal. AKO is the largest and most mature of all DoD portals; it offers many applications with features

and capabilities that are not available on other DoD portals and has been identified as the best-of-breed portal in DoD. These features and capabilities include instant messaging, e-mail, education, computer based training, chat rooms, video messaging, file storage and sharing and more. As a result of AKO's reputation and success, other DoD Components, Services, and Agencies desire to leverage AKO capabilities to establish web-based workspaces and communities by which to improve the way information and knowledge is managed with their respective organizations. Since its inception, Army Knowledge Online has increased communication and knowledge management across the Army. Its strong ties to serving the individual Soldier have enabled it to become a relevant and highly used tool.

END STATE:

By 2015, the Army, in synchronization with Joint and DoD data strategies, will have implemented a Services Oriented Architecture (SOA) nested within Federal, DoD, and Joint architecture frameworks. The Army will implement its approved data strategy to include: making data visible (advertise information holdings – tag data), making data accessible (web enable sources, remove impediments – need to share), and making data understandable (Communities of Interest – shared vocabularies) for searches that enable analysis; forward stage content to support time sensitive operations; mature data to drive continued analysis and creation of knowledge to integrate into estimates, plans and orders. By 2015, data strategy implementation will enable applications to become part of the services layer. The following services will be enabled for the Warfighter; providing Soldiers data beyond local capabilities; the ability to tailor IM/IT capabilities based on local requirements; the capability to store, categorize and discover relevant information for analysis and mission development; the capability to automate the timely, prioritized, dissemination of information to those who need it across multiple applications to achieve the vision of a global collaborative environment at all echelons of the Army.

STRATEGIC GOAL 2

Data



Standardizing data is the key to interoperability and collaboration in a global environment. The Army's goals to make data visible, accessible, understandable, trusted, interoperable, responsible to user needs, and institutionalized have never been more important nor the need to implement more urgent. The Army's Net-Centric data implementation strategy is comprehensive and is

making progress. Communities of Interest (COIs), collaborative groups of users and developers needing to exchange information have been and are continuously being formed to jointly make decisions and come to agreement on their data exchange needs and policies in support of Blue Force Tracking, Biometrics, Data Initialization, Global Strike and the Warfighter Mission Area, among others. In support of COIs, the Army has established the Net-Centric Data Center of Excellence to provide stakeholders with expert subject matter support, data engineering services and data products. The Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) is being implemented and tested in support of the Multilateral Interoperability Program (MIP) to achieve international interoperability of Command and Control Information Systems (C2SI) at all levels from corps to battalion and the Data Migration Plan will lay out a strategy for federated models.

The first step in realizing the end-state for the data strategy is to focus on eXtensible Markup Language (XML), the standard from which multiple supplementary standards have evolved to form the core representation (model) architecture. XML is modular, and the use of XML within Web services allows for the consumption of XML data from any model: JC3IEDM, Geography Markup Language (GML), or a DoD agreed upon common standard.

Services



We are striving to focus on the improvement of information technology services to our Warfighter and Business leaders who support them. For the Army, migrating to a Service Oriented Architecture (SOA) is critical in transitioning from legacy services to Future Combat Systems (FCS). SOA is an architectural approach capitalizing on the

deployment of loosely coupled services with defined interfaces to support end users and business processes. Implementation of the SOA required extensive planning and testing to assure that all aspects of the selected systems are interoperable and compatible. Within the Army, Software Blocking, an evolutionary method of delivering system of systems integration for a pre-determined timeframe (block), provides a rigorous and comprehensive methodology to make the plan of the SOA a reality. It provides a robust method of integration testing designed to replicate the employment of systems in a deployed arena, therefore ensuring interoperability and deployment of comprehensive capabilities in the hands of the warfighter.

As AKO matures into Defense Knowledge Online (DKO), its capabilities will continue to enhance the use of shared IT infrastructure facilitating best practices in knowledge sharing, management, and collaboration. When DKO reaches its Full Operational Capability, DKO is projected to provide an estimated five million users with a secure, adaptive, and agile information sharing environment to Warfighters, policy makers and support personnel alike. Army Knowledge Online will continue to be the foundation to evolve DKO to a Service Oriented Architecture. As the Army migrates to a Service Oriented Architecture applications will become services in the SOA framework.

Once XML has been achieved, the Army SOA efforts will be directed at the service orientation of the following web services: loose coupling, service contracts, autonomy, abstraction, reusability, composability, statelessness, and discoverability. SOA will be critical to transitioning from Army Battle Command Systems to Future Combat Systems.

Applications



Transforming applications to serve the Warfighter will be accomplished by the Mission Areas and Domains engaged in application development and enhancement, however the standards to which those applications must be developed and enhanced to permit them to optimally become part of LandWarNet's net-centric, end-to-end, global collaborative environment will be established by the CIO/

G-6 and then tested against during the Software Blocking Implementation phases at the Combined Technical Support Facility.

STRATEGIC GOAL 2

Governance/Standards



LandWarNet core capabilities: Connect, Identity, Data, Services, and Applications are supported and enabled by unifying standards and effective governance.

Title 40, Subtitle III/Clinger-Cohen Act

The Title 40/CCA generated a number of significant changes in the roles and responsibilities of various Federal agencies in managing acquisition of IT. It elevated oversight responsibility to the Director, OMB, and established oversight responsibilities to the departmental CIO offices. In the Department of Defense, the Assistant Secretary of Defense for Networks & Information Integration has been designated as the DoD Chief Information Officer and provides management and oversight of all DoD information technology, including national security systems.

The Act places responsibility for “developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture” onto the agency CIO. In practice, the term information technology architecture is now known as Enterprise architecture.

The Clinger-Cohen Act (Title 40, Subtitle III) mandated that all major Federal Agencies establish the position of Chief Information Officer (CIO). The Secretary of the Army designated the Office of the Chief Information Officer/G-6 as the CIO for the Army. The Army CIO/G-6 is charged with analyzing data collected during the Title 40/CCA Compliance and Certification process and recommending to the Milestone Decision Authority whether to continue, modify, or terminate Army Information Technology, Command, Control, Communication, Computers and Intelligence, and National Security Systems.

All Acquisition Category (ACAT) and Special Interest programs require a CIO assessment prior to a Milestone (MS) Decision. The Army CIO/G-6 assesses Army ACAT I, ACAT II, and Special Interest programs, while ACAT III programs are assessed by the Program Management Office’s (PMO) CIO functional organization. The requirements for Title 40/CCA and applicable program documen-

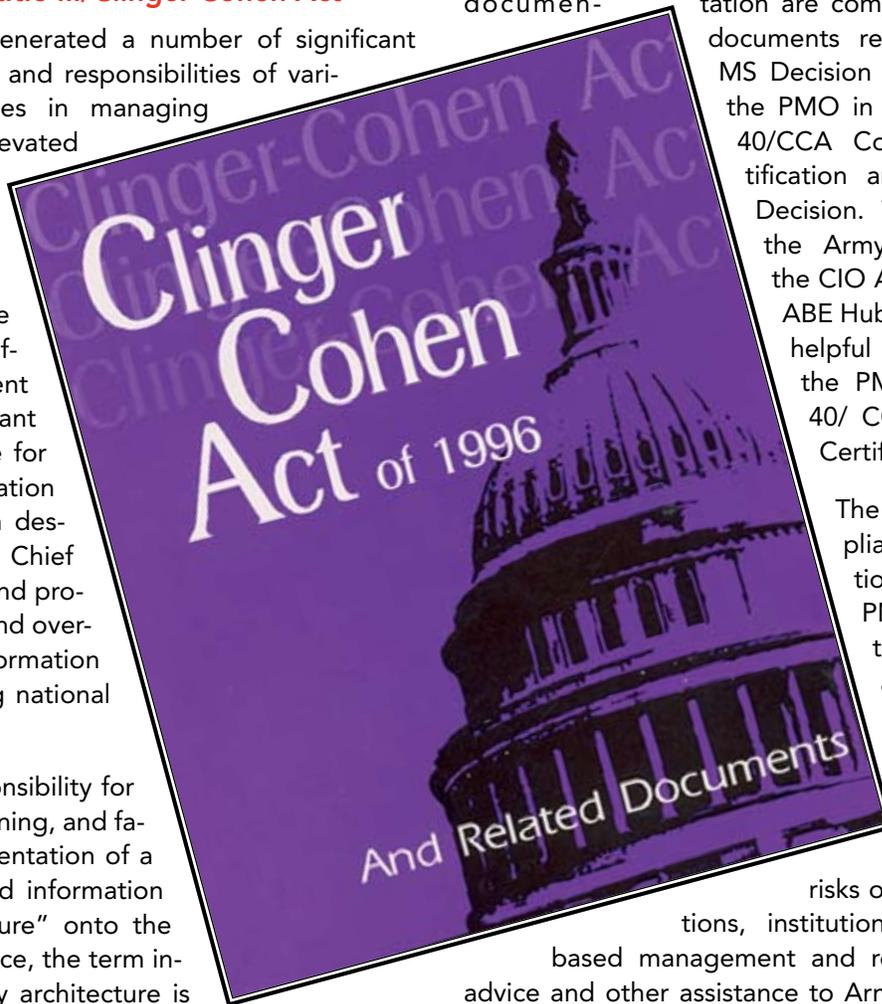
tation are complementary to those documents required to obtain a MS Decision and meant to assist the PMO in achieving both Title 40/CCA Compliance and Certification and a favorable MS Decision. To assist the PMO, the Army CIO/G-6 provides the CIO Assessment Tool. The ABE Hub contains a wealth of helpful information to assist the PMO during the Title 40/CCA Compliance and Certification process.

The Title 40/CCA Compliance and Certification process guides the PMO through statutory, regulatory, and acquisition policy compliance. The Title 40/CCA process maximizes the value and assesses and manages the

risks of IT/C4I/NSS acquisitions, institutionalizes performance-based management and results, and provides advice and other assistance to Army Senior Leaders to ensure that information resources are acquired and managed appropriately.

The Clinger-Cohen Act was the most significant IT reform of the last decade. Based on proven, practical IT best practices, it is designed to ensure that IT investments provide measurable improvements in mission performance. It directs Federal Agencies to establish a comprehensive approach to manage the acquisition, use, and disposal of IT.

The following summary outlines the roles and functions of the CIO/G6 as directed in Title 40/CCA:



STRATEGIC GOAL 2

Acquisition and Management of IT Resources

The CIO/G-6 provides advice and other assistance to the Secretary of the Army and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed in a manner consistent with chapter 35 of Title 44, United States Code, and the priorities established by the head of the executive agency.

Strategic Planning

This function pertains to the CIO responsibility for setting an Army IT strategy that supports the DoD IT strategy. Specifically, the plan should incorporate DoD/Army C4 mission, resource, and management objectives to drive Army IT plans and priorities. Clinger-Cohen directs the development and maintenance of a strategic information resources management plan that shall describe how information resources management activities help accomplish to the Army's assigned missions.

Drive Integrated Enterprise Architecture

This function pertains to the CIO responsibility for developing, maintaining, and facilitating the implementation of an Integrated Enterprise Architecture. Specifically, the CIO will define the functional and technical requirements (DoD and Army) and policy governing the architecture and ensure that it supports the objectives of the Army strategy. The CIO is also required to act as an advisor to stakeholder organizations that required guidance in meeting architecture standards.

General Order Number 3 (Under Revision)

Although currently under review/revision General Order Number 3 provides the following direction relating to strategic planning requirements of the CIO/G-6:

- Develop, maintain, and facilitate the implementation of a sound and integrated information technology architecture.

- Develop policy and guidance on information management and C4/IT (including automation, telecommunications, visual information, and related activities, services and programs).

- Develop, coordinate, and implement the Army Knowledge Management, Enterprise Architecture, Enterprise Infrastructure and Enterprise Portal.

- Provide guidance on and validation of business process initiatives and programs with C4/IT impact.

- Develop, in conjunction with Army G-2, a process to ensure all-source intelligence support focused on cyber threats to assist with procurement/acquisition Milestone Decisions for ACAT I-III.



STRATEGIC GOAL 3

PROTECT AND DEFEND THE ARMY'S SYSTEMS, NETWORKS, AND INFORMATION.



The CIO/G-6 will defend, protect and manage the information infrastructure through a proactive Information Assurance (IA) policy, governance, and operations. This requires a defense-in-depth strategy using risk management principles and multi-level security mechanisms to protect the layers of the Army information systems, networks and data. The Army's approach concentrates on protecting information, defending systems and networks, providing IA situational awareness, fostering innovation, and creating an empowered workforce. The Army has led DoD on several strategic fronts: During the Quadrennial Defense Review the Army leadership highlighted IA as a key military strategic capability for securing Cyberspace and the Warfighter. Federal Information Systems Management Act (FISMA) requirements have been exceeded by the Army

in systems accreditation, security controls, contingency planning, annual security reviews, and has taken the initiative to document user and specialized training. In addition, the Army has executed the phased implementation of Homeland Security Presidential Directive-12 (HSPD-12) and has surpassed Joint Task Force – Global Network Operations (JTF-GNO) requirements in the implementation of Cryptographic Common Access Card Logon for users and machines, Contractor Verification System implementation, and Electronic Digital Signatures for authoritative authentication. Currently the Army CIO/G-6 is taking steps to secure two way wireless devices and extending physical security measures to the DoD Smart Card technology. The

Army has become an integral partner with the National Security Agency in developing the Global Information Grid Information Assurance Architecture, and collaborated in the development of capabilities documents and strategies for the GIG Information Assurance Portfolio. The Army developed and implemented an aggressive policy for Data at Rest and Data in Motion.

Additionally, the NETCOM/9TH SC(A) Campaign Plan contains extensive strategic and tactical details about the IA objectives.

END STATE:

By 2015, the Army will achieve the capability for global force management, mature identity management to include role-based information access (individual identity).

STRATEGIC GOAL 3

Area Processing Centers and Network Service Centers will be operating to reduce the number of access points and strengthen LandWarNet.

By 2015 the Army will have an Information Assurance architecture that is integrated within the DoD vision for Cyberspace Operations. DoD-wide Information Assurance standards and network management tools will have been incorporated into LandWarNet Network Operations enterprise-wide. The Army CIO/G-6 will have established strong, formal collaborative relationships with industry partners for advancing information security capabilities. By 2015 the Army CIO/G-6, in collaboration with DoD, will have implemented an active risk management program to continuously identify information security operational dependencies and vulnerabilities. By 2015 the Army, in collaboration with the Joint community, will have implemented an IA sensor grid to enhance defense-in-depth of the GIG in support of the Army and Combatant Commands worldwide. Solutions for providing access to needed information with the Army's enterprise environment for family members, all retirees, and other federal and state agency personnel will be implemented by 2015.

Identity



While the work on the capability to connect – the network – continues, the Army's focus is expanding to the collaborative capabilities that the network enables and the complex security environment necessitating strident protective and security tools, measures and policies to protect the global collaborative environment. Our current challenge is finding the right balance between protecting the network and data and providing access to networks and information.

As the DoD and the Army moves to a global collaborative environment, we must recognize that our enemies will occupy the same global network fabric, seeking to be active, but malicious participants in the global collaborative environment. The need to accurately differentiate between the "friendly" and the "threat" and the ability to understand the "situation" in which both exist and interact has never been more urgent. As with the ability to connect, the Army has made substantial progress in its ability to secure the network by limiting access

to only authorized users through a variety of information assurance, cryptographic, and identity management solutions such as: Host Based Security System (HBSS) - the single most important Information Assurance/Computer Network Defense (IA/CND) transformation effort to counter and defend against ongoing exploitation of DoD computers at the enterprise level providing an integrated, end-to-end management console; Efforts to secure Data at Rest (DAR) include providing a contract to acquire encryption software protecting data on mobile computers (laptops) and storage devices. Two-Factor Authentication - providing the Army Common Access Card (CAC)/Public Key Infrastructure (PKI) alternative Smart Card Login tokens allowing system administrators to authenticate into the Army's Active Directory (AD) using two-factor authentication. Through advances in identity management and network security, the Army strives to provide commanders with situational certainty: the ability to determine friend from foe and then the opportunity to match friendly capability to threat vulnerability while shaping an advantageous environment. As the Cyberspace domain is being defined we must continue to transform our Information Assurance (IA) processes and tools to continue to strengthen our network. Three-factor authentication through the implementation of role-based access will be implemented in synchronization with the Department of Defense. Standardization of installation architectures and full implementation of a single DOIM on installations is critical to improved security and network performance. The reduction of the number of entry points into the network backbone through the implementation of Area Processing Centers, Fixed-Based Regional Hubs, and Network Service Centers is key to securing LandWarNet.



STRATEGIC GOAL 4

ENSURE ARMY INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY INVESTMENTS MAXIMIZE JOINT AND ARMY CAPABILITIES.

The CIO/G-6 will improve effectiveness and identify efficiencies that free resources to better support operational requirements. The CIO/G-6 will ensure IT investments support only transformed, integrated processes that further achieve the development and validation of capital planning strategies that improve combat capability, warfighting readiness, and mission performance.

These investments will be managed as portfolios and will be in compliance with the Army Enterprise Architecture; additionally, the CIO/G-6 will continue to support the Army Audit Agency initiative to review Army Commands' IT expenditures. The Army CIO/G-6 established the Army Portfolio Management Solution (APMS) as the Army's authoritative database for registration/reporting of IT investments supporting DoD and internal Army data calls (AITR module), the Domain Certification process for Business Mission Area (BMA) investments which expend more than \$1 million in development or modernization (Domain Certification module) and the prioritization of IT MDEPS in support of the POM build through the Capital Planning and Investment Management Process (CPIM module). The three modules rest upon an interactive database residing behind AKO. APMS enables the linking of IT investments to capabilities/functions (based on the Business Enterprise Architecture supporting the BMA, defined Joint Capability Areas supporting the Warfighting Mission Area (WMA) or defined Enterprise Information Environment (EIEMA) capabilities). This linking of

investments to capabilities supports the identification of redundant IT investments for potential consolidation or elimination, as required by the AKM Guidance Memorandum co-signed by the Secretary of the Army and Chief of Staff, Army.

END STATE:

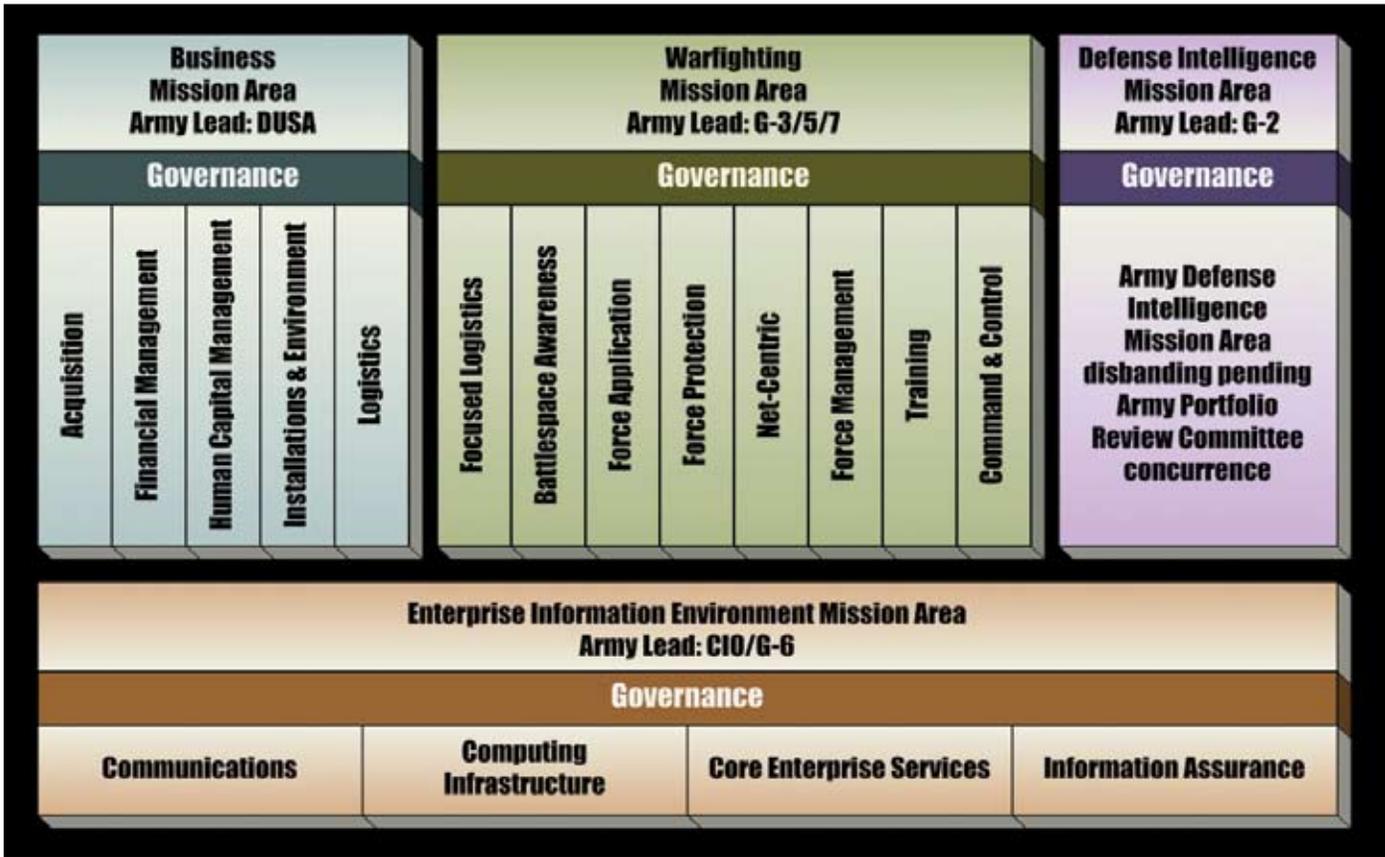
By 2015 the CIO/G-6 will have synchronized the Army's IT Portfolio Management process with the DoD and Joint Portfolio processes and institutionalized the process to drive IT investments to support the Army's capability requirements and established priorities. IT PfM will be fully integrated into the Army Core Business Processes of Joint Capabilities Integration and Development System (JCIDS), Planning, Programming, Budget Execution (PPBE) Process, and the Defense Acquisition System (DAS). The CIO/G-6 working in collaboration with the G-3/5/7, G-8 and ASA(ALT) will have developed an information technology acquisition process that takes into account the nature of IT lifecycles and technology developments and provides Warfighters with the best IT capabilities available.

Applications

The Army's Global Enterprise is among the largest in the world. To successfully provide assured services for a global Enterprise, establishment and management of Army IT assets is essential. Of all the Army's IT assets, applications are specifically and uniquely developed and enhanced to deliver user-specific capabilities and each Mission Area guides the development and enhancement of applications respective to the specific needs of their domains. But it is through IT Portfolio Management (IT PfM) that the management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability is accomplished. IT PfM helps ensure that the Army invests its IT resources



STRATEGIC GOAL 4



to align with approved enterprise architectures and complies with applicable regulatory guidance for information security to ensure that Information Assurance (IA), Computer Network Defense (CND), and other defense and protection measures are designed based on validated intelligence defining the threat and includes measurable outcomes and return on investment. IT PfM is driven by the Clinger-Cohen Act (CCA) of 1996, DoD Directive 8115.01 – IT Portfolio Management, and other recent DoD and the Office of Management and Budget (OMB) direction.

IT Portfolio Management Structure: Mission Areas and Domains

The designation of Army Leads aligned with the DoD construct establishes reporting authorities and responsibilities consistent with current laws, policies and regulations. IT investments/capabilities supporting the Army have grown in number, scope and complexity. As new capabilities are required and new technologies evolve, a coordinated policy and process must ensure IT investments provide the “right capabilities” at the “right time.”

Management of the Army’s IT investments/capabilities as portfolios, capitalizing upon best practices, emerging technology and common solutions is essential to the Army’s transformational efforts. As the Army transforms, it is imperative that IT investment portfolios support the Army’s Mission, Vision, and Strategic Goals; ensure an efficient delivery of capabilities to the Warfighter; and maximize return on investment to the enterprise. At the Enterprise level, management of IT portfolios begins with Mission Areas and Domains aligning functional requirements and capabilities with IT solutions. This will enable the Army to increase efficiency/effectiveness through the elimination or consolidation of redundant or outdated capabilities, and provide increased technical performance. IT Investments must be analyzed and prioritized to maximize strategic alignment and support to the Warfighter.

EIEMA Construct

The Enterprise Information Environment Mission Area (EIEMA) enablers support virtually all of the Army’s strategic level initiatives to some extent. Two specific Army Strategic Initiatives are led by the CIO/G-6; LandWarNet

STRATEGIC GOAL 4

Operational Capabilities and LandWarNet Institutional Infrastructure. The CIO/G-6 vision is that the Enterprise Information Environment is end-to-end, connecting Warfighters in the operational environment seamlessly to the institutional infrastructure and the Army's Core Business Processes. Our mission is to provide these capabilities to Warfighters during all Joint Operational Phases. In the end LandWarNet is an enhanced orders process for Battle Commanders and a decision-support capability for the Business Process leaders who support them.

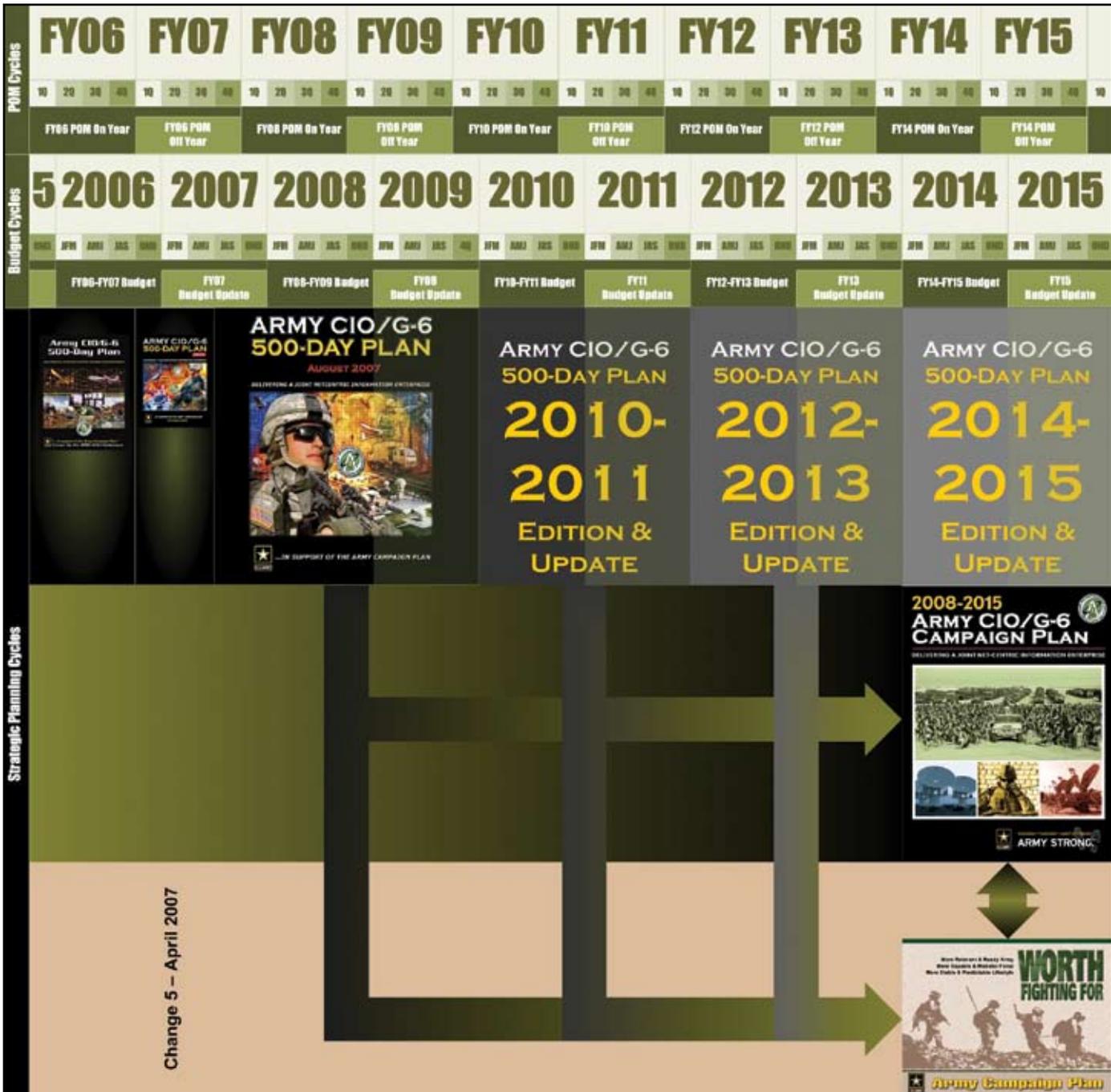
The EIEMA is one of four DoD Information Technology (IT) Mission Areas contributing to DoD IT management. The EIEMA includes four IT Domains that provide oversight to applicable Army components IT programs. EIEMA IT programs, systems, and initiatives are designed to support and enhance the Army's warfighting abilities while supporting actions to create a Net-Centric force, capable of IT system and information superiority. The Army CIO/G-6 is the EIEMA Lead. The four Domains within the EIEMA, which are all also led by CIO/G-6, are: (1) Communications; (2) Computing Infrastructure;

(3) Core Enterprise Services, and Information Assurance. The CIO/G-6 also leads the Net-Centric Domain, which resides within the Warfighter Mission Area (WMA).

At the DoD level, the EIEMA is led by the DoD Chief Information Officer. Under the DoD IT PFM structure, the DoD CIO conducts EIEMA Investment Review Boards (IRB) and develops and submits both POM Issue papers and off-year Change Proposals. In addition, at the DoD level, there is a Joint Net-Centric Operations (JNO) Capabilities Portfolio Manager, which is the Assistant Secretary of Defense (Networks, Information and Integration) (ASD(NII)). Under authority provided by Deputy Secretary of Defense, the JNO CPM also develops and submits POM Issue papers and Change Proposals for the EIEMA, and, has additional authorities including direct access to Program Managers, authority to conduct independent program reviews and access to pre-decisional POM information for programs within the Army EIEMA portfolio. Lastly, the JNO CPM may submit POM Issue Papers directly to the Deputy's Advisory Working Group (DAWG).



STRATEGIC GOAL 4



Financial Resources Alignment

The Army CIO/G-6 Campaign Plan guides the Program Budget Review Boards (PBRB) for both budget and POM year requirements for the development of unfunded requirements (UFR) prioritization. Funding, as available, can be applied to the top priority UFRs. Strategy development and implementation is a cyclic and iterative process incorporating updated and revised direction and

guidance; stakeholder feedback, and optimally, synchronizing with funding through the Planning, Programming Budgeting and Execution System (PPBES). By aligning the short-term execution plan (the Army CIO/ G-6 500-Day Plan), and the long-term strategic plan (the Army CIO/G-6 Campaign Plan) to the Army Campaign Plan's time frame, the IM/IT strategy stays relevant and funded by being synchronized with the other Defense budget documents.

STRATEGIC GOAL 5

DEVELOP THE ARMY'S INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY KNOWLEDGE AND SKILLS TO SUPPORT MISSION NEEDS.

The CIO/G-6 will lead the Signal Regiment's development of strategy to support Army Signal Forces requirements in support of Army Transformation in accordance with the Army Force Generation (ARFORGEN) process. The CIO/G-6 will lead the human capital initiatives to expand the capabilities of all Soldiers and Army Civilians by strengthening their knowledge, skills, and abilities in managing technology, processes, and information. IM and IT competencies enhance the capabilities of Army personnel whose innovative nature and desire to excel give the Army our greatest competitive advantage.

As part of the Army's Grow the Force effort, the Signal Regiment identified the following requirements: a CONUS Theater Signal Command; three additional Expeditionary Signal Battalions (ESB); two active and one reserve component; two Tactical Installation and Networking Companies – Enhanced (TIN-E) (cable and wire capability); one active and one reserve component; and the buy-back of all Reserve Component spaces in the

35th Signal Brigade. The additive Active Component ESB and TIN-E requirements are critical to meet ARFORGEN requirements and bridge capability gaps. These gaps are due to Corps and Division signal structure inactivation and the resultant increased mission load on ESBs to support all phases of ARFORGEN; Reserve Component rotation policies; and lack of heavy cable/wire capability in the current force structure. In addition, DAMO-FM approved one Active Component ESB, one Reserve Component ESB, the buy-back of the Reserve Component spaces in the 93rd Signal Brigade, and the required increase in signal force structure to resource approved designs.

Accomplishments in the Army Knowledge Leaders program include twenty-seven emerging leaders who have completed the program and are being intensively managed within the Army. The Presidential Management Fellows Program has been established as a two year leadership training program for top professionals who have recently completed masters or doctoral programs.



STRATEGIC GOAL 5

The mission of the National Security Personnel System (NSPS) is to place the right civilian in the right job with the right skills at the right time at the right cost. Within the Signal Regiment we must insure our civilian personnel management is "mission based" and is linked to the CIO/G-6 Goals.

Contract support has always been important to our Army. An emerging requirement is to train contract support personnel on the Army's technical architecture and standards in the execution of Army systems contracts. Training that is being provided to Signal Soldiers, Leaders, and Department of Army Civilians is also important for selected contractors in support of Army support contracts. The CIO/G-6 will work in collaboration with TRADOC and the United States Army Signal Center and School to develop the policies and processes to enable this emerging requirement.

END STATE:

SIGNAL FORCE STRUCTURE: The Signal Regiment and FORSCOM support requirement for more Active Component ESB and TIN-E force structure. Any additional ESBs and TIN-E units must compete in TAA 10-15 for resourcing either as new units or Active Component/Reserve Component re-balance. The first step is obtaining validation for the increased requirements during the TAA 10-15 Rule Of Allocation (ROA) CoC in April and follow on GOSCs, and the resourcing forums during the fall 2007 TAA resourcing phase. The CIO/G-6 will lead the synchronization of the Signal Regiment Strategic Plan for Force Structure requirements in support of the Army TAA and ARFORGEN processes.

HUMAN CAPITAL: The primary asset of today's organization is its human capital. In the future we must continue to attract and develop the right talent to create an expert and enduring future force for the Army. IT workers need to build flexible skills in technology, business and leadership that are relevant and adaptable to an ever-changing world. Human capital management must include several dimensions: (1) Strategic alignment of Human Capital strategy to organization goals; (2) Leadership development, succession planning, and continuous learning; (3) High performance culture that promotes diversity and rewards excellence; (4) Talent management process to attract, promote and retain quality talent; and, (5) Accountability using standards and metrics to attain measurable results.



Human Resources Alignment

Aligning the efforts to manage both the military and DA Civilian human resource requirements necessitates the coordination between the Army CIO/G-6 as the primary proponent for the DA civilian IM and IT training programs: the ITM Civilian Career Program-34, the IM/IT Workforce Development programs, and the Workforce Accession Program; and TRADOC's LandWarNet University at the United States Army Signal Center and School. The CIO/G-6 will continue to support the development of the e-Learning portal as a primary training venue for the Active and Reserve Signal components. Additionally, the CIO/G-6 is responsible for developing Knowledge Management (KM) competencies and skills across the Army and leveraging e-Learning for all Army functions. Therefore the Signal Force Structure development program and the Human Capital development efforts of the CIO/G-6 are interdependent; advancements and changes in one produce a ripple effect of necessary changes to the methodology and curricula of the others, but the overall needs of the warfighter will be supported and met with collaboration between TRADOC and the CIO/G-6.

STRATEGIC GOAL 6

DELIVER AN INTEGRATED ENTERPRISE STRATEGY THAT INFLUENCES JOINT AND ARMY USE OF INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY IN FURTHERING THE WARFIGHTING CAPABILITIES.

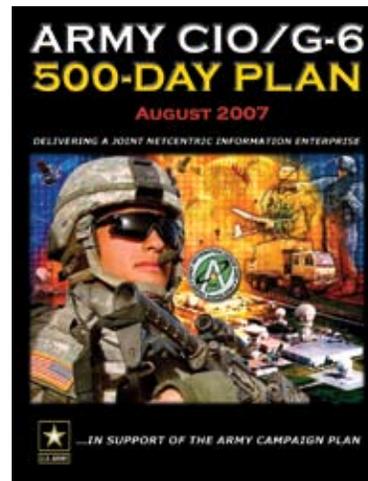
Strategy Management is a continuous process that encompasses: Strategic Planning, Communications, Performance Management/Assessment, Gap/Risk Analysis and Performance Improvement. It is the Army CIO/G-6 responsibility to produce and communicate an integrated Army IM and IT strategy and ensure related policy positions influence DoD and Joint Strategies and planning efforts. It is essential that the Army's IM and IT strategy reflects an understanding of and incorporates Joint warfighting capability requirements. It is also imperative for the CIO/G-6 to lead the resolution of emerging strategic IM and IT gaps and risks to the Warfighter. Consistent with General Order Number 3 and statutory requirements outlined in Title 40/CCA, the CIO/G-6 is responsible for oversight of all IM/IT risk assessment processes for the Army (Active, USAR, and ARNG) components.

END STATE:

The CIO/G-6 will improve the strategic planning process for IM/IT that provides realistic long-range guidance to the Army that enables achievement of assigned missions, and near-term execution plans that ensure timely delivery of the best IT capabilities in support of Warfighters. The CIO/G-6 will effectively synchronize and integrate NETCOM/9TH SC(A), USAR, and ARNG IM/IT strategic plans with the Army CIO/G-6 strategic plans. The CIO/G-6 will effectively implement the 500-Day Plan that focuses near-term IM/IT resources on critical Army priorities. The CIO/G-6 strategic communications processes will be improved to effectively communicate to internal and external customers to achieve understanding by key audiences (Commanders, Congress, Industry, Media). The CIO/G-6 will strive to foster relationships that establish trust and confidence by conveying timely, truthful, and clear messages relating to the importance of IM/IT initiatives to our Warfighters and the importance of a synchronized strategy. A strategy execution process will be intensively managed through the implementation of 100-day performance review process. The process will effectively assess strategy execution and provide a forum for focused discussion of priorities and resource alignment. The CIO/G-6 will institutionalize the Army's selected performance improvement process, Lean Six Sigma, to continuously pursue process

improvement within the Army to achieve more effective and efficient IM/IT management processes in support of Warfighters.

Implementation Strategy – CIO/G-6 500-Day Plan



As the near-term implementation plan for the Army CIO/G-6 Campaign Plan, the Army CIO/G-6 500-Day Plan iterates the six Strategic Goals and establishes supporting Objectives owned by the CIO/G-6 and decomposes those Objectives into specific near-term Initiatives. The 500-Day Plan will be revised and updated in synchronization

with the PPBE process to assure that IM/IT resources are aligned with the CIO/G-6 strategy and support established priorities.

NETCOM/9TH SC(A), the Signal Center and the Reserve Components also have strategic plans for the execution of their IM/IT Objectives as well as for implementation of their respective command responsibilities.

Performance Reviews

At approximately 100-day increments, the CIO/G-6 leadership will conduct performance reviews of the status of the 500-Day Plan's execution efforts of the six Strategic Goals and corresponding Objectives and Initiatives through in-depth tracking of the Projects and scheduled Tasks associated with the Initiatives. New Initiatives necessary to accomplish the Objectives may also be added to the 500-Day Plan.

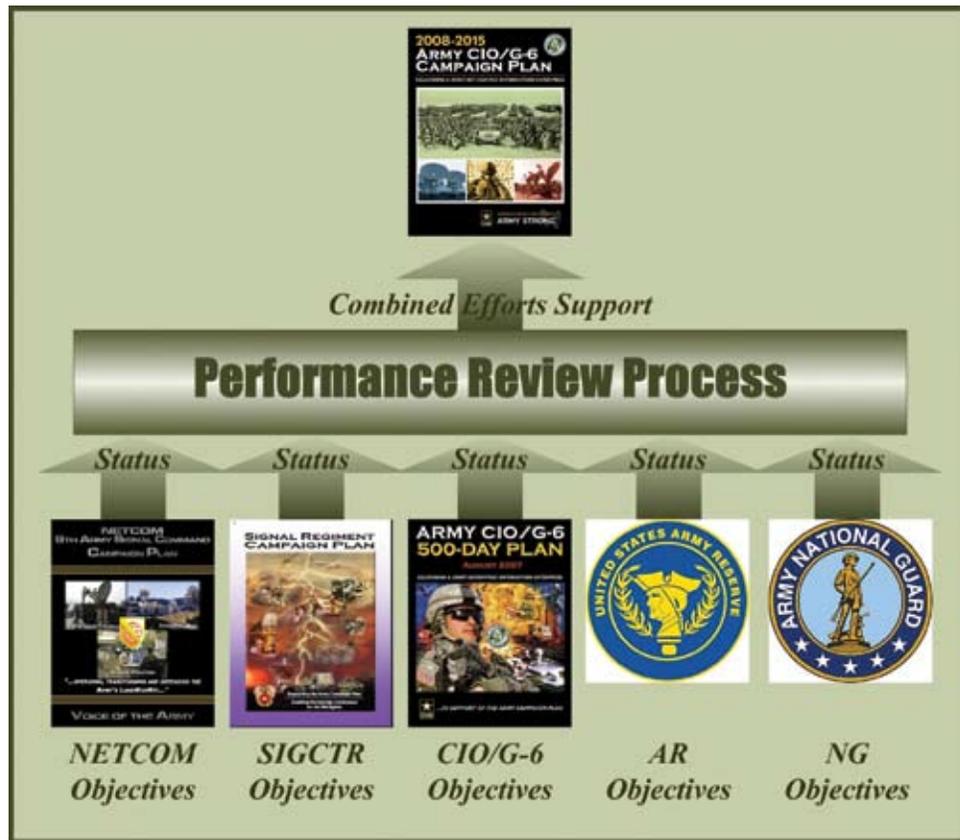
The CIO/G-6 will further the effectiveness of the performance reviews by implementing a program management tracking tool by which the schedule, financial, and manpower details of the near-term Initiatives in the CIO/

STRATEGIC GOAL 6

G-6 500-Day Plan as well as the NETCOM/9TH SC(A) Campaign, the Signal Regiment Campaign Plan, the U.S. Army Reserve G-2/6 C4IT Strategic Plan and the National Guard efforts will be tracked in a consolidated view.

Process Improvement

Strategy management includes the continuous assessment of core processes within the CIO/G-6 and NETCOM/9TH SC(A), identification of improvement opportunities and the development and implementation of process improvements. The Army adopted methodology for process improvement is Lean Six Sigma. The Army CIO/G-6 will implement their plan for Lean Six Sigma process improvements and institutionalize the Lean Six Sigma process by 2010.



Strategic Communications

The CIO/G-6 will strive to continuously improve strategic communication capabilities to effectively communicate with internal and external audiences by building stronger relationships through better strategic communications. To overcome this challenge, all of us, from the CIO/G-6 to our Soldiers and DA Civilians must engage the American public to close the gap between perception and reality. The Signal Regiment's senior leaders have a key role in this mission - they must engage, must speak with one voice, and foster a "culture of engagement" in which telling our story is a responsibility for all who serve. This requires: an understanding of the dynamic information environment; strategic communication planning being prominent in the strategy, policy, planning and execution processes. In the near term, we must: increase level of participation in the current program and process; improve the level of awareness of the CIO/G-6 and NETCOM/9TH SC(A) of current strategic communication tools and products; and improve our current communication plans, programs, and processes to provide better support for the long term. Objectives are:

1. Institutionalize a strategic communication process by integrating Strategic Communication planning so engagement strategies, tools and products are available for senior leaders as decisions are made to enable immediate, effective, and timely communication across the Army.
2. Build and sustain relationships with stakeholders and key audiences that foster trust and confidence (American public, Congress, and the media) by institutionalizing the 3+2+1 engagement initiatives that aligns messengers and information delivered with the right audience.

Program Executive Office, Enterprise Integration System (PEO EIS) Oversight

The Program Executive Office was established in 1987 as Program Executive Office, Standard Army Management Information Systems (PEO STAMIS) to help implement of the Goldwater-Nichols Act. The Army Reorganization on 26 October 2001 resulted in PEO STAMIS changing its name to Program Executive Office, Enterprise Informa-

STRATEGIC GOAL 6

tion Systems (PEO EIS). PEO EIS' program management responsibility grew significantly over the years from thirteen systems to overall acquisition responsibility for over fifty systems and products. The reorganization resulted in the addition of several Communications-Electronics Command Systems Management Center programs as well as the Research, Development and Acquisition Information Systems Activity.

The PEO EIS reports to the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) and to the Chief Information Officer (CIO)/G-6. PEO EIS provides infrastructure and information management systems enabling the Army to achieve victory through total information dominance. PEO EIS develops, acquires and deploys tactical and non-tactical information technology systems and communications and is also responsible for total life cycle support for many of these systems.

The mission of CIO/G-6 is to provide architecture, governance, portfolio management, strategy, C4/IT acquisition oversight and operational capabilities to enable joint expeditionary net-centric information dominance for the Army. This mission strategically aligns with the mission of PEO EIS. PEO EIS provides information dominance by developing, acquiring, integrating, deploying, and sustaining network-centric knowledge-based information

technology systems and business management systems, communications and infrastructure solutions through leveraged commercial and enterprise capabilities that support the total Army. CIO/G-6 has a principal responsibility for the Army's information management functions and is responsible for setting the strategic direction, determining objectives, and supervising the Army's Command, Control, Communications, and Computers/Information Technology (C4/IT) functions. The CIO/G-6 develops, coordinates, and implements Army Knowledge Management, the Army Enterprise Architecture, the total Army Enterprise Infrastructure and the Army Enterprise portal. Additionally, the CIO/G-6 develops, coordinates, and implements IT portfolio management to provide the Army with Enterprise-level investment strategies on C4/IT systems.

The PEO EIS programs comprise network accessible programs and ensuring Information Assurance and security is also captured through the CIO/G-6 oversight of the programs.

The CIO/G-6, in the Title 40/CCA role, works in coordination with the PEO to ensure compliance with applicable policies, regulations and statutes prior to program reviews for their ACAT I programs. This oversight includes, but is not limited to, attending programmatic meetings



STRATEGIC GOAL 6



headed by the specific Program Management offices; reviewing requirements documents used in fulfilling the Title 40/CCA statutory requirements for milestone decisions, and the review and coordination of CCA assessments and packages requiring approval by the CIO/G-6.

Army Chief Information Officer (CIO) Executive Board

The Army CIO Executive Board, established in April 2001, is the executive forum to advise the Army CIO on the full range of matters pertaining to information management and information technology. The CIO Executive Board is in its sixth year of operation with forty member organizations from the Headquarters, Department of the Army, Army Service Component Commands, and Reserve Components.

The Title 40/Clinger-Cohen Act (CCA) provides direction to Federal agencies on IT management. The Act establishes agency Chief Information Officers, requires capital planning and investment control of information technology assets, and mandates performance-based and results-based management. The implementation of Title 40/CCA involves identifying ways to improve the efficiency and effectiveness of the Army's operations through the smart use of IT.

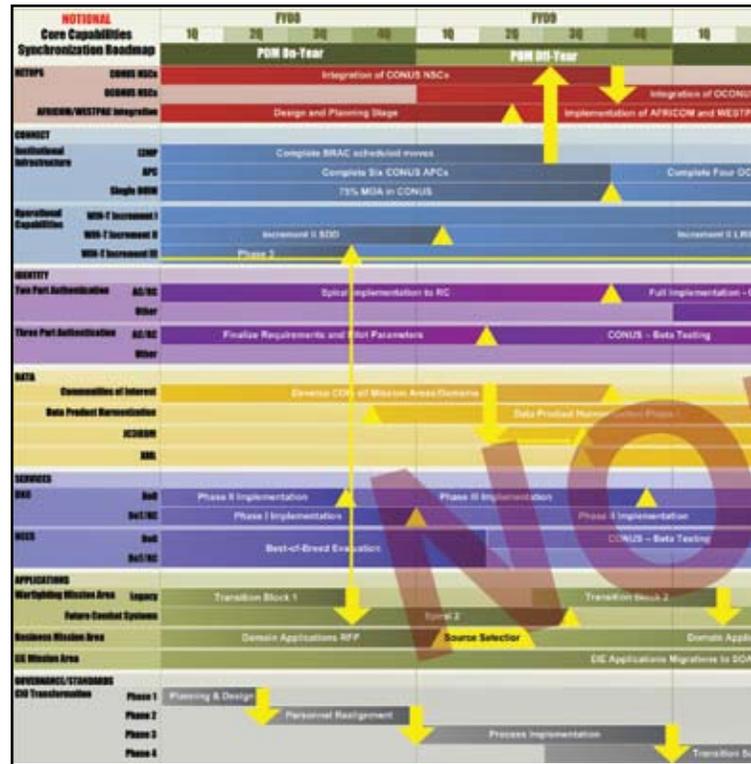
The CIO/G-6 will ensure the Board involves Army senior leadership from across functional areas in the implementation of the Title 40/CCA and actions affecting the Army IM/IT enterprise capabilities. In addition, the Board will make recommendations for, and sponsor cooperative efforts to broaden the use of IT initiatives. The Board will actively collaborate with the DoD CIO Executive Board and the Federal CIO Council on matters of mutual interest.

The Army CIO Executive Board Meetings will continue to be convened quarterly and will comprise briefings and case studies focused around a central theme. A variety of informative and decision-advisory material will be presented to the board members for the purpose of advising the Army CIO.

The Army CIO/G-6 is committed to transformation and to addressing the delicate balance of risk between current and future demands while providing the best capabilities to our Soldiers and DA Civilians who remain engaged in the global struggle against violent extremists and face the constant risk of catastrophic natural disasters at home and abroad. The Army CIO Executive Board will remain the primary forum for discussing strategic level IM/IT issues at the executive level with representatives from across the Army.

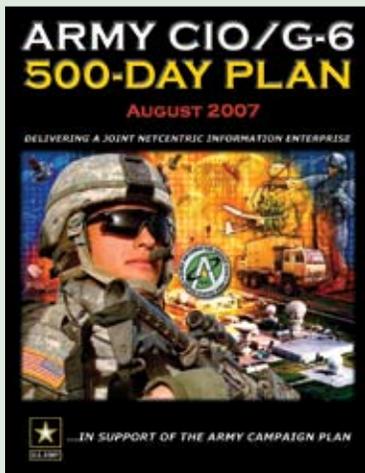
ARMY CIO/G-6 CAMPAIGN PLAN

The CIO/G-6 Campaign Plan includes three separate appendices that provide a greater level of detail, specificity and time relevance to specific areas. The first appendix (Appendix A), the 500-Day Plan, is the short-term execution plan for the CIO/G-6 Campaign Plan. It will be updated annually and will align to the CIO/G-6 funding plan. The second appendix (Appendix B) is the combined Roadmaps for the long-term sequencing plans for the LandWarNet core capabilities. These roadmaps will be continually updated, but the sensitive nature of their contents will preclude them from being available for the general public. They will be stored behind Army Knowledge Online-SIPRNet (AKO-S) and accessed via the CIO/G-6 web page to allow the CIO/G-6 to make them available to the widest, cleared audience possible. The third appendix (Appendix C), will be Emerging Trends in which advances in technology and changes in the situational environments will be examined and discussed. Appendix C will also be available via the CIO/G-6 web page, but depending upon the contents, may be secured behind AKO-S. All appendices will be updated as necessary to ensure their relevance.



Appendix A – The CIO/G-6 500-Day Plan

The latest 500-Day Plan was released in August 2007. It is the third in a series of Plans published by the CIO/G-6 detailing the immediate execution efforts for the development and enhancement of LandWarNet. This third Plan focuses on objectives and initiatives specifically discussed at the General Officer/Senior Executive Service and Command Sergeant Major Signal Summit held April 2007; initiatives to deliver immediate value to the Warfighter.

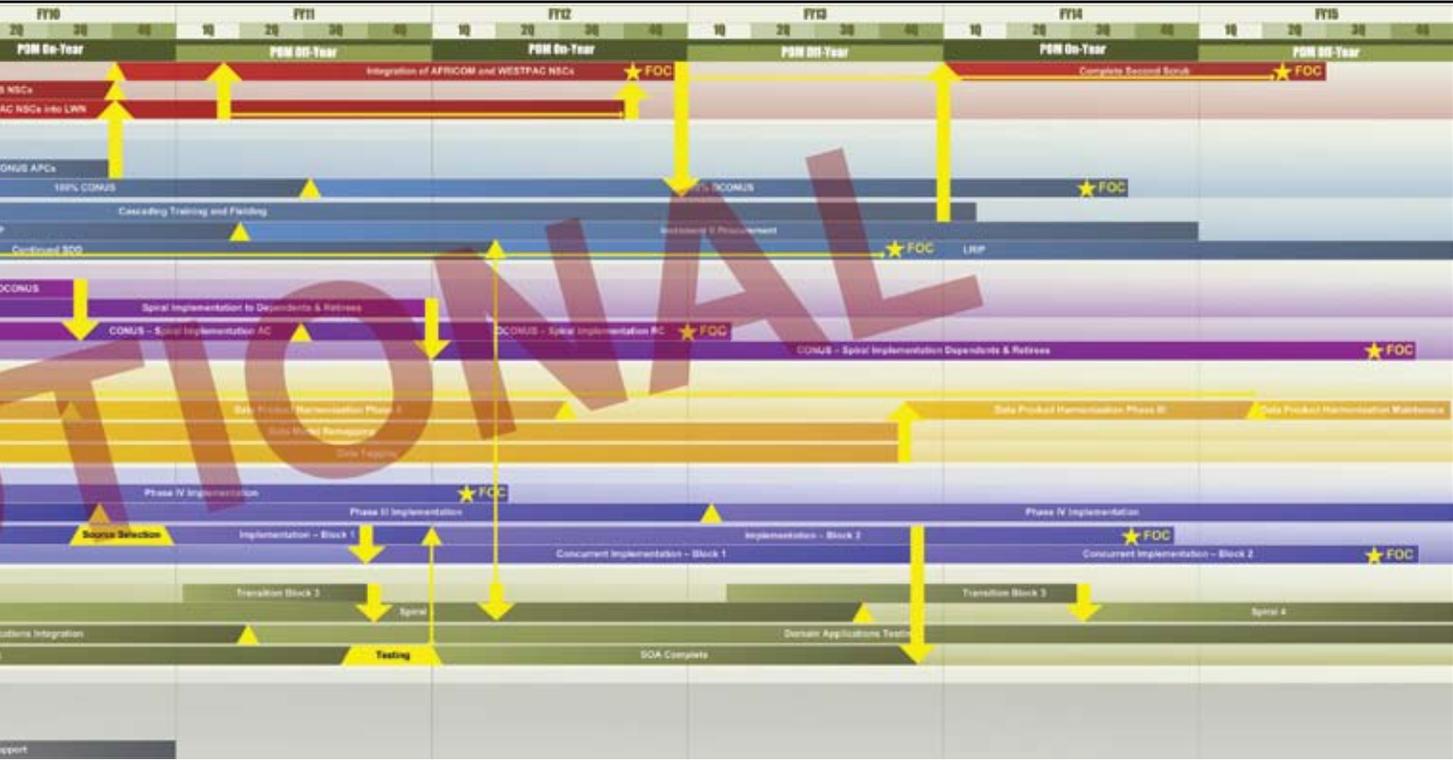


initatives specifically discussed at the General Officer/Senior Executive Service and Command Sergeant Major Signal Summit held April 2007; initiatives to deliver immediate value to the Warfighter.

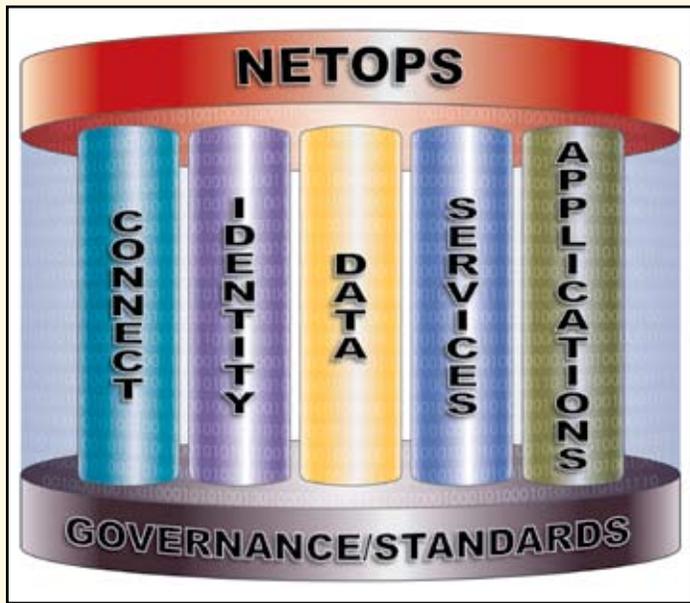
Appendix B – Roadmaps

Roadmaps are being developed to provide a graphical view of the LandWarNet Core Capabilities (Connect, Identity, Data, Applications, Services, NETOPS and Standards/Governance) to lay out the deployment of architecture segments and the enabling Information Management and Information Technology solutions. These Roadmaps will be developed initially for the 2008 – 2015 time frames. The Roadmaps will be living documents that reflect the most current plans for rolling out enabling IM/IT capabilities in support of the Army. Due to the nature of the content, these Roadmaps will reside behind AKO-S to provide adequate protection consistent with the classification level of the content, to effectively maintain the currency of the data,

IGN PLAN APPENDICES



and to provide easy access for authorized users. Roadmaps are currently under development and will be posted to AKO-S in mid-October 2007.



Appendix C – Emerging Trends

Information technology is an especially volatile and rapidly changing technology subject to extremely fast advances in response to consumer needs. No other technology evolves as quickly. In response to this rapid-fire environment, the CIO/G-6 is working to modify the way the Army buys IT to prevent obsolescence prior to full implementation. This is a very ambitious undertaking that requires the CIO/G-6 to remain constantly abreast of the advances and trends in industry and in the way the world uses Information Management and Information Technology. Updates to the Emerging Trends Appendix will be continuous and in concert with the global environment driving the inevitable and ever accelerating change.

TAKE AWAYS

Summary of the Campaign Plan Major Initiatives for 2008-2015:

- The CIO/G-6 will transform from a functionally-based organization to a process-based organization in the near term and fully transform to a service-based organization by 2015.
- Align Information Management/Information Technology Budget with CIO/G-6 Strategy – 500-Day Plan and Campaign Plan.
- LandWarNet will be the Enterprise Virtual Network and the Army will have fully implemented Everything over Internet Protocol.
- The Operational Army will achieve On-the-Move connectivity to LandWarNet for all operational units down to Battalion level and Separate Company level by 2015.
- Expansion of broadband and narrow-band capabilities to meet the bandwidth requirements for pushing On-the-Move capability to Battalion and Separate Company level, and achieve a balance of commercial to military satellite capabilities of 50/50 by 2010.
- The Operational Army will achieve a minimum level of airborne layer coverage to meet Combatant Commanders' requirements in Operational Theaters.
- The Army will complete the Information Infrastructure Improvement Modernization Program on all Active Army installations and extend the program to the United States Army Reserve and National Guard infrastructure by 2015.
- The Army will achieve full implementation of the Single Director of Information Management on Army Installations and realize "train as we fight" capabilities in garrison environment to include SIPRNet to Battalion and Separate Company levels in Active and Reserve Components.
- The Army will integrate Warfighter Information Network - Tactical capabilities and the Joint CONUS Communications Support Environment capabilities to support the full spectrum of conflict to include CONUS-based support to Homeland Security.
- The CIO/G-6 will be hosting Enterprise-wide data services from Area Processing Centers worldwide.
- The Army will achieve full Network-Centric Operational Environment as envisioned by Joint Task Force–Global Network Operations.
- The CIO/G-6 will implement a full spectrum Network Operations & Security Center capability through an Army Global Network Operations and Security Center and supporting Network Operations and Security Centers.

TAKE AWAYS

- The CIO/G-6 will Implement an Army Enterprise Service Oriented Architecture.
- Consolidate and strengthen Army Entry Points into the Defense Information Service Network.
- The CIO/G-6 will have established Network Service Centers Enterprise-Wide.
- The Army CIO/G-6 will have achieved Enterprise-Wide authoritative Directory Services.
- By 2015 Army Knowledge On-line/Defense Knowledge On-line will be the single portal to access all enterprise services for the Army Enterprise.
- Performance metrics for delivery of services to Army customers will be based on industry standards for service delivery and not best effort.
- The Army CIO/G-6 will have institutionalized the Information Technology Infrastructure Library framework for service delivery.
- Information Technology investments and life cycle management of Information Technology enterprise resources will be based on an institutionalized Information Technology Portfolio Management process.
- The CIO/G-6 will stand up an Army Enterprise Information Management capability that provides visibility of all assets connected to LandWarNet.
- The Army will implement the Army Data Strategy in synchronization with DoD to enhance information sharing in alignment with the DoD vision.
- The CIO/G-6 will have led the transformation of Signal Force Structure to meet sustained Army Force Generation requirements through adequate strategic and tactical signal forces and the proper mix of Active and Reserve Components.
- The CIO/G-6 will fully implement an Enterprise-wide Information Assurance Architecture.



Department of the Army
Chief Information Officer/G-6
107 Army, Pentagon
Washington, DC 20310
www.ARMY.mil/CIOG6



AMERICA'S ARMY:
THE STRENGTH OF THE NATION™