LandWarNet 2020 and Beyond Enterprise Architecture

Version 2.0

As of: 1 August 2014

Revision History

Revision	Source	Date	Description of Change
V 1.0	SAIS-AOB	1 August 2013	Initial Release
V 2.0	SAIS-AOB	1 August 2014	Major Revision

Table of Contents

Table of Figures

Executive Summary

The Department of Defense Chief Information Officer (DoD CIO) has defined the DoD information enterprise as:

> *The Department of Defense information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners.*
>
> (DoD Information Enterprise Architecture V 1.1)

LandWarNet is the Army's portion of the DoD information enterprise, and it encompasses the IT contributions of all Army activities, agencies, and components. It is the Army's single, global, information enterprise that provides information technology (IT) capabilities, services, and information securely to Army users and Unified Action Partners. GuardNet XXI is the ARNG's portion of the DoD's information enterprise. Within the overall context of LandWarNet, some IT systems (e.g., GuardNet) are separate and distinct from other IT systems due to their unique statutory, regulatory, and operational requirements. As a mission enabler, it is continually evolving to meet the changing mission and business needs of the Army, including the changing threat environment, and to incorporate advances in IT that sustain or increase technological overmatch. In addition, the LandWarNet architectural paradigm is changing from a loose federation of stovepiped IT systems, to a single, integrated, service-oriented, shared environment.

This document describes, and provides guidance for, the end-state enterprise architecture (EA) of LandWarNet (abbreviated as LWN 2020 EA). It informs near- and mid-term Army IT investment and acquisition decisions to assure that they are aligned with the Army Network Campaign Plan (ANCP) and the DoD Information Enterprise Architecture (IEA), which encompasses the Joint Information Environment (JIE).

This document, together with its two annexes and associated Army Reference Architectures (published separately), captures the desired architectural characteristics of the end-state LandWarNet EA, and conveys Army architecture guidance and direction, to be followed across all Army activities, agencies, and components. The architecture guidance and direction is organized according to the layered structure of the DoD IEA. These layers are Communication

Services, Computing and Storage Services, Application and Data Services, Mission Application Services, and End-Users / End User Devices. In addition, it provides architecture guidance and direction in the areas of Network Operations (NetOps), Cybersecurity, and Information Management (IM).

BLOHM.GARY.W.1228949589

Digitally signed by BLOHM.GARY.W.1228949589
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=BLOHM.GARY.W.1228949589
Date: 2014.07.30 16:06:57 -04'00'

Mr. Gary W. Blohm
Director, Army Architecture Integration Center

1. Introduction

1.1 Mission / Vision

The Army's vision and mission statements for LandWarNet are:

> *Vision – The network must be capable, reliable, and trusted. To get there it must be a single, secure, and standards-based environment that ensures access at the point of need and enables global collaboration.*
>
> *Mission – Lead LandWarNet transformation to deliver timely, trusted, and shared information. Create an environment where innovation and service empowers Army and mission partners through an unsurpassed, responsive, collaborative, and trusted information enterprise.*

The desired outcomes associated with the LandWarNet transformation are addressed in the Army Network Campaign Plan (ANCP) [Reference B-5]. The ANCP describes how LandWarNet will transform over time to achieve these outcomes. The ANCP is introduced in Section 2.2.

1.2 Purpose / Rationale

This document describes the end-state enterprise architecture of LandWarNet in the 2020 and beyond timeframe. This document, together with its two annexes and the associated Army Reference Architectures (see Section 4), provides the objective (that is, end-state) architecture and architecture guidance that guides near- and mid-term Army IT investment and acquisition decisions in alignment with the DoD IEA[1]. This document is not intended to address the transformation of LandWarNet from its current architecture to this end-state architecture. The transformation process is described in the ANCP.

[1] Reference B-4

1.3 Scope

The LandWarNet is defined as a subset of the Department of Defense Information Enterprise (DoD IE) (see Section 2.1). As such, the LandWarNet includes the information resources, assets, and processes of all Army activities, agencies, and components required to achieve an information advantage and share information across the Army and with its Unified Action Partners. GuardNet XXI is the ARNG's portion of the DoD's information enterprise. The LandWarNet includes: (a) the information itself, and the Army's management over the information lifecycle; (b) the processes, including risk management, associated with managing information to accomplish the Army mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and information technology, including national security systems. Within the overall context of LandWarNet, some IT systems (e.g., GuardNet) are separate and distinct from other IT systems due to their unique statutory, regulatory, and operational requirements. This document does not address IT that is not network-enabled (for example, software that is embedded in weapons systems).

The scope of the LWN 2020 EA encompasses the end-to-end LandWarNet, from garrison to foxhole. It focuses on the materiel solutions and associated service management processes. The LWN 2020 EA specifically addresses Communication Services, Computing and Storage Services, Enterprise and Data Services, Mission Application Services, and End-Users / End User Devices.

1.4 Audience

The LWN 2020 EA audience includes the LandWarNet stakeholders across the Army's activities, agencies, and components. Stakeholders will read and follow this guidance to directly inform: (a) the development of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) solutions, and (b) Army Enterprise Network Portfolio (AENP) decisions. In addition to directly influencing the materiel designs of LandWarNet IT systems, stakeholders will use the guidance in this document to more accurately understand and plan for the emerging LandWarNet capabilities and services. The

LWN 2020 EA will also enable industry partners to focus their technology and Research and Development (R&D) efforts to best support the future IT needs of the Army.

1.5 Document Structure / Assumptions

This document (LWN 2020 EA) is structured into five major sections: Introduction, Key Concepts, Architecture Guidance and Direction, Description of Annexes / Reference Architectures, and Way Ahead; and two appendices: Appendix A (Acronyms / Glossary) and Appendix B (References). This document also has two annexes: Annex A (Technical Standards Guidance) and Annex B (Definitions and Guidance for the Common Operating Environment). These documents provide amplifying guidance on specific topics.

The following statements aid in the understanding of this document:

1. The glossary contained in Appendix A defines architecture-related terms as they are used in this document and in the Army Reference Architectures.
2. LandWarNet includes Army information resources, assets, and processes required to achieve an information advantage and share information across the Army and with mission partners. This architecture specifically focuses on the materiel solutions and associated management processes.
3. LandWarNet is not equivalent to “Army IT.” LandWarNet encompasses all of the IT systems that are network-enabled within Army activities, agencies, and components, but excludes those that are not network-enabled.
4. LandWarNet does encompass IT capabilities that are provided to the Army by external agencies as “services” (for example, the wideband communication services provided by the Defense Information Systems Agency (DISA)). However, the physical materiel used to provide these services is not part of LandWarNet. For example, a server providing IaaS capabilities is not part of LandWarNet, but an Army mission application being executed on the server is.
5. All of the networks that are owned or operated by Army activities, agencies, and components (for example, GuardNet, Intelligence Surveillance Reconnaissance (ISR) Net, etc.) are included in LandWarNet. In addition, the associated network interface equipment enabling connectivity to non-Army networks is part of LandWarNet.

6. LandWarNet encompasses data and networks up to the top secret/sensitive compartmented information (TS/SCI) security classification level. However, architecture guidance regarding the TS/SCI aspects of LWN 2020 EA is outside the scope of this document.

2. Key Concepts

This section discusses five concepts that are key to understanding LWN 2020 EA and its context. These concepts are:

a) The Department of Defense Information Enterprise (DoD IE)

b) The Army Network Campaign Plan (ANCP)

c) The new LandWarNet paradigm

d) The Army Enterprise Network Portfolio (AENP)

e) The governance, alignment, and compliance of LandWarNet

2.1 DoD Information Enterprise

The architecture of the DoD Information Enterprise, as defined by the DoD CIO, is described in the Department of Defense Information Enterprise Architecture (DoD IE) as:

> *The Department of Defense information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. It includes: (a) the information itself, and the Department's management over the information lifecycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and information technology, including national security systems.*

Analogous to the DoD IE, LandWarNet is the information enterprise of the Army. In its "joint" role, LandWarNet receives IT services from, and provides IT services to, other components of the DoD IE. However, its primary role is to provide the IT capabilities required to enable and support the Army mission, regardless of whether these IT capabilities are provided directly by the Army or by other DoD Services and/or agencies.

The DoD IE (encompassing the Joint Information Environment [JIE]) is not a program of record (POR). The DoD CIO envisions that it will be realized through Service and/or agency IT investments and systems that adhere to DoD IE reference architectures and standards that facilitate joint interoperability. It is an initiative to achieve the set of architecture characteristics necessary to meet Department-level objectives. These architecture characteristics are provided as direction from DoD CIO to each of the Services / agencies for incorporation into their own individual service-level IT architectures. The 10 key architecture characteristics are summarized below:

1. Single security architecture (SSA) – to provide a unified, comprehensive approach to cybersecurity.
2. Normalized, federated networks – to provide the required connectivity, while reducing cost and vulnerability.
3. Identity and access management (IdAM) – to improve interoperability, while improving security.
4. Data center standardization and consolidation – to reduce the total cost of computing and data storage via facility consolidation and establishing data center standardization.
5. Software application rationalization and server virtualization – to reduce functional overlap in the Department’s software assets, and to use hardware assets (for example, servers) more efficiently.
6. Desktop virtualization and thin-client environment, and smart client environment – to increase standardization across IT systems, to improve the management of IT devices, and to transition from a desktop computing paradigm to a cloud computing paradigm.
7. Mobility services – to enable and support new concepts-of-operation that increase mission effectiveness via mobile devices.
8. Enterprise services – to increase interoperability and standardization by providing IT services across the Department (that is, at the enterprise level).
9. Cloud computing – to reduce the total cost of computing and data storage, and improve individual and collective performance (via the use of shared IT resources as opposed to dedicated (that is, stovepiped) IT resources).

10. Governance – to improve the Department's overall effectiveness in validating, acquiring and providing IT capabilities.

The DoD IEA is a primary source of input to LWN 2020 EA. LWN 2020 EA is aligned with the DoD IEA, so that LandWarNet itself will be interoperable with other components of the DoD information enterprise.

2.2 Army Network Campaign Plan

The ANCP is a primary source of input for LWN 2020 EA. It establishes the framework for how the Army will design, develop, modernize, and secure the Army Network. The LandWarNet vision stated in this document is:

> *[LandWarNet will] provide global collaboration for the Army and its mission partners while efficiently delivering timely, trusted, and secure information from the Enterprise to the tactical edge, on an adaptive, single, secure, standards-based Army network.*

As currently defined, the ANCP contains three primary parts: the Army Network Strategy, the Army Network Campaign Plan – Near, which covers the planned IT investments over the next two years, and the Army Network Campaign Plan – Mid-term, which covers the planned IT investments during the next POM cycle.

The Strategy defines four outcomes that will achieve the Army's strategic imperatives regarding the use of LandWarNet to achieve its mission. The LWN 2020 EA is the objective end-state architecture that achieves these desired outcomes:

1. An operationally focused and unified network that supports global warfighting and generating force functions.
2. A resilient, multi-tiered, and rapidly configurable network supporting Soldiers in all environments.
3. A secure network and information environment that is protected from external and internal threats.
4. A global environment that offers seamless and timely access to relevant information, services, and applications.

2.3 The New LandWarNet Paradigm

The Army's traditional IT paradigm has been to develop stand-alone IT systems (containing both hardware and software components) for particular purposes or to provide mission-specific IT capabilities. This paradigm applied to both network-enabled and embedded IT systems, and led to the uncontrolled, non-standardized, proliferation of IT systems. These IT systems were dedicated to specific organizations, domains, or applications.

The emerging IT paradigm for the 2020 and beyond timeframe is essentially a transformation from the use of dedicated IT resources to shared IT resources. This means that LandWarNet will be structured to support end-users through a balanced application of general purpose resources and dedicated resources. To the extent possible, LandWarNet will use distributed resources that are not dedicated to particular organizations to provision IT services to end-users. At the same time, LandWarNet will contain local and regional resources which maintain quality of service in DIL situations, and maintain resilience in a congested / contested cyber electromagnetic environment. LandWarNet will be virtualized with resilient architectures so that there are few, if any, constraints on which resources can be used to satisfy a particular service request. Ideally, LandWarNet will provide the same IT capabilities to an end-user regardless of user location, DIL situations, or end-user device.

Within this new paradigm, the Warfighting Mission Area (WMA) (represented by G-3/5/7), the Business Mission Area (BMA) (represented by OBT), and the Defense Intelligence Mission Area (DIMA) (represented by Army G-2) continue to be responsible for establishing and validating Army mission and business requirements, and for DOTMLPF-P solutions.

2.3.1 Logical IT Environments

Traditionally, the LandWarNet hardware and software architectures have been logically partitioned into three sub-environments: Enterprise, Installation, and Operational. These sub-environments are described in the following sections. This partitioning recognizes the fact that while the Enterprise IT Environment provides a core set of enterprise services, other IT services are better provided locally at installations (by the Installation IT Environment) or in tactical areas-of-operation (by the Operational IT Environment). It is the intention of the Army that the Enterprise IT Environment will be the provider of IT capabilities and services in preference to the

Installation and Operational IT Environments to the maximum extent practicable that retains operational effectiveness of a lean, lethal, and expeditionary force in line with the Army strategic priorities. This is depicted in Figure 2-1.

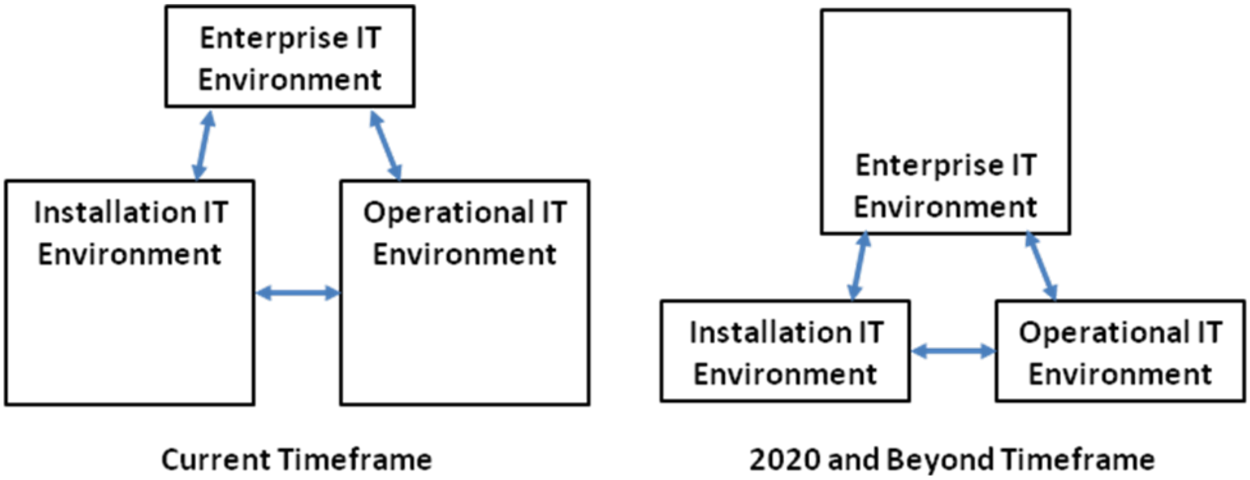
Enterprise IT Environment
Installation IT Environment
Operational IT Environment
Current Timeframe
Enterprise IT Environment
Installation IT Environment
Operational IT Environment
2020 and Beyond Timeframe

Figure 2-1 Paradigm Shift in Relative Sizes of IT Environments

2.3.1.1 Enterprise IT Environment

The Enterprise IT Environment is the portion of the LandWarNet hardware and software architectures that provide global and/or shared IT services. It encompasses all global, regional and inter-installation data transport capabilities, the enterprise-level computing / storage cloud, and all IT services designated as Core Enterprise Services. The Enterprise IT Environment also contains the LandWarNet NetOps and security functionality, except as waived on a system-by-system basis (for example, for tactical networks) in favor of the Installation or Operational IT Environments. It may also contain the connectivity to commercial networks, such as the Internet.

2.3.1.2 Installation IT Environment

The Installation IT Environment is the portion of the LandWarNet hardware and software architectures that provides local IT services on installations for business, education, force projection, readiness, and training purposes. Local IT services are those IT services that are only provided to end-users at a particular installation, or are required to enable the installation to continue operations in the absence of IT services normally provided by the Enterprise IT Environment.

The Installation IT Environment is the aggregate of all of the IT systems that provide local IT services to individual installations. Each installation has a particular instantiation of the Installation IT Environment, which is managed by a single IT authority at the installation.

2.3.1.3 Operational IT Environment

The Operational IT Environment is the portion of the LandWarNet hardware and software architectures that provide local IT services to end-users in deployed areas-of-operation or who are engaged in training exercises, regardless of location. The Operational IT Environment ensures that units maintain critical information flows. It contains local and regional resources. The Operational IT Environment goes out to the point of need (e.g., the tactical edge), and must accommodate operations in Disconnected, Intermittent, Low Bandwidth (DIL) environments.

2.4 Army Enterprise Network Portfolio (AENP)

The Army organizes LandWarNet investments into four mission areas (MAs): WMA, BMA, DIMA, and EIEMA. Each MA is responsible for guiding the investment in, and maintaining oversight over, a specific set of Army capabilities, through the management of an appropriate investment portfolio. The IT investments in each of the four MA portfolios are integrated to form the Army Enterprise Network Portfolio (AENP). The AENP contains all of the IT investments within the LandWarNet, as defined in Section 1.3. This structure is illustrated in Figure 2-2. Note that EIEMA does not have a non-IT portfolio. It is solely focused on IT. Additionally, LandWarNet results from the integration of the IT portfolios from each of the four Army mission areas, not the EIEMA portfolio only.

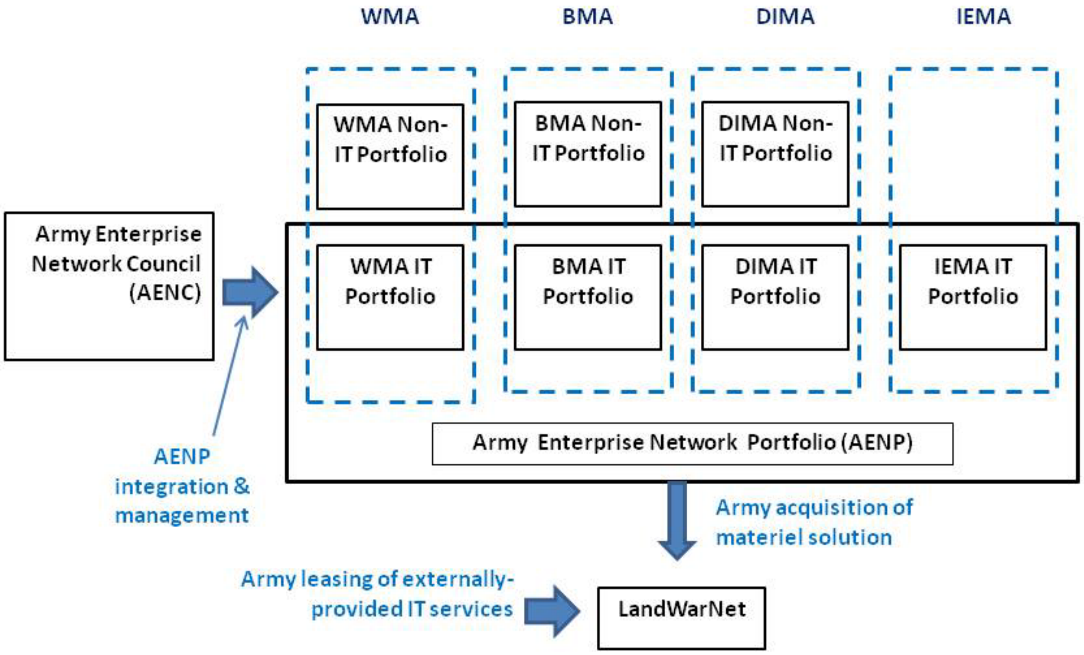
WMA
BMA
DIMA
IEMA
WMA Non-IT Portfolio
BMA Non-IT Portfolio
DIMA Non-IT Portfolio
Army Enterprise Network Council (AENC)
WMA IT Portfolio
BMA IT Portfolio
DIMA IT Portfolio
IEMA IT Portfolio
Army Enterprise Network Portfolio (AENP)
AENP integration & management
Army acquisition of materiel solution
Army leasing of externally-provided IT services
LandWarNet

Figure 2-2 Concept of the Integrated Army Enterprise Network Portfolio

MA portfolios are further divided into functional areas (or domains) that represent common collections of related, or highly dependent, information capabilities and services, such as an end-to-end business process. In general, WMA, BMA, and DIMA manage the portfolios of investments associated with a particular set of capabilities. EIEMA shapes the information environment (that is, LandWarNet) that hosts and executes these mission / business applications. In addition, EIEMA manages the portfolio of Core Enterprise Services (for example, Enterprise email) and the information-related capabilities required of LandWarNet.

The EIEMA is a “supporting” MA, in that its capabilities support and enable the other MAs. The EIEMA portfolio is internally subdivided into the following three functional capability areas: Network Capacity, Core Enterprise Services, and NetOps and Security.

Note that all of the Army’s IT investments, regardless of mission area, are within the purview of CIO/G-6 from the perspective of providing visibility into Army IT expenditures, and of complying with the Army’s technical standards and profiles. Budgetary execution authority remains with the Mission Area proponent.

2.5 Governance, Alignment, and Compliance

The following subsections describe the governance, alignment and compliance aspects of LWN 2020 EA.

2.5.1 Governance

In the context of LWN 2020 EA, governance is the process of controlling the evolution of LandWarNet (towards the objective architecture provided in this document) by actively integrating and managing the entire AENP. The items in the AENP (that is, Army IT investments) are provided by the four mission areas individually in pursuit of their own unique capabilities. These IT investments are derived from validated operational requirements of each MA[2]. Note that most items in the AENP imply changes to the LandWarNet architecture.

This governance is provided by the Army Enterprise Network Council (AENC). The AENC, chaired by CIO/G-6, has two primary roles. First, it is responsible for the integration and optimization of the AENP. Second, it is the governance structure of the EIEMA. In this role, it is analogous to the LandWarNet Mission Command (LM) General Officer Steering Committee (GOSC) in the WMA, and the Army Business Council (ABC) in the BMA.

The AENC makes requirement, technical, architectural, resource, and funding decisions to optimize the AENP in accordance with the ANCP, the DoD IEA, and relevant Army and DoD directives.

The LandWarNet architecture development and governance processes are defined in AR 25-1 (Army Information Technology)[3] and in PAM 25-1-1 (Army Information Technology Implementation Instructions)[4].

[2] The term “operational requirement” has traditionally been applied to the WMA / Operating Force, and generated by G-3/5/7 and TRADOC. This concept has been analogously expanded to the other mission areas.

[3] Reference B-1

[4] Reference B-3

2.5.2 Alignment

Alignment is the degree to which the LandWarNet information environment supports and enables realization of the LWN 2020 EA presented in this document. It is incumbent on all MAs to consider this alignment as a criterion in their IT investment and acquisition decisions. Architecture deviations (that is, planned misalignments from the enterprise architecture) will be assessed by CIO/G-6 and resolved through the MA governance forums, if possible, or be considered for waiver by CIO/G-6 through existing waiver processes. LWN 2020 EA will evolve to remain in alignment with the ANCP, so that all subordinate architectures will continue to be in alignment as well.

2.5.3 Compliance

Four types of compliance are relevant to LandWarNet: interface compliance, security compliance, standards compliance, and architecture compliance. These types of compliance are all applicable to an IT system or component being certified for network connectivity (that is, “networthiness”).

Interface compliance refers to the assurance that IT system / components satisfy the physical and logical connectivity requirements established by 2nd Army, and are compatible with NetOps policies and procedures. Security compliance assures that all of the security requirements imposed by ARCYBER are met, such as integration with the IdAM capabilities. Standards compliance, performed by CIO/G-6, assures that all relevant technical standards and profiles imposed by CIO/G-6 on IT systems / components are satisfied.

Architecture compliance, also monitored by CIO/G-6, refers to compliance with architecture guidance and direction provided in this document, its two annexes, and the associated Reference Architectures. Section 4 describes the purpose / contents of these peripheral documents. Note that the Reference Architectures may impose additional technical standards and profiles.

It is incumbent on the LandWarNet System Architect (that is, ASA(ALT)) to enforce and assess the compliance of each IT component (both individually and collectively) and report the results to CIO/G-6. Additionally, it is the responsibility of CIO/G-6 to certify every IT component for

Network use (as per AR 25-1 [Army Information Technology] and AR 25--2 [Information Assurance]).

3. Architecture Guidance and Direction

This section contains the guidance and direction provided by the Army relative to the LandWarNet end-state architecture. The intended audience for this architecture guidance and direction is defined in Section 1.4. The primary objective of architecture guidance is to inform the development and prioritization of IT investments. These investments will, over time, result in the transformation of the current LandWarNet architecture to enable the realization of the LWN 2020 EA.

Architecture direction captures architecture decisions that have been made by Army senior leadership, such as the decision to adopt a cloud-computing paradigm.

The architecture guidance and direction provided in this document is presented in terms of the desired characteristics and attributes of the end-state architecture. This Section is organized into the seven subsections listed below, which are derived from a similar structure in the DoD IEA. (The use of the term “services” in these categories reflect the overarching concept that LandWarNet is or [will be] a service-oriented architecture).

1. General
2. Communication / Data Transport Services
3. Computing and Storage Services
4. Enterprise and Data Services
5. Mission Application Services
6. End-User / End-User Services
7. Mission Assurance

For the purpose of this document, Mission Assurance is an overall topic that includes NetOps, Cybersecurity, and Information Management (IM).

Annexes A and B and the Reference Architectures also provide architecture guidance and direction (see Section 4).

3.1 General

General architecture guidance and direction appears below:

1. LandWarNet is a single, unified, information environment.
2. LandWarNet is composed of: (a) the IT systems and components (hardware and software), which are physically located on Army installations, in areas-of-operation, or in facilities owned / leased by the Army, and (b) Army application software that is hosted / executed in non-Army facilities (for example, in DoD Enterprise Computing Centers (DECCs)).
3. IT systems and components that are not acquired or owned by Army activities, agencies, or components, but which are used to provide IT services to the Army (for example, commercial SATCOM terminals) via lease agreements (or other business arrangements), are not considered to be part of LandWarNet, but must meet Army and DoD standards to ensure interoperability.
4. LandWarNet is a service-oriented architecture (SOA) that is tailored to a net-centric environment. This may be referred to as a “web-centric” architecture. IT services are transparently provided to end-users on request.
5. LandWarNet provides IT services within the cumulative scope of the service-level agreements (SLA) that exist between CIO/G-6 and end-user organizations (for example, Combatant Commands).
6. All IT systems and components comply with the mandated technical standards and with the constraints of the Common Operating Environment (COE).
7. LandWarNet is standards-based. All IT systems and components will be certified for operational use by CIO/G-6 in coordination with other authorized Army organizations (see Section 2.5.3). Certification criteria are contained in AR 25-1[5] and AR 25-2[6]. Certification will occur at the system, subsystem, or component level, as appropriate.

[5] Reference B-1

[6] Reference B-2

3.2 Communication / Data Transport

The following list contains architecture guidance and direction related to data transport within LandWarNet:

1. Data transport within the LandWarNet infrastructure is accomplished via a hierarchy of interconnected data transport networks, including wide area networks, regional networks, campus networks, local area networks, and tactical networks.
2. All Army installations are connected to one or more inter-installation data transport networks, nominally through the DISA-provided Department of Defense Information Network (DODIN). Army installations may also be connected to diverse networks to improve fault tolerance, availability, and other network characteristics.
3. LandWarNet has sufficient data transport capacity and operational performance to satisfy the Army's communications and data transport usage models. These data transport usage models define peak vs. off-peak requirements, nominal vs. off-nominal requirements (for example, surge), and various quality-of-service (QoS) levels.
4. All communications services (including voice, video, and data) are unified.
5. The number of distinct networks / sub-networks is minimized to the extent possible, consistent with architectural best practice, cost effectiveness, statute, and operational requirements.
6. LandWarNet will accommodate the transfer and processing of data at all security classification levels required by Army mission and business processes. These levels include UNCLASSIFIED, SECRET, TOP SECRET, and SENSITIVE COMPARTMENTED INFORMATION.

3.3 Computing and Storage

End-users and software applications may request computing services from LandWarNet. Data storage and the maintenance of storage directories are autonomous functions performed by middleware, such as database management systems (DBMS). The following includes architecture guidance and direction regarding computing and storage within LandWarNet:

1. Computing within the LandWarNet infrastructure is accomplished via a hierarchy of computational nodes, including Core Data Centers (CDC), Installation Processing Nodes (IPN), Special Purpose Processing Nodes (SPPN), and Tactical / Mobile Processing Nodes (TPN). (Note: two other types of facilities are defined by JIE that do not provide general purpose processing – Installation Service Nodes (ISN) and Geographically Separated Units [GSU]).
2. LandWarNet has sufficient capacity / performance to satisfy the Army's peak vs. off-peak and nominal vs. off-nominal computing usage models.
3. LandWarNet has sufficient capacity / performance to satisfy the Army's peak vs. off-peak and nominal vs. off-nominal storage usage models.
4. LandWarNet follows the paradigm of cloud-based computing. Cloud computing has the following characteristics:
   a) Common resources are allocated as needed among a population of end-users.
   b) Processing and storage are nominally accomplished through distributed resources. At the enterprise level, this is nominally accomplished in large-scale data centers, such as CDCs. At regional and local levels, this is accomplished through harnessing the combined processing and storage capabilities of the available resources / devices.
   c) In general, software is virtualized so that it can be executed on virtual machines.
   d) The mapping of applications and data to physical and/or virtual resources is transparent to end-users. There is also a single framework which allows each level to leverage the other levels when conditions allow, although each level is structured to operate in DIL situations to permit operations in degraded network conditions.

3.4 Enterprise and Data Services

Enterprise services are generic, non-mission-specific services that are available to most if not all Army end-users (for example, enterprise email). Data services are enterprise services that are specifically related to discovering, accessing, and managing data / information. These services are provided by enterprise software and/or middleware. Middleware is the software that implements the foundations of service-oriented and cloud architectures. Examples of middleware include service registration, discovery and brokering capabilities, enterprise search systems, and messaging systems. In this document, enterprise resource planning (ERP) systems are considered to be middleware. The following presents architecture guidance and direction regarding the enterprise services and data services that LandWarNet will provide:

1. Enterprise services consist of two types; services that are explicitly provided by enterprise software (for example, email), and services that are provided by middleware (for example, mission application execution).
2. Enterprise services are not mission or domain-specific.
3. Enterprise services are intended to be available to all Army end-users, but access may be practically constrained by infrastructure constraints, security restrictions, service-level agreement (SLA) constraints, and so on.
4. Enterprise software and middleware are developed, tested and integrated in software development environments compliant with the COE, unless waived on a case-by-case basis by CIO/G-6[7].
5. LandWarNet provides mechanisms for end-users to discover the enterprise and data services available to them, and the conditions of their use. Note: enterprise software and middleware may themselves request enterprise services.
6. LandWarNet provides mechanisms for end-users to discover available data assets, and the data models or schema that define them.
7. Access to enterprise and data services (and the data itself) is controlled via Attribute-Based and Role-Based Access Control methodologies (ABAC and RBAC respectively).

3.5 Mission Application Services

Mission / business applications are IT software components that are identified and acquired by mission areas with direct mission or business responsibilities (that is, by WMA, BMA, and/or

[7] Reference B-7

DIMA), but are hosted and executed by LandwarNet. The following list provides architecture guidance and direction regarding mission / business application services:

1. Mission / business applications are mission- or domain specific.
2. Access to mission / business applications is controlled via RBAC methodologies.
3. Mission / business applications are developed, tested, and integrated in software development environments compliant with the COE, unless waived on a case-by-case basis by CIO/G-6[8].
4. Mission / business applications are executable in one or more of the Computing Environments (CE) defined in the COE[9].
5. Mission / business applications are virtualized to the extent practicable, unless waived on a case-by-case basis by CIO/G-6.
6. LandWarNet provides mechanisms for end-users to discover the mission / business applications available to them, and their intended uses.

3.6 End-Users / End-User Devices

The following provides architecture guidance and direction regarding end-users, and their interactions with LandWarNet:

1. Army end-users span the Total Force.
2. Army end-users interact with LandWarNet through end-user devices. End-user devices are IT hardware components that contain and execute human / machine interface (HMI) software.
3. End-user devices are thin- or zero-client devices (consistent with the cloud-oriented computing paradigm), to the extent possible.

[8] Reference B-7

[9] Reference B-7

4. End-users will have the same user experience (that is, look, feel, content, and utility) regardless of location or end-user device, to the extent practicable.

5. LandWarNet will tailor the “view” presented to each user based on his/her role(s) and the IT capabilities / limitations of his/her end-user device, to the extent possible.

6. All mobile devices are end-user devices.

3.7 Mission Assurance

In this document, mission assurance encompasses three, internally-focused, aspects of LandWarNet: NetOps, Cybersecurity, and Information Management.

3.7.1 Network Operations (NetOps)

NetOps provides the following functionality within LandWarNet:

1. NetOps manages the configuration of IT components (hardware, system software, and middleware) in the LandWarNet operational environment.

2. NetOps manages and controls the flow of data within LandWarNet transport networks (unless this function has been explicitly assigned to another organization, as may be the case for specific tactical networks).

3. NetOps manages and controls operational IT components within LandWarNet to optimize the efficiency and effectiveness of IT service delivery to end-users.

4. NetOps supports the identification, isolation, and resolution of problems that either reduce network availability or impair the ability of end-users to use LandWarNet.

There are two categories of networks for which NetOps is not responsible for providing the above NetOps functionality. The first is networks that provide IT services to Army end-users, but are not “owned” by the Army. For example, DODIN provides wideband data transport services, but is operated by DISA. The second category contains the tactical and other systems for which it is operationally justifiable that NetOps functionality be provided by the tactical units themselves. In both of these cases, NetOps does monitor the traffic entering and leaving LandWarNet from an SLA perspective.

This section contains general architecture guidance and direction regarding LandWarNet NetOps:

1. NetOps manages and controls the LandWarNet network(s) to dynamically optimize the flow of data.
2. NetOps manages and controls operational IT components within LandWarNet to optimize the efficiency and effectiveness of IT service delivery to end-users.
3. NetOps resolves resource contention in the use of network capacity in accordance with Army policy, service-level agreements, and quality-of-service guidelines.
4. LandWarNet provides sufficient operational and status data so that complete operational situational awareness can be achieved (by NetOps).
5. IT components provide sufficient control mechanisms so that the configuration and operations of LandWarNet can be dynamically controlled.
6. All IT components will be capable of being configured remotely.
7. NetOps functionality within LandWarNet is provided by a single organizational entity with access to all LandWarNet operational and status data.
8. NetOps functionality is provided in a consistent, uniform, and standardized manner.
9. NetOps is the organizational entity in LandWarNet responsible for the reporting, tracking, and resolution of end-user problems / issues. The following three categories of problems are within the purview of NetOps:

    a) Problems associated with the use of supported IT components (hardware or software).

    b) Problems associated with the use / availability of provided IT services.

    c) Problems arising from the fact that “expected” IT services are not provided by LandWarNet, or are not accessible by end-users.

3.7.2 Cybersecurity

Cybersecurity refers to the ability to defend LandWarNet from attack in cyberspace. There are three primary aspects of LandWarNet security: (a) the ability to identify authorized end-users and end-user devices (and to enforce their access privileges), (b) the ability to detect attempts at unauthorized access, and (c) the ability to respond appropriately to attacks (whether successful or unsuccessful). These attempts at unauthorized access and cyberspace attacks can be internal or external, and intended or unintended. Architecture guidance regarding the ability of LandWarNet to support offensive actions in cyberspace is not included in this document nor is guidance related to physical security. The following provides architecture guidance and direction regarding Cybersecurity:

1. LandWarNet provides sufficient operational and status data so that complete Cybersecurity situational awareness can be achieved.
2. The Army maintains a cyber threat model for the LandWarNet infrastructure.
3. The LandWarNet infrastructure (including data and information) is (designed to be) protected from the cyber threats identified in the cyber threat model.
4. LandWarNet uses both attribute-based and role-based access control methodologies to control access to its resources. (Note: role-based access control may be considered to be a subset of attribute-based access control).
5. LandWarNet identifies and authenticates end-users via “two-factor” authentication (for example, CAC) that are presented by end-users through end-user devices. Land WarNet will implement the Public Key Infrastructure (PKI) standard that allows for the implementation of PKI technical specifications and algorithms as software components or computer systems.
6. LandWarNet continuously monitors all data transport networks (including tactical networks) to detect unauthorized activities and possible attacks.
7. Cybersecurity for the LandWarNet infrastructure is performed by a single, virtual, organizational entity.

8. LandWarNet minimizes the “threat surface” that is exposed both internally and externally.
9. The Cybersecurity organizational entity (as a single collection point) receives all security-relevant data provided by the LandWarNet infrastructure and generates / maintains complete situational awareness of the state of LandWarNet cybersecurity.
10. LandWarNet has, and enforces, security enclaves at the Secret and Unclassified security classification levels. This includes the policies and mechanism that allow cross-enclave information transfer.
11. End-users, enabled by appropriate end-user devices, have single sign-on (SSO) across LandWarNet.

3.7.3 Information Management (IM)

IM refers to the ability to define and manage data artifacts over their lifecycles. It includes the ability to organize data artifacts, both logically and physically, and allow end-user discovery and access. The following provides architecture guidance and direction regarding Information Management (IM):

1. LandWarNet allocates storage space for, and controls the storage of, all data artifacts. A “data artifact” is a uniquely identifiable set or collection of data items.
2. All data artifacts are tagged according to the LandWarNet Metadata Specification (LMS). The LMS reflects ontology of LandWarNet content. (Note: the LMS has not yet been defined).
3. Data artifacts can be searched / discovered via enterprise services.
4. The physical storage locations of data artifacts are transparent to end-users.
5. Data within LandWarNet is partitioned into two categories: authoritative data and non-authoritative data. Non-authoritative data is any data that is not authoritative, and which may or may not have been derived from authoritative data.
6. Authoritative data is provided and maintained by authoritative data sources (ADS). Data received from ADSs is assumed to be “trustworthy.”

7. Authoritative data is to be used where applicable, in preference to derived data.
8. The semantics of all individual data elements (authoritative and non-authoritative) are defined in logical data models.
9. All structured data assets (organized groups of data elements) are defined by data schema. Unstructured data assets (for example, media files) may or may not have data schema.
10. All data assets are described via standardized metadata. Data assets are characterized and discoverable via their metadata.
11. LandWarNet will detect if data has been altered or corrupted, and restore that data to its intended state.
12. LandWarNet will establish and enforce the “create / read / update / delete” (CRUD) criteria for each authoritative data element.
13. LandWarNet will establish and publish the semantics of each authoritative data element.
14. LandWarNet will actively manage data quality.
15. LandWarNet will assure that authoritative data is consistent, synchronized, and current to the extent possible. LandWarNet will provide “configuration management” over data.
16. LandWarNet will assure that data and information is accessible by multiple end-users simultaneously.
17. LandWarNet will maintain audit trails of all operations performed on authoritative data, and will be able to analyze those audit trails. This includes information to prevent the repudiation of executed operations.

4. Description of Annexes / Reference Architectures

4.1 Annexes

Two annexes accompany this document: Annex A (Technical Standards Guidance), and Annex B (Definitions and Guidance for the Common Operating Environment). These annexes guide and constrain the design of LandWarNet IT materiel solutions with the goal of increasing the level of standardization across LandWarNet.

Annex A establishes the Technical Standards lifecycle management processes by which the Army will effectively manage IT technical standards and profiles, in alignment with DoD mandates. It also provides a Technical Standards maturity model that enables the assessment of the value of individual technical standards.

Annex A describes the Army Technical Guidance Repository (ATGR) used to generate the minimum set of standards that are (or may be) associated with particular IT functions or technologies. The ATGR facilitates the selection of technical standards in the development of reference and solution architectures, and the generation of the Army's standards profiles. Annex A also provides guidance to materiel developers on the process for selecting information technologies and associated emerging standards in order to balance innovation with cost in order to provide our Warfighter and business leaders with technology advantage.

Annex B provides guidance for the implementation of the COE. The COE is a methodology in which the IT components (hardware, software, applications, and services) that provide data processing and data storage capabilities are standardized to the extent that they are able to facilitate the Army's ability to rapidly develop, integrate, certify, and deploy secure and interoperable IT systems and applications. That is, to achieve a balance between unconstrained innovation and standardization. Implementation of the COE will better enable Army communities of interest to produce and/or acquire high-quality applications resulting in improved security, reduced complexities of configuration and support and streamlined training requirements, all resulting in great effectiveness at reduced costs. This Annex also presents a Technical Reference Model (TRM) that illustrates the boundaries and organization of the COE.

4.2 Identification of Reference Architectures

CIO/G-6 develops Army Reference Architectures to further define the characteristics of this enterprise architecture. Current versions and future revisions of these documents will be available on the CIO/G-6 website: http://ciog6.army.mil/Architecture/tabid/146/Default.aspx

5. Way Ahead

To satisfy its intended purposes of informing Army IT investment decisions and providing architecture guidance and direction to LandWarNet stakeholders, LWN 2020 EA must remain aligned with the ANCP, the DoD IEA, and other primary source documents. This document will be revised as needed by the CIO/G-6 Army Architecture Integration Center (AAIC) to address significant changes in the source documents. LWN 2020 EA will continue to address changing missions, operational concepts, and doctrine, and be sensitive to technological advancements and commercial best practices. Changes to LWN 2020 EA may also be warranted by architectural analyses at the system-of-systems and/or solution levels.

Appendix A: Acronyms / Glossary

The Table of Acronyms is presented in Table A-1. The Glossary is presented in Table A-2.

Table A-1 Table of Acronyms

Acronym	Term
AAIC	Army Architecture Integration Center
ABAC	Attribute-Based Access Control
ABC	Army Business Council
ADS	Authoritative Data Source
AENC	Army Enterprise Network Council
AENP	Army Enterprise Network Portfolio
AIA	Army Information Architecture
ANS	Army Network Strategy
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
ATGR	Army Technical Guidance Repository
BMA	Business Mission Area
CE	Computing Environment
COCOM	Combatant Command
COE	Common Operating Environment
CRUD	Create / Read / Update / Delete
DBMS	Database Management System
DECC	Defense Enterprise Computing Center
DIL	Disconnected, Intermittent, Low Bandwidth
DIMA	Defense Intelligence Mission Area
DISA	Defense Information Systems Agency
DoD	Department of Defense

DODIN	Department of Defense Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
EA	Enterprise Architecture
EIEMA	Enterprise Information Environment Mission Area
ERP	Enterprise Resource Planning
GOSC	General Officer Steering Committee
IA	Information Assurance
IdAM	Identity and Access Management
IE (1)	Information Enterprise
IE (2)	Information Environment
IM	Information Management
IPN	Installation Processing Node
IT	Information Technology
JIE	Joint Information Environment
LWN	LandWarNet
LMS	LandWarNet Metadata Specification
MA (1)	Mission Area
MA (2)	Mission Assurrance
NCS	Network Capability Set
NetOps	Network Operations
NIPR	Non-Classified Internet Protocol Router
OBT	Office of Business Transformation
PKI	Public Key Infrastructure
QoS	Quality-of-Service
R&D	Research and Development
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SPPN	Special Purpose Processing Node

SSO	Single Sign-On
TA	Technical Architecture
TPN	Tactical Processing Node
TRADOC	Training and Doctrine Command
TRM	Technical Reference Model
TS/SCI	Top Secret / Sensitive Compartmented Information
UAP	Unified Action Partner
UC	Unified Capabilities
WMA	Warfighting Mission Area

Table B-2 Glossary

Term	Definition
Activity	A unit of effort that, when executed, produces a useful result. Activities are composed of one or more tasks.
Application	A software program that, when executed, causes a computer to perform a specific function, or produce a specific result.
Architecture	The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution. An architecture describes how a system will satisfy its intended purpose.
Architecture Artifact	A human- or machine-consumable product, in any format, that contains information about an architecture.
Architecture Development Process	The Army-level process that specifies how all Army information technology (IT) architectures are developed, and the architecture artifacts that describe them.
Area of Operations	A geographic area, under the operational control of a military commander, in which military operations are (or may be) conducted.
Army Enterprise Architecture	By convention, the Army Enterprise Architecture refers to the IT architecture of the Army (that is, to the LandWarNet architecture).
Business Capability	A capability required by one or more of the following Business Mission Area (BMA) domains (or functional areas): Acquisition, Financial Management, Human Resource Management, Logistics, Installations Energy & Environment, Defense Security Enterprise, Training and Readiness.
Business Mission Area (BMA)	The Army mission area whose portfolio contains those mission-specific investments needed to provide business capabilities. BMA is governed by the Army Business Council.
Capability	The ability to achieve a desired effect under specified standards and conditions.
Capability Gap	A capability that the Army does not currently have, either wholly or in part.
Capability Set	A set of capabilities that are aggregated for the purpose of Operational planning.
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Common Operating Environment	An approved set of IT components (hardware and/or software) and IT technologies whose use is intended to facilitate the Army's ability to rapidly develop, integrate, certify, and deploy secure and interoperable IT systems and applications.
Compliance	A condition in which a person or a system meets applicable mandates, such as standards, policies, procedures, and so on.
Component	A discrete element of a system. Components are hardware, software, or personnel. Systems are composed of components.
Computing Environment	A logical grouping of systems with similar deployment and environmental characteristics used to organize the Common Operating Environment. The six Computing Environments are: Data Center / Cloud, Command Post, Mounted, Mobile / Handheld, Sensor, and Real-Time / Safety Critical / Embedded.
Cybersecurity	A general term that refers to the protection of IT systems and the information contained within them.
Data	Any symbolic or numeric value to which meaning can be assigned.
Domain	A logical partition within a mission area that aligns areas of common operational and functional requirements. Within a mission area, domains are mutually exclusive and collectively exhaustive. (Note: a domain is equivalent to a functional area.)
End State Architecture	An architecture that is desired, or envisioned, to exist at some point in the future. It serves as a goal or objective towards which current architectures can be evolved. It is a "to-be" architecture.
End User Device	A device that provides a human machine interface (HMI), most specifically when connected to a network.
End-to-End (Communications)	Communication that occurs between an originating source and an intended receiver, regardless of the communications path or intermediate relay points.
End-to-End (Process)	The concept that every process has a definable scope and that all activities within that scope are encompassed by the process.
Enterprise	A complex entity that has a mission or goal. An enterprise typically possesses a set of resources that are utilized to accomplish the mission or goal. For the purpose of this document, the enterprise is LandWarNet [2].
Enterprise Architecture (EA)	An architecture whose scope is an enterprise. In general, enterprise architectures are described at higher levels of abstraction.
Enterprise Information Environment Mission Area (EIEMA)	The Army mission area whose portfolio contains the IT investments associated with the network aspects of LandWarNet and the set of enterprise services. The EIEMA is governed by the Army Enterprise Network Council. The EIEMA IT portfolio is the Army Enterprise Network Portfolio.

EIEMA Process	The process that EIEMA executes annually to generate its contribution to the Army Program Objective Memorandum submission and to revise the Army Network Campaign Plan.
Enterprise Service / Core Enterprise Service	A mission-agnostic IT service that enables or supports collaboration and/or communications between two or more users on or over a network. (Note: enterprise services are acquired via the EIEMA portfolio.)
Function	[1] A fundamental operation that is performed by IT systems, such as data processing, data storage, and so on. [2] The role that a component (including personnel) plays in a system. [3] An Army-level function that is equivalent to a domain within a mission area (for example, logistics).
Functional Architecture	An architecture that describes how the functionality of a single domain is provided.
Information	The meaning (semantics) assigned to, and recoverable from, data.
Information Assurance (IA)	A comprehensive that encompasses all of the mechanisms and processes used to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
Information Management (IM)	A comprehensive term that encompasses all of the mechanisms and processes used to manage data / information artifacts throughout their lifecycle.
Information Technology (IT)	A comprehensive term that encompasses all technologies related to the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
IT Architecture	The architecture of IT systems.
IT Capability	A capability whose desired effect is the generation, processing, storage, transmission, display, protection, control, and/or management of data and/or information.
IT Component	A functional component of an IT system, either hardware or software.
IT Portfolio	A set of current and proposed IT investments.
IT Portfolio Management	The process of prioritizing the investments in an IT portfolio to maximize the total expected value of the portfolio (according to a predetermined set of optimization criteria).
IT System	A system that provides IT capabilities.
Infrastructure	A comprehensive term that refers to the set of materiel solutions (hardware and software) in an enterprise or functional domain. (Note: this definition does not include the people or processes that use or operate the infrastructure.)

Installation	A small geographic area which contains one or more discrete facilities in which Army activities are performed. Typically, installations are forts, bases, posts, camps, or stations. Army components such as the ARNG may expand the definition of installation to include states, reservations, etc. as appropriate.
Installation Variant / Variant)	A categorization of Army installations based on their primary purpose. Variants include: Power Projection, Industrial Base, Training Base, and Mobilization Stations and Armories.
Institutional Capability Set	A capability set that contains capabilities required by Army's Generating Force.
Interoperability	The condition achieved when of two or more systems, units, forces, or physical components are able to exchange and use information.
(LandWarNet)	[1] The Army's portion / contribution to the Department of Defense Information Enterprise. [2] The IT environment that provides IT capabilities to Army users and Unified Action Partners. Its scope includes the Army's IT infrastructure plus all of the people, processes, and technologies required to provide those IT capabilities.
LandWarNet Infrastructure	The Army's IT infrastructure, including those infrastructure components leased from other governmental or commercial organizations.
Level of Abstraction	An indication of where on the abstraction continuum (from "conceptual" to "concrete") an architecture artifact lies. Typically, the three values that express levels of abstraction are "conceptual," "logical," and "physical."
Metrics	The elements of a measurement system consisting of key performance indicators, measures, and measurement methodologies.
Mission Area (MA)	A defined area of responsibility within the Army that is responsible for defining and overseeing a particular set of mission or business capabilities. Four mission areas are currently defined within the Army: Warfighting (WMA), Business (BMA), Defense Intelligence (DIMA), and Information Environment (EIEMA).
Mission Area Architecture	An architecture that describes how the capabilities associated with a mission area are achieved.
Mission Capability	A capability required by one or more of the following WMA domains (or functional areas): Intelligence, Movement and Maneuvers, Fires, Protection, Sustainment.
Mission Environment	A physical environment in which IT equipment is located and operated. Mission Environments are characterized by physical and environmental parameters and attributes.
Mobile Device / Handheld Device	An end user device that is not hardwired to a network (that is, a wireless device).
Net-Centric	The condition in which an organization's capabilities are achieved via meaningful interactions over networks.

Network	[1] A system whose function is to connect, and transfer data between, a set of network nodes. [2] (see LandWarNet [2])
Network Capability Set (NCS)	A capability set that contains IT capabilities. (Note: typically, an NCS reflects the organization and/or aggregation of IT capabilities within the EIEMA).
Network Capability Set Reference Architecture (NCSRA)	An Army IT architecture that reflects (at the enterprise level of abstraction) the IT capabilities defined in a particular NCS.
Network Integration Evaluation (NIE)	An activity that integrates and evaluates new IT systems / solutions prior to their being made operational.
Network Node	A device or system that is logically and/or physically connected to a network.
Network Operations	A comprehensive term that encompasses the services, capabilities, and activities needed to manage, operate, maintain, and defend the data transport components of LandWarNet.
Network Roadmap	An artifact generated by EIEMA that specifies the sequence of IT capabilities, and their intended locations, that are planned to be added to (or deleted from) LandWarNet over time. The Network Roadmap is organized by Network Capability Sets (NCS).
Operational Architecture	An architecture that describes (from a mission perspective) an organization’s mission, functional requirements, information requirements, system components, and information flows among the components. (Note: An operational architecture is not equivalent to an operational view (OV) of an architecture).
Operational Capability Set	A capability set that contains the capabilities required by Army’s Operating Force.
Operational Requirement	A mission or business capability that has been approved / validated by an appropriate authority (normally at the Mission Area level). (Note: by convention, operational requirements are equivalent to validated capabilities).
Operational View / Viewpoint	An architecture artifact that describes architecture from the perspective of how the systems specified by the architecture are expected to operate and interact.
Process / Business Process	An ordered sequence of activities that achieves a high-level mission and/or business functions for the Army.
Public Key Infrastructure	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates, for the purpose of secure communications.

Reference Architecture (RA)	An authoritative source of architecture information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.
Rule	A statement that expresses either a decision about architecture or provides guidance / direction regarding the architecture. (Note: in a Rules-Based Architecture, a rule is not an IF/THEN construct).
Rules-Based Architecture	An approach for representing and communicating architectural decisions and guidance in the form of operational and/or technical rules.
Service / IT Service	A mechanism which enables users to request IT capabilities, which are then provided in a manner transparent to the user.
Service Description	The description of a service that specifies: (a) the functionality of the service, including inputs and outputs, (b) the calling and return protocols for the use of the service, and (c) constraints or limitations on the use of the service.
Service Level Agreement	A formal agreement between the customer(s) and the service provider specifying service levels and the terms under which a service or a package of services is provided to the customer.
Shared Computing	An IT architectural concept in which a significant portion of the IT infrastructure is shared (or is potentially shareable) among users. (Note: shared computing is the opposite of dedicated computing).
Software	A general term that refers to computed-executable sequences of instructions which cause the achievement of useful functions or results.
Solution	[1] The set of DOTMLPF changes required to provide a specific mission or business capability. [2] The set of implemented systems that together provide a specific capability.
Solution Architecture	The architecture of a solution. (Note: Solution architecture is equivalent to System architecture at the physical level of abstraction).
Standard	A document (issued by a recognized Standards Development Organization) that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. A standard may also be a specification that establishes requirements for the selection, application, and design criteria for materiel solutions (hardware and/or software).
System	An organized assembly of interacting and interdependent components that may be operated so as to provide a specific set of functions [1]. In the context of AEA, systems encompass the people, IT components (hardware and software), and procedures needed to provide their intended functions.
System Architecture	The portion of an architecture that describes the functional components of systems, their attributes and characteristics, where they are located, and how they are interconnected.

System Requirement	A functional, performance, operational, technical, and/or interface requirement that a system being acquired is contractually obligated to satisfy (as per a contract with an Acquisition Agency).
System View / Viewpoint	An architecture artifact that contains information about system architecture.
System-of-Systems	A set of discrete systems, each of which can be independently acquired and operated, but which together provide a level of functionality that can only be achieved collectively.
System-of-Systems Architecture	The architecture of a system-of-systems.
Task	An atomic (that is, indivisible) action that is performed by an individual, a system, or an organization.
Technical Architecture	A set of IT standards and technical system implementation guidelines which are applicable to the implementation of a system. Additionally, a technical architecture identifies the technologies that are used (or may be used) in a system.
Unified Action Partner	A non-Army entity that may receive IT capabilities and services from Army IT systems, generally for operational and/or training purposes.
User	An entity (human or machine) that is able to request, and make use of, an IT service [2] to meet an operational need.
User Interface	The logical and physical interface between humans and IT systems.
View / Viewpoint	The perspective of an architecture, expressed in an architecture artifact, that provides and organizes architecture data and/or information as required for a particular purpose. In general, views / viewpoints are designed to address the needs of particular classes of stakeholders.
Virtual Machine	A fully functional computer that is abstracted from physical hardware by be means of a software hypervisor.
Virtualization / Server Virtualization	The process of logically configuring and managing computer servers to host multiple virtual machines, and of configuring applications to be executable on virtual machines.
Warfighting Mission Area (WMA)	The Army mission area whose portfolio contains those mission-specific investments needed to provide Mission Capabilities. WMA is governed by the LandWarNet Mission Command General Officer Steering Committee. WMA is traditionally focused on the Brigade echelon and below.
Wireless Communications	The ability to transport data and/or information without the presence of a physical connection.

Appendix B: References

[B-1] AR 25-1, Army Information Technology, CIO/G-6, 25 June 2013 (http://www.adp.army.mil/pdffiles/r25_1.pdf)

[B-2] AR 25-2, Information Assurance, CIO/G-6, 23 March 2009 (http://www.adp.army.mil/pdffiles/r25_1.pdf)

[B-3] DA PAM 25-1-1, Army Information Technology Implementation Instructions CIO/G-6, 25 June 2013 (http://www.adp.army.mil/pdffiles/p25_1_1.pdf)

[B-4] DoD Information Enterprise Architecture (DoD IEA) v2.0, DoD CIO, published July 2012 (http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx)

[B-5] Army Network Campaign Plan (ANCP), CIO/G-6 (to be published in August 2014)

[B-6] Technical Standards Guidance (Annex A to LandWarNet 2020 and Beyond Enterprise Architecture), CIO/G-6, (to be published in August 2014)

[B-7] Definitions and Guidance for the Common Operating Environment (Annex B to LandWarNet 2020 and Beyond Enterprise Architecture), CIO/G-6, (to be published in August 2014)