

Appendix B to LandWarNet 2020 and Beyond Enterprise Architecture

Installation (Post/Camp/Station) Network Architecture



Version 1.0

7 August 2013

Revision History

Revision	Source	Date	Description of Change
V 0.1	SAIS-AOB	24 May 2013	Preliminary Draft
V 0.2	SAIS-AOB	31 May 2013	Draft for Internal Review
V 0.3	SAIS-AOB	11 June 2013	Draft for Form 5 Staffing
V 0.4	SAIS-AOB	1 August 2103	Draft for CIO/G-6 Approval
V 1.0	SAIS-AOB	7 August 2103	Document Approved

Executive Summary

Army Installation Networks have evolved rapidly over the past 20 years and include support to the Department of Defense (DOD), Joint, Agency, Army, and other Services with workplace, mobile user, and unique sensor IT requirements. Initially, installations were managed and resourced by Army Major Commands and their subordinate commands. As information technology matured and senior installation commanders identified administrative, training, and operational information technology requirements, they developed and resourced local solutions. Recently the Army has implemented a strategy to standardize Army Network standards, services, resourcing and command and control under a single network provider. More recently, over the past 10 years the Army has focused on enhancing LandWarNet support to the Warfighter globally in the Operational Theaters. As Army operational forces transition back to CONUS the network will be critical to providing Warfighters with the ability to train as they fight through developing the capability of "Installation as Docking Stations".

LandWarNet 2020 and Beyond provides the following vision: "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." This document builds on the vision and describes objectives that define the LandWarNet 2020 and Beyond Architecture as it relates to the Army's Installation IT Environment (IIE). By doing so, this document will inform Army IT network investment and design decisions, ensuring IT capabilities are developed in accordance with both the LandWarNet 2020 and Beyond vision and the LandWarNet 2020 and Beyond Strategy executed via the Integrated Network Plan.

Appendix B of the LandWarNet and Beyond Enterprise Architecture supplies the end state objectives that define the network architecture for the Army's CONUS and OCONUS-based, fixed, semi-fixed, and Joint service installations as well as special purpose campuses and facilities for which the Army has responsibility. It provides a sufficient level of detail to inform design and investment decisions, but not to the specificity of "reference" architectures or technical "design books" that provide system, solution, or implementation levels of detail.

This document will be reviewed annually, and updated based on: 1) enduring changes in the LandWarNet 2020 and Beyond Enterprise Architecture; and 2) revisions to the CIO/G6 Army Network Strategy in regards to emerging technology for the End-State architecture.

Approved By:



Mr. Gary Blohm

Director, Army Architecture Integration Center

CIO/G-6

Table of Content

Executive Summary	3
Table of Content	5
1. Introduction	6
1.1. Background	6
1.2. Purpose	7
1.3. Scope	7
1.4. Approach	8
2. Network Components on an Installation	8
2.1. Transport	9
2.2. Computing	10
2.3. Applications	10
2.4. Services	12
2.5. Data	13
3. Installation IT Environment (IIE)	13
3.1. Network Enterprise Center (NEC) Mission Environment	15
3.2. Workplace Mission Environment	16
3.3. Mobile User Mission Environment	18
3.4. Sensor Mission Environment	19
3.5. Installation as A Docking Station (IADS)	20
3.6. Variations Between Installations	22
4. Summary	22
TAB A – Acronyms	24
TAB B – References	26

1. Introduction

The Secretary of the Army includes network modernizations as one of his top priorities. With tighter budgets but an active threat environment, the Army will have to produce a force that is smaller yet still highly capable. The Network is the core of that smaller but highly capable force. Army Directive 2013-02, "The entire network must be treated as a single entity, unified from the Global Information Grid to the installation to the farthest tactical edge, and provide the integrated capabilities that support a seamless link from home station, through the enterprise, to the lone dismounted Soldier in theater"¹. This means the Army must design, develop, acquire and field the network in a comprehensive, synchronized manner. The Army's re-stationing of forces from Europe to CONUS and the return of forces from Southwest Asia (SWA) to their home stations means that over 80% of the Army's forces will be stationed on Army installations in CONUS. As a result, the center of gravity for the Army's LandWarNet 2020 and Beyond Strategy will be the Army's Installation IT Environment in order to achieve the seamless integration of Operational Force IT capabilities, support the growing IT requirements of the Army's business users, and fully align with the Joint Information Environment. This appendix addresses the Installation component of LandWarNet, the Army Network and the end state of the installation IT environment.

1.1. Background

Army installation networks have evolved rapidly over the past 20 years and include support to the Department of Defense (DOD), Joint, Agency, Army, and other Services with workplace, mobile user, and unique sensor IT requirements. Initially, installations were managed and resourced by Army Major Commands and their subordinate commands. As information technology matured and installation senior mission commanders and installation tenants identified administrative, training, and operational information technology requirements, they developed and resourced local solutions. Recently the Army has implemented a strategy to standardize Army Network standards, services, resourcing and command and control under a

¹ Department of the Army Memorandum, SUBJECT: Army Directive 2013 – 02, SUBJECT: (Network2020 and Beyond: The Way Forward), dated 11 March 2013.

single network provider.² Rapid change in the Army installation network Architecture and IT solutions will continue as technology, national strategy, operational requirements, and the global cyber threat continue to evolve and as available network resources and force structure contract. As an appendix to LandWarNet 2020 and Beyond Enterprise Architecture, Appendix B describes Installation IT Architecture for all network components of the Army's installation network including transport, applications, computing, services, and data in support of Army LWN 2020 and Beyond Strategy, aligned with the Joint Information Environment (JIE).

1.2. Purpose

This document describes the end state objectives that define the LandWarNet 2020 and Beyond Architecture as it relates to the Army's Installation IT Environment (IIE). Its purpose is to inform Army IT network investment and design decisions, ensuring IT capabilities are developed in accordance with the LandWarNet 2020 and Beyond vision.

1.3. Scope

Appendix B supplies the guidance, rules, and objectives that define the network architecture for the Army's CONUS and OCONUS-based, fixed, semi-fixed, and Joint service installations as well as special purpose campuses and facilities for which the Army has responsibility. This document uses the Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms* ³definition for an installation: "A grouping of facilities, located in the same vicinity, which support particular functions. A base or group of installations for which a local commander is responsible, consisting of facilities necessary for support of Army activities including security, internal lines of communications, utilities, plants and systems, and real property for which the Army has operating responsibility." In Appendix B, all posts, camps, stations, and bases are referred to as installations. This appendix applies to the entire installation network, which begins at the installation Point of Presence (PoP), Figure 1, and extends throughout the rest of the installation. It provides a sufficient level of detail to inform design and investment decisions, but not to the specificity of "reference" architectures or technical "design books" that provide

² Department of the Army Memorandum, Subject: Transition of All Army Network to the LandWarNet, dated November 16, 2012.

³ Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, dated November 2010, as Amended through 13 March 2013.

system, solution, or implementation levels of detail. Figure 1 also depicts the LWN 2020 EA from a functional perspective, showing the three IT Environments.

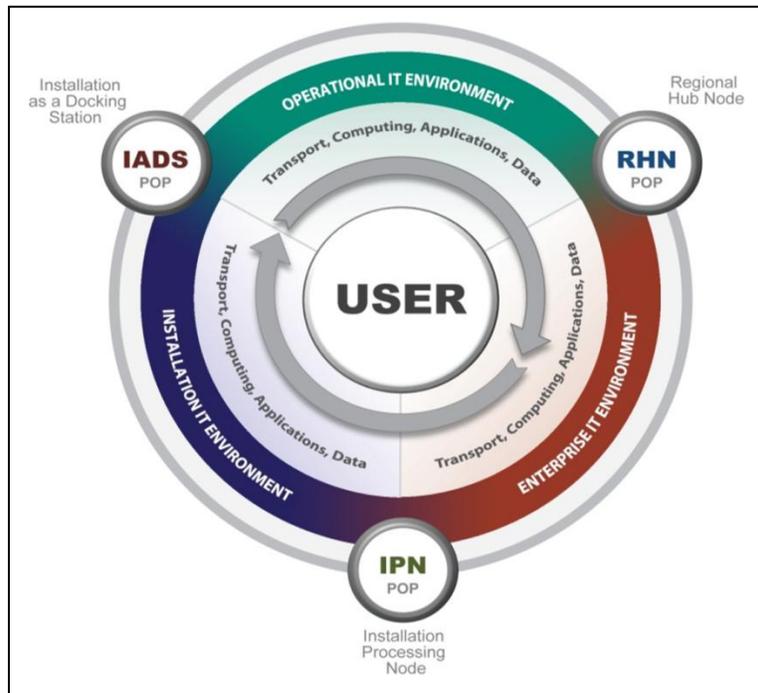


Figure 1: LandWarNet Functional View - Network Environments Approach

Appendix B describes the LandWarNet Enterprise Architecture end-state for the Army's installation network. This appendix follows architectural objectives from the LandWarNet 2020 & Beyond Enterprise Architecture and translates them to address the unique network architecture of the Installation IT Environment. It follows the Mission Environment (ME) and network component framework laid out in the LandWarNet 2020 & Beyond Enterprise Architecture document. This appendix translates applicable architecture objectives into specific end-state guidance.

2. Network Components on an Installation

The LandWarNet Concept of Operations describes “one Army battle command system” as part of “one network” which facilitates a consistent alignment of joint capabilities across all layers of

the network including platforms and sensors, applications, services, transport, and standards. It also describes LandWarNet as an integrated system of systems - underpinned by integrated architectures - that provides the link from Soldier to sustaining base, with tailored software applications that are optimized for conducting joint operations.⁴ This integrated LandWarNet architecture framework describes IT network component material solutions: Transport, Computing, Applications, Services, Data Management. These network component solutions are tailored to support the unique installation garrison and tenant functional missions as required within the overall approved architectural framework.

2.1. Transport

Intra-Installation transport. Voice, video and data information will use various transport solutions on an Army installation. The primary IP network transport infrastructure solution on an Army installation consists of fiber optic cable, coaxial cable or twisted pair cable (and other IP network transport components such as switches, routers, and other IP unique components) which interconnect all key buildings, facilities, ranges, training areas, airfields, and maintenance facilities to the NEC or other supporting network management capabilities. Directional line of sight microwave radio systems are used on many installations to augment an installation's cable infrastructure. Wi-Fi or other wireless IP transport systems are also used to interconnect installation facilities or mobile users. Non IP transport systems include broadcast radio, public safety and special purpose dedicated radio, commercial wire and wireless telephone and data systems and satellite based transport systems. The NEC is generally responsible for managing intra-installation network transport capabilities.

Inter-Installation transport. Network transport solutions between installations (sometimes called long-haul or wide area networks) are generally considered to be enterprise network capabilities and are normally provided through a combination of commercial providers contracted through DISA and dedicated Army and DoD network components and management services. Enterprise transport means include fiber optic (and other) cable, satellite (commercial and military) and microwave line of sight solutions (also commercial and military). Enterprise transport supporting infrastructure includes enterprise IP solutions (routers, switches, etc.) as well as legacy circuit based switching of various technologies.

⁴ TRADOC Pamphlet 525-5-600, The United States Army's Concept of Operations, LandWarNet 2015, dated 11 February 2008.

2.2. Computing

Army installations provide general purpose computing support to installation garrison and tenant users. This computing capability is either provided to installation tenants as an enterprise service or as a local service managed by the Network Enterprise Center (NEC). General purpose computing supports most common user application and storage requirements as well as some tenant-funded special purpose application and computing requirements. Installation computing support is provided through one of the following means:

- **Enterprise Computing.** Enterprise computing services provided by an off-installation or commercial computing service provider (i.e. DoD enterprise or commercially contracted computing center).
- **Regional Computing.** Army computing services supporting Regional Army computing requirements (i.e. Army provided or commercially contracted regional computing center).
- **Installation Computing.** Computing services provided by and managed by the NEC in support of local installation users. Installation computing can be provided, as required, to support off installation users.
- **Special Purpose Computing.** Specialized, function specific computing services that cannot be supported by the installation computing center. Special purpose computing may or may not be located at a NEC facility. Examples of special purpose computing include; research and development (R&D) laboratories, intelligence, medical, battle labs, simulation centers, classrooms, ranges, airfields, etc.

2.3. Applications

Applications represent the software that capture, accesses, manipulate, and present data in support of specific functional missions or general purpose information exchange requirements. Applications are hosted in a variety of computing environments based on technology and mission requirements. For the purposes of this appendix, applications can either be accessed by users directly on their own user systems (physically loaded into a user's computer hardware) or remotely accessed (via thin-client or web based access) using user systems. Applications support specific user voice, data and video information exchange or management requirements. Whether managed and operated by the user or accessed remotely, a networked application is periodically or continuously connected to a network specifically designed to support information

exchange with other applications. Applications can either be mission or functionally specific, enterprise, or infrastructure related. Although today most software based applications are IP based, unique non-IP applications will be considered as exceptions. This appendix will focus on IP based applications as they relate to the functional purpose for which they are designed – not how they are acquired or managed within the formal Army mission area portfolio process. Applications used on an installation are generally classified as either business applications or mission command applications. The examples listed below are meant to be illustrative and not an exhaustive list:

- **Business Applications:**

This category includes but is not limited to:

- **Enterprise Resource Planning (ERP):** Financial, personnel, logistics, medical and others.
 - **General purpose Collaboration and Data Sharing:** Office voice, email, video teleconferencing, white boarding, imagery, and others applications: (document development, spreadsheet, database management, music, graphics, modeling and simulation, photography, gaming, video, and others.
 - **Special Purpose:** Modeling and Simulation, training, manufacturing, R&D sensor management, and many others.
 - **Network Management Applications:** used to control network components (transport, data, services, and computing environments) that provide the infrastructure that support information exchange via applications.
- **Mission Command Applications:**
- **Intelligence Applications:** This category includes strategic intelligence capabilities and functions provided by national and joint assets and provided as a service to national and Department of Defense (DoD) forces through classified network access services. Deployed tactical forces access these capabilities and applications through JWICS or other Intelligence Community (IC) networks or they are delivered to deployed commanders via organic networks.
-

-
- **Warfighting Applications:** This category includes Army, Joint, allied and coalition applications that support Joint Planning and Force Management, Maneuver, Intelligence, Fires, Protection, and Sustainment. (Note: Many Army Mission Command and functional warfighting applications are not available through the enterprise as they reside only in the command post. The Army 'End State' network goals include transitioning converged Operations-Intelligence (OPS-Intel) applications to the enterprise to support home station, ARFORGEN and Phase 0 – 5 operations, while retaining the right balance of capabilities at the command post to allow the commander to continue operations when temporarily disconnected from the network.)

2.4. Services

The installation network supports locally provided network services as well as enterprise network services that are managed by the Army, DoD, agencies, or commercial providers and extended to the installation. Services are described as those enterprise and local network capabilities that allow installation users to access Internet Protocol (IP) or Non-Internet Protocol capabilities which provide specific network user services.

- **Enterprise Network Services:**

- **IP Services:** Network services are extended into Army installations from the enterprise to allow installation users (with the appropriate permissions) to “access” enterprise and local applications and collaboration resources at the appropriate classification level. Army installations are generally supported by three primary IP Network Services: NIPRNET (sensitive but unclassified); SIPRNET (Secret) and Joint Worldwide Intelligence Communications System (JWICS) Top Secret /Sensitive Compartmented Information (TS/SCI). Other IP Networks may be extended to designated installation network users based on specific mission or functional requirements.

- **Non IP Services:** Although the Army is moving toward an everything-over-IP (EoIP) network architecture some functional mission requirements continue to use network services that are not IP based. These services can be enterprise provided (circuit switched video and telephony) or installation provided (manufacturing process, sensors, etc.).

— **NetOps:** Network Operations is a critical network services component that supports network management and control functions including IP and Non-IP based capabilities. These include: spectrum management, network management, identity management, services management, knowledge management, crypto management, and computer network defense. NetOps has both enterprise and installation level functions.

— **End-User Services:** End user services describe specific user capabilities such as voice, data and video collaboration, email, imagery, geospatial, directory services, content discovery, content delivery, storage, help desk, and others. End-User services are currently delivered by several technologies including dedicated circuits, and appropriate Enterprise IP Network Services. End-User services can also be delivered wirelessly. Wireless end user services can be provided by the NEC, commercial providers and by the owning organization as required to satisfy the mission requirements in accordance with DoD policy.⁵

2.5. Data

Data management for the purposes of this appendix data refers to information that has been created or translated to an electronic format. Such data is stored within a computing environment and manipulated through an application or a network service. The Army Information Architecture (AIA) describes, prescribes, and specifies the elements, the behavior of the elements, and the relationships among the elements, that comprise the data required by Army users and business processes.

3. Installation IT Environment (IIE)

For this Appendix, the Installation IT Environment (IIE) includes all of the network systems and capabilities required to support an installation's tenant mission network requirements. Every Army installation is unique in geography, topography, environment, facilities infrastructure, tenant units and supporting network infrastructures. As described in the LWN 2020 EA, this document uses mission environments to provide better fidelity into the IT capability requirements on an installation. Figure 4 provides a graphical representation of Installation Mission Environments (ME) and Control Points (CP).

⁵ Department of Defense Memorandum, SUBJECT: Department of Defense Mobile Device Strategy, dated June 8, 2012.

The following sections describe each ME in terms of the five network components and provides associated clear end-state architecture guidance. These sections provide sufficient detail to support the development of Network Capability Sets (NCS) and reference architectures. More detailed System of System, System, Solution, and Implementation level architectures will adjust for installation different mission variants (i.e. Power Projection Platforms, Training Bases, Industrial Bases, and Army Mobilization Stations and Army Reserve Center or National Guard Armories), topography, and other unique characteristics.

Control Points in Figure 4 are conceptual and used to depict an exchange interface points between two or more mission environments that enable operational data exchange between the environments. The Control Points describe ME boundaries that often require different transport, computing, application, services and data solutions to support information exchange in that mission environment.

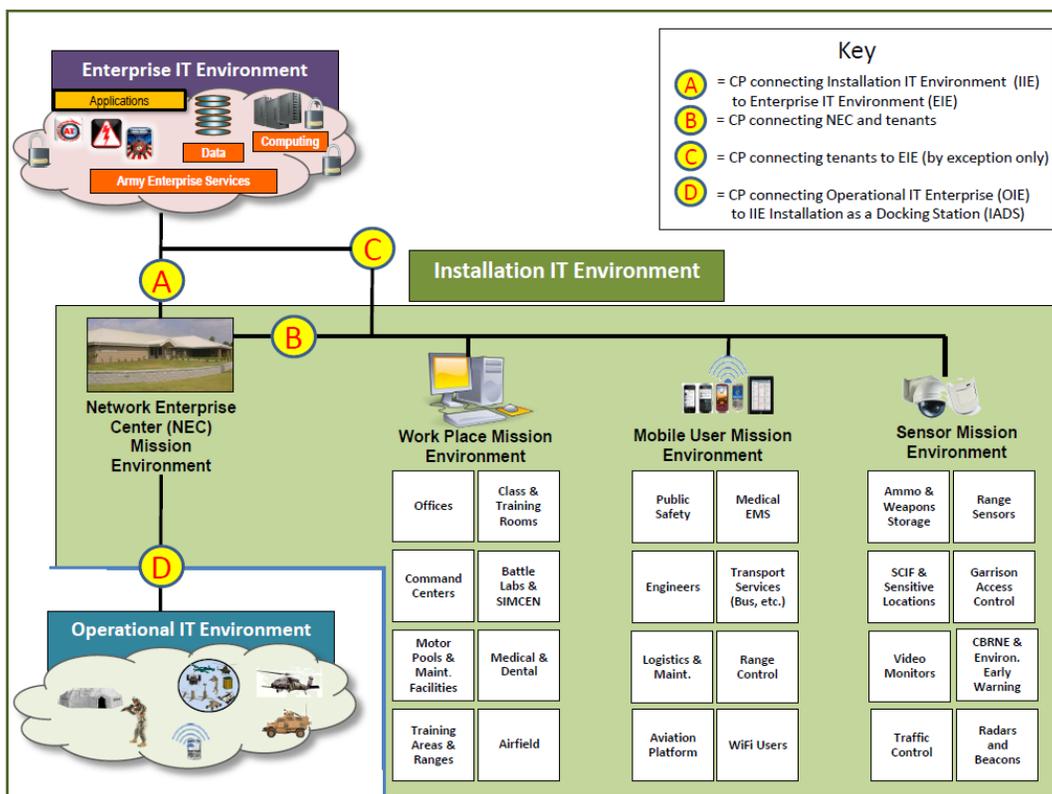


Figure 2: Installation Mission Environments and Control Points

3.1. Network Enterprise Center (NEC) Mission Environment

The NEC ME is the primary IT services provider on an installation. The NEC is also the primary interface between the installation and the Enterprise IT Environment (EIE). The NEC manages the intra-installation campus area network that includes: transport, application hosting and management, computing services, data management services, and network operations. The NEC coordinates with Army and DoD enterprise network providers and network managers to ensure continuous support to its tenant network users. The NEC also supports the Army's coordination and collaboration with local civil and commercial community network capability providers and spectrum managers.

LandWarNet 2020 and Beyond NEC end state architecture guidance includes:

- **The Installation Service Node.** The physical instantiation of the Army's network enterprise at an installation. It includes all networks capabilities and components and represents a virtual extension of Army and DOD enterprise capabilities to the installation and will be responsible for the delivery of services to tenant users on an installation, P/C/S.
- **Application Hosting.** The default hosting option for all installation applications will be an off-installation Army or Joint Computing Center. Applications and services will only be hosted locally if there is a requirement for a capability for a unique tenant functional mission. All ISN hosted applications and services will have a Quality of Service (QoS) agreement with their users.
- **Installation Network Services.** Locally managed network services will be aligned with functional mission owner in order to detect mission impacts from service disruptions.
- **Network Security.** Network security for the NEC ME will follow the Single Security Architecture (SSA) Reference Architecture (RA) and the prescribed JIE security model.
- **Network Operations and Service Management.** NetOps and service management will be primarily an enterprise function. Installation unique NetOps and service management capabilities will be limited to unique installation network service requirements.
- **Installation Network Infrastructure.** All materiel solution architectures will be traceable to approved requirements and technical standards. Architectures will be validated through the Network Mission Area (NMA) process.

Table 1 displays the capabilities that will be resident in the Installation NEC ME Architecture by 2020.

Table 1: NEC / IPN Mission Environment End-State

NEC Mission Environment End State		
Transport	Enterprise	Diverse, multiple enterprise fiber optic cable paths to the installation - redundancy and assured communications
		Enterprise transport convergence - Everything over IP - reduce, eliminate non IP transport requirements
		On demand transport capacity
	Installation	Diverse installation transport capability: Fiber, Wireless, LOS Microwave and Radio
		Installation transport convergence - Everything over IP
Computing	Enterprise	Enterprise Computing Centers - primary support to installation and deployed operational users
		Army Regional Computing Centers - secondary support to installation and deployed operational users
		Installation Computing Centers - support to special purpose installation and deployed operational users
	Installation	Functional or Mission Specific Computing - dedicated computing for specified mission purposes only
Services	Enterprise	Network Operations - primary NetOps for installation
		Services Management - Enterprise Service Management is the primary services management for the installation
		Single Security Architecture (SSA) - primary security architecture for installation access to enterprise networks
	Installation	Installation managed network management and services management will be minimized
		Accessible from any installation workplace or mobile environment
Applications	Enterprise	Trusted user access to installation and enterprise services
		On-demand capacity and self-provisioned services that can scale, as required to user needs
	Installation	Enterprise applications available to all users that are secure, highly scalable, and can be rapidly configured and deployed
		The default host location for all applications will be an Army Core Data Center (CDC) or other enterprise location
Data	Enterprise	Installation tenant functional or mission required unique applications can be hosted in an installation computing center
		Installation tenant functional or mission specific applications hosted in installation computing centers will include Quality of Service (QoS) measures
	Installation	Installation data stored in Enterprise or Regional Computing Centers (primary)
		Enterprise data is visible, accessible and understandable based on user access and security privileges
	Installation tenant functional or mission specific data hosted in installation computing centers will include Quality of Service (QoS) measures.	
	Installation tenant functional or mission unique data will be visible, accessible and understandable based on user access and security privileges	

3.2. Workplace Mission Environment

The installation Workplace Mission Environment describes the physical location on an installation where users access and use network capabilities. The installation’s office buildings, hospitals, labs, and other permanent facilities usually fit into the Workplace ME. Similar to the NEC ME, the Workplace ME usually has high speed, reliable bandwidth that is both fixed (e.g. fiber) and wireless. Computing capacity and power is robust with capabilities being provided locally via desktops/laptops or consumed as a service (e.g. thin/zero client) from the NEC ME or EIE. Army IT users in the Workplace ME are consumers, rather than providers, of services, which will be delivered by or through the NEC ME. Finally, the workplace ME can be both a data producer and data consumer. Data in this ME is usually functionally related to the tenant’s mission and, when consumed, is dynamically integrated with other information assets to enable

decisions at all levels. The following guidance further defines the Workplace ME as part of the LandWarNet 2020 and Beyond vision for the installation:

- **Computing.** Computing capacity within the Workplace ME, when not already provided as a service by the EIE or NEC ME, will be visible and manageable by the same.
- **Applications.** Applications will be developed as enterprise applications unless otherwise approved by NMA guidance.
- **Services.** The delivery of all services to the Workplace ME will be orchestrated through the NEC ME.
- **Network materiel solutions.** All materiel solution architectures will be traceable to approved functional requirements and technical standards. Architectures will be validated through the NMA process.
- **User Identity.** User interfaces will be role based wherever possible and will follow the Identity and Access Management (IdAM) Reference Architecture.

Table 2 displays the capabilities that will be resident in the Installation Work Place ME Architecture by 2020.

Table 2: Installation Work Place Mission Environment End State

Installation Work Place Mission Environment End State	
Transport	Diverse installation transport capability: Fiber, Wireless, LOS Microwave and Radio
	Installation transport convergence - Everything over IP
	High capacity installation transport - supports access to enterprise network services
Computing	Enterprise computing unless otherwise approved
	Installation tenant functional or mission unique, when not nested in the NEC computing center, will be visible to the NEC
	Primary installation workplace computing will be and approved end-user device
Services	Installation tenant computing will be device agnostic
	Installation tenant users have a single service desk interface
	Installation tenant users have a single enterprise identity that allows access to required information & services across organizational and security boundaries
	Installation tenant users will receive enterprise NetOps support under a single network common
	Installation tenant user access to network services will be role based IAW Army Identity and Access Management (IdAM) policy and architecture
Applications	Installation tenants will receive all services (enterprise and installation) through the NEC
	Installation tenant users will access Warfighting and Business Applications from the enterprise
	Applications designed for enterprise consumption and will reside in Army or Joint Cloud Computing environment
	Installation tenant functional or mission unique applications will be hosted in the NEC as an exception to the enterprise hosting policy
Data	Installation tenant functional or mission unique applications will be visible to the enterprise IAW appropriate access and security policies
	Installation tenants will access enterprise and locally hosted data through the NEC

3.3. Mobile User Mission Environment

Mobile users are becoming more commonplace on all Army installations. Whether they are Department of the Army Civilians using personal electronic devices (PED), emergency medical personnel, or maintenance workers performing base operations support (BASEOPS), or mobile users using government capabilities to access Army network services what they all have in common is wireless network access. Transport requirements for the Mobile User ME are usually lower than that of a Workplace ME. Today, mobile computing capability exceeds the capabilities of most installation wireless network capabilities. Most mobile users access enterprise applications which are, for the most part, not hosted in an installation computing environment. Network Operations and network service management for mobile devices will follow the same architecture as fiber/cable NetOps – enterprise focused with NEC provided NetOps on an exception basis.

As the Army makes IT investments that move the Mobile User ME closer to the LandWarNet 2020 and Beyond vision the following architecture guidance be followed:

- **Mobile Applications.** Designed as enterprise applications.
- **Materiel Solutions.** All materiel solution architectures will be traceable to approved functional requirements and technical standards. Architectures will be validated through the NMA process.

The following table displays the capabilities that will be resident in the Mobile User ME Architecture by 2020.

Table 3: Installation Mobile User Mission Environment End State

Installation Mobile User Mission Environment End State	
Transport	Diverse installation transport capability - wireless, broadcast, radio and commercial mobile
	Mobility standard is Everything over IP (EoIP) - unless mission or technology limitations dictate otherwise
	Installation will support IADS mobile device access to the installation or enterprise environment IAW IADS policy and architecture
	Mobile transport will comply with the National Telecommunications Information Administration Federal Spectrum Efficiency Mandate and the Association of Public-Safety Communications Officials Project 25 (P25) Interoperability Standard
Computing	Approved mobile devices will access installation or enterprise computing centers
	Mobile devices will be hardware agnostic unless commercial or military mobile services require otherwise
Services	NetOps of installation mobile networks will be negotiated based on technology, mission and NetOps tool capabilities
	A single identity available across the enterprise to improve access control to systems and data IAW mobile network access policies and architecture
Applications	The default host location for mobile applications will be a core data center (CDC) or other enterprise location IAW mobile network access policies and architecture
	Applications will be designed for enterprise consumption
	Installation unique functional or mission specific mobile applications will be hosted at the NEC but accessible to the enterprise IAW mobile network access policies and architecture
Data	The default host location for mobile data will be a core data center (CDC) or other enterprise location IAW mobile network access policies and architecture
	Installation unique functional or mission specific mobile applications will be hosted at the NEC but accessible to the enterprise IAW mobile network access policies and architecture

3.4. Sensor Mission Environment

From video monitoring, to weapons storage, to access control, the installation sensor environment is primarily focused on force protection, safety and installation infrastructure management. The Sensor ME will use all installation network capabilities and components. For the Sensor ME transport, applications, services and computing requirements may be unique based on the primary function of the sensor and the integrated sensor network. As the Army makes IT investments that move the Sensor ME closer to the LandWarNet 2020 and Beyond vision, it is imperative that the following architecture guidance be followed and implemented.

- Sensor transport. Sensors will use the installation network transport solution that best supports its functional purpose.
- Sensor data storage and management is usually installation specific and is based on ISN-centric architectures. Installation sensor data is shared with enterprise sensor data users in accordance with mission requirements.

- All Sensor materiel solution architectures will be traceable to approved functional requirements and technical standards compatible with the installation network infrastructure. Architectures will be validated through the NMA process.

Table 4 displays the capabilities that will be resident in the Sensor ME Architecture by 2020.

Table 4: Installation Sensor Mission Environment End State

Installation Sensor Mission Environment End State	
Transport	Installation Sensors will use installation transport capabilities unless unique sensor technology or security requirements demand a stand alone solution
	Wireless sensor transport will comply with the National Telecommunications Information Administration Federal spectrum efficiency mandate and the Association of Public-Safety Communications Officials Project 25 (P25) Interoperability Standard
Computing	Sensors will use the NEC or enterprise computing environment unless unique sensor technology or security requirements demand a stand alone solution
	Sensor Computing capability, when not managed by the NEC, will be visible to the NEC
Services	Sensors which use NEC or enterprise network capabilities will be integrated into the Army's NetOps policies and architecture
	Where possible sensors will be given a unique network identity
	Installation sensor network status will be visible to appropriate installation functional or mission managers as well as the network manager
Applications	Unique Installation Sensor applications will be hosted in the NEC unless unique sensor technology or security requirements demand a stand alone solution
	Installation sensor applications will be standardized across all installations unless installation unique public safety or security requirements demand an installation unique solution
Data	Installation sensor data will be available to authorized users IAW established policies and architecture

3.5. Installation as A Docking Station (IADS)

The IADS is a standardized procedure for connecting Operating Force Mission Command applications (such as currently hosted/accessed on the Battle Command Common Services [BCCS], etc.) to their Home Station network infrastructure to allow Commanders and Soldiers in garrison to continuously operate tactical Mission Command systems, maintain unit readiness and sustain Soldier proficiency in an operational mission environment. The intent of the IADS initiative is to use the installation network to support Mission Command connectivity (instead of the units own tactical network transport systems, WIN-T, etc.) to maintain 24/7 connectivity in support of training and mission rehearsals. IADS includes the requirement for tactical tenants to access specified Mission Command applications from their work place, from mobile tactical platforms in the motor pool or training areas and the use of tactical mobile hand held devices on

the installation without having to install their own tactical network systems. The NEC will be the primary provider of Operating Forces IADS connectivity to Joint mission environments. Control Point D, in Figure 2, represents the Installation as a Docking Station interface between installation tenant Operating Force network capabilities and supporting installation network capabilities and services. As the IADS concept evolves, the installation network will have to accommodate the various Operational IT Environment mission environments directly into the installation network. Appendix D: Deployed Tactical Network Architecture End-State Guidance, which has more detailed information regarding the Operational IT Environment network, identifies the following as operational MEs: Command Post, Mobile Platform, Dismounted Soldier, and Tactical Sensors. Regardless of whether IADS technologies are provided by the NEC or another provider, the LandWarNet 2020 and Beyond strategy requires that installation IADS architectures be traceable to approved functional requirements and technical standards. As the Army makes IT investments that move IADS closer to the LandWarNet 2020 and Beyond vision, it is imperative to adhere to the end state guidance.

Table 5 displays the capabilities that will be resident in the Installation as a Docking Station Architecture by 2020.

Table 5: Installation as A Docking Station End State

Installation As a Docking Station End State	
Transport	Installation IADS users will use NEC provided installation wired or wireless IP transport capabilities to connect to the JIE
	Installation IADS users can connect tactical mobile devices will be able to connect directly to the installation mobile transport capabilities at the workplace, motor pool, training areas or ranges
Computing	Installation IADS user computing capability, when not hosted by the NEC, will be visible to the NEC
Services	Installation IADS Mission Command application users will be supported by JIE NetOps and Enterprise Service Management
	Installation IADS users will have trusted access to the network and the Joint Information Environment
	When connected to the network installation IADS user computing and applications will be continuously monitored for network compliance with Army and DoD policies
Applications	Installation IADS users will have a single identity available across the enterprise
	IADS Warfighting Applications will be hosted in the organizations tactical computing environment or in the enterprise IAW technology limitations imposed by unique applications, operational necessity and security requirements
Data	Mission Command applications will be re-designed to be hosed in the enterprise computing environment
	TBD

3.6. Variations Between Installations

Installations serve various purposes and are shaped to support the mission needs of a specific major tenant organization. Some installations are identified as Power Projection Platforms (PPP) to support the Army Forces Generation (ARFORGEN) requirements. Other installations are identified as Training Base installations to support the Training and Doctrine Command (TRADOC) institutional training missions. Army Materiel Command (AMC) is normally associated with Industrial Base installations which develop, deliver, and sustain materiel solutions. And finally the Army Mobilization Stations, which can be Active Component (AC) installations, Reserve Centers or National Guard Armories that are responsible for coordinating medical and dental screening, Soldier readiness processing, theater specific clothing and equipment issue, weapon familiarization and qualification, theater-specific individual readiness training, and coordinate movement of personnel into the Area of Operation. An Army installation for the purpose of this appendix, falls into one of these four installation variances with mission environments and control points.

4. Summary

LandWarNet 2020 and Beyond is a critical component for empowering our Soldiers to fight and win our Nation's wars through prompt and sustained land combat. It is because of this the Army is undergoing a modernization transformation and paradigm shift to establish the LandWarNet 2020 & Beyond as a "single, secure, standards-based, versatile network that provides the overarching end-to-end architecture connecting Soldiers and their equipment to vital information and our Unified Action Partners that will create overwhelming synergy and technology overmatch on future battlefields."

To achieve the LandWarNet 2020 and Beyond vision and The Army Network LandWarNet 2020 and Beyond strategy the Army is pursuing a capability set management construct that will cut across functional areas containing both Institutional and Operational Capability Sets and delivering enterprise services to the entire Army. The Network must be treated as a single entity, unified from the Global Information Grid, to the installation, to the farthest tactical edge, and provide the same basic capabilities from home station to the lone dismounted Soldier in theater.

For the Army to realize the full operation capabilities of LandWarNet 2020 and Beyond it must design, develop, acquire and field the Network in a comprehensive, synchronized manner. The first step to achieving this desired end state on Army P/C/S is through this the Army Installation Architecture presented in this document.

TAB A – Acronyms

The acronyms found in this document are presented below:

Acronym	Description
AMC	Army Materiel Command
ASCC	Army Service Component Command
AMC	Army Material Command
AR	Army Regulation
ARFORGEN	Army Forces Generation
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics, and Technology
BaseOps	Base Operations
BI	Base Infrastructure (BI)
C2	Command and Control
C4	Command, Control, Communications, and Computers
C4IM	Command, Control, Communications, Computers and Information Management
CBA	Capabilities Based Assessment
CCI	Communications and Computing Infrastructure
CCTV	Closed Circuit Television
CDD	Capabilities Design Document
CE	Computing Environment
CENTRIXS	Combined Enterprise Regional Information Exchange System
CIO	Chief Information Officer
COE	Common Operating Environment
CONUS	Continental United States
CONOPS	Concept of Operations
CS	Capability Set
CSM	Capability Set Management
DISN	Defense Information Systems Network
DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership Development and Education, Personnel, and Facilities
EA	Enterprise Architecture
EMS	Emergency Medical Services
ESB	Expeditionary Signal Battalions
EoIP	Everything over Internet Protocol
FORSCOM	Forces Command
GIG	Global Information Grid
IADS	Installation as a Docking Station
IC	Intelligence Community
IdAM	Identity and Access Management
IIE	Installation Information Environment
IP	Internet Protocol
IPN	Installation Processing Node
IT	Information Technology
ITMR	Information Technology Management Reform
JIE	Joint Information Environment

Acronym	Description
JIE-EA	Joint Information Environment - Enterprise Architecture
JIIM	Joint, Interagency, Intergovernmental, and Multinational
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
MC	Mission Command
ME	Mission Environment
MEDCOM	Medical Command
NCS	Network Capability Sets
NEC	Network Enterprise Center
NetOps	Network Operations
NIE	Network Integration Evaluation
NIPRNET	Unclassified but Sensitive Internet Protocol Network (formerly the Non-Classified Internet Protocol Network)
NMA	Network Mission Area
OCS	Operational Capability Sets
PAM	Pamphlet
P/C/S	Posts Camps, Stations
PoP	Point of Presence
RA	Reference Architecture
QoS	Quality of Service
SIPRNET	Secure Internet Protocol Router Network
SoS	Systems of Systems
SPPN	Special Purpose Processing Node
SSA	Single Security Architecture
TRADOC	Training and Doctrine Command
TS/SCI	Top Secret /Sensitive Compartmented Information
UC	Unified Capabilities
VCSA	Vice Chief of Staff of the United States Army
WIN-T	Warfighter Information Network-Tactical

TAB B – References

- Department of Defense Memorandum, SUBJECT: Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration, dated 11 July 2013.
- Department of Defense Memorandum, SUBJECT: Department of Defense Mobile Device Strategy, dated 8 June 2012.
- Department of the Army Memorandum, SUBJECT: Army Directive 2013 – 02, SUBJECT: (Network2020 and Beyond: The Way Forward), dated 11 March 2013.
- Department of the Army Memorandum, SUBJECT: Information Technology Management Reform (ITMR) Implementation Plan, dated 20 February 2013.
- Department of the Army Memorandum, SUBJECT: Transition of All Army Network to the LandWarNet, dated 16 November 2012.
- Secretary of the Army Top Priorities, 5 November 2012.
- Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 31 August 2005.
- TRADOC Pamphlet 525-5-600, The United States Army's Concept of Operations, (CONOPS) - LandWarNet 2015, 11 February 2008.
- The Army Network Strategy (DRAFT)
- LandWarNet 2020 and Beyond End State Architecture, 1 August 2013.
- LandWarNet 2020 and Beyond Network Capability Sets White Paper, 1 March 2013.