Office of the Army Chief Information Officer/G-6

ARMY NETWORK CAMPAIGN PLAN 2020 & BEYOND

Implementation Guidance

MID-TERM

2017-2021

February 2015

CIO/G-6

ENABLING SUCCESS FOR TODAY & TOMORROW

UNCLASSIFIED/FOR OFFICIAL USE ONLY

U.S.ARMY

CIOG6.ARMY.MIL

DISCLAIMER

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 Do not cite this document for the purpose of advertisement.

CHANGES

Refer requests for all changes that affect this document to: Architecture, Operations, Networks and Space (SAIS-AON),
CIO/G-6, ATTN: Mr. Edwin Payne, 107 Army Pentagon, Washington, DC 20310-0107.

Executive Summary

To enable a smaller and more agile Army that is globally responsive and regionally aligned, the Army network must be dynamic, flexible, resilient and always capable of supporting user demand. The *Army Network Campaign Plan (ANCP) Implementation Guidance, Mid-Term* guides modernization planning and execution activities across multiple communities of interest and practice, including resource planning, acquisition and policy development, to ensure that investments and information technology solutions optimize global operations. As part of these efforts, the Army will synchronize the hardware, applications and services that support both warfighting and business operations using assessments conducted as part of the Army Enterprise Network (AEN) portfolio management process[1]. As discussed in this document, the Army will maintain and modernize the network in fiscal years (FY) 17-21 through targeted capabilities designed to improve network infrastructure, deliver enterprise-level services and manage and secure the network.

By the end of FY 16, Army network infrastructure will provide the throughput and computing infrastructure necessary to extend enterprise services and unified capabilities (UC) to the point of need across a majority of the institutional Army. This will empower garrison-based and distributed mission command (MC) operations; enable distributed live, virtual, constructive and gaming (L/V/C/G) training; and enhance the readiness of the deployable network components. The Army will have standard policies, protocols, supporting initiatives and tools to synchronize cybersecurity and network operations across all organizations. The Army will use a service-based integrated enterprise access management framework to identify, authenticate, authorize and account for users accessing enterprise resources. This centralized capability will manage user privileges for access to resources across the Army.

Network modernization planning and activities will also spur changes across the Army that will require analysis from a doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy (DOTMLPF-P) perspective. Examining these areas will present opportunities for the Army to look again at how it is task-organized and trains and fights. As network capabilities are developed and fielded at the enterprise level, disparate and standalone systems will be converged or retired, allowing the Army to gain efficiencies while reducing costs. By synchronizing the whole network portfolio and leveraging advances in technology, the Army will be equipped to meet future challenges and enable the Soldier to effectively communicate and exchange information for mission success.

Robert S. Ferrell
Lieutenant General
Chief Information Officer/G-6

[1] The Army Enterprise Network portfolio management process reviews network capabilities on a yearly basis to determine network gaps needed to support Army strategy. The main outputs of the portfolio management process are the ANCP, near- and mid-term implementation guidance documents.

This page intentionally left blank.

Table of Contents

Introduction 7
Army Network Campaign Plan (ANCP) Construct 7
ANCP, Mid-Term Construct 7-8
The Network in FY 16 8
FY 17-21 Overview 9
Impacts to the Army 11
Appendix 1 – Network Capacity Domain 1-1
- Domain Overview 1-1
- Network Capacity at the End of FY 16 1-2
- Overview of FY 17-21 Activities 1-2
- Mandates Driving Network Capability Modernization 1-2
- Capability Gaps and Priorities 1-3
- Capability Progression/Joint Capability Area (JCA) Alignment (FY 17, FY 18-21) 1-4
- Dependencies 1-7
- Summary 1-7

Appendix 2 – Enterprise Services Domain 2-1
- Domain Overview 2-1
- Enterprise Services at the End of FY 16 2-1
- Mandates Driving Network Capability Modernization 2-2
- Capability Gaps and Priorities 2-3
- Capability Progression/JCA Alignment (FY 17, FY 18-21) 2-3
- Dependencies 2-7
- Summary 2-8

Appendix 3 – Network Operations and Security Domain 3-1
- Domain Overview 3-1
- Network Operations and Security at the End of FY 16 3-2
- Overview of FY 17-21 Activities 3-2
- Mandates Driving Network Capability Modernization 3-2
- Capability Gaps 3-3
- Capability Progression/JCA Alignment (FY 17, FY 18–21) 3-5
- Dependencies 3-11
- Summary 3-12

Appendix 4 – Capability Taxonomy by Domains 4-1
Appendix 5 – Acronyms 5-1

This page intentionally left blank.

Introduction

To meet the future global challenges and other factors that impact Army missions, the Army network must remain flexible, adaptable, affordable, scalable and capable of supporting user demand. Using the AEN process, the Army will maintain and modernize the network via synchronization of institutional and operational capabilities in FY 2017-2021. This document begins to reflect the alignment of planning across all Army mission areas (the Enterprise Information Environment and the Warfighting, Business and Defense Intelligence Mission Areas), building upon activities occurring in the FY 15-16 timeframe. *The Army Network Campaign Plan – Implementation Guidance, Mid-Term* informs follow-on modernization planning and execution activities across multiple communities of interest and practice, including resourcing, acquisition and policy development.

Army Network Campaign Plan (ANCP) Construct

The ANCP is comprised of three documents: the *Army Network Campaign Plan*, the *ANCP – Implementation Guidance, Near-Term* and the *ANCP – Implementation Guidance, Mid-Term*. These documents each serve a purpose and are intended to impact planning activities across the Army.

The table below describes the purpose of each document and the associated timeframes.

ANCP Document	Purpose	Timeframe
Army Network Campaign Plan (ANCP)	• Links with relevant Army and Department of Defense (DoD) strategies. • Describes network-related end states at a high level and outlines Lines of Effort (LOEs).	2020 and beyond
ANCP – Implementation Guidance, Near-Term	• Describes execution activities within a two-year time frame. • Reflects acquisition, resource and mission reality. • Guides the design and development of the next Network Capability Set.	2015–2016
ANCP – Implementation Guidance, Mid-Term	• Focuses on network capabilities. • Designed to impact resource planning within Program Objective Memorandum venues.	2017–2021

Table 1: ANCP Construct

ANCP, Mid-Term Construct

The *ANCP – Implementation Guidance, Mid-Term* is a living document, developed on an annual basis to reflect the realities of Army mission obligations, acquisition planning and resourcing. Aligned with the *Army Network Campaign Plan,* it provides the framework for network capability packages, to be reflected in an annual Institutional Network Modernization Execution Order, and detailed information on execution-level activities.

The *ANCP – Implementation Guidance, Mid-Term* is developed by the AEN domains (Network Capacity, Enterprise Services and Network Operations and Security) in coordination with multiple communities of practice, including: functional experts, mission area representatives, information technology (IT) strategic planners, resource planners and managers, and acquisition experts. The AEN domains conduct cross-cutting analysis, utilizing multiple data sources that include Army strategic guidance, senior leader goals and objectives, current Army mission obligations, the status of Enterprise Information Environment Mission Area IT investments, acquisition plans and resourcing plans. Near- to mid-term activities, supported through IT investments, will be aligned, managed and tracked through five LOEs.

Described below in Figure 1, LOEs link tasks, effects and conditions to the strategic vision and end state, and help define how individual actions contribute and combine to achieve the outcomes desired in 2020 and beyond. The LOEs, depicted below and described in the *ANCP*, are the current set of priorities for the near and mid terms. New LOEs will emerge based on the progress achieved in the execution of the near- and mid-term implementation guidance.

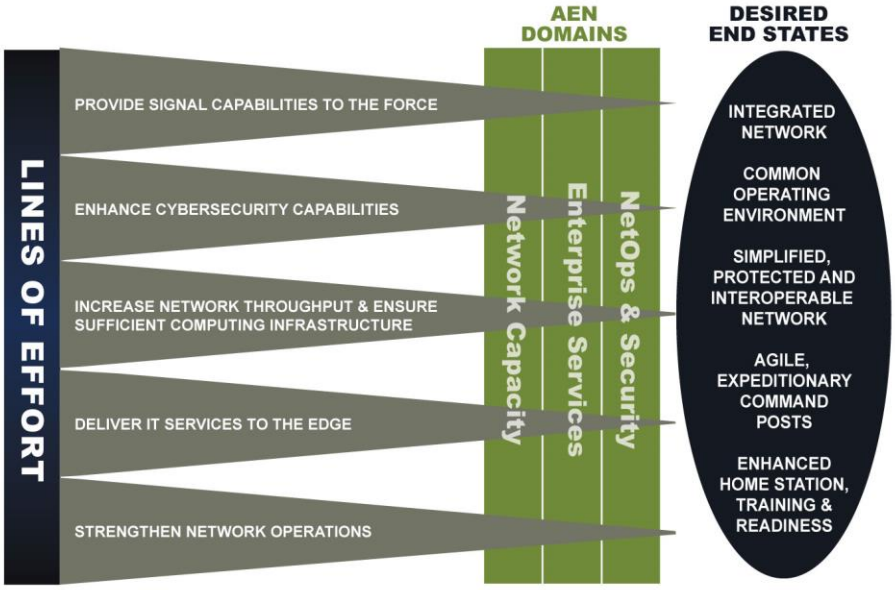

Figure 1: ANCP Operating Construct

The Network in FY 16

By the end of FY 16, assuming that all required resources are provided and acquisition activities are completed, Army network infrastructure will be upgraded to provide the throughput and computing infrastructure necessary to extend enterprise services and unified capabilities to the point of need across a majority of the institutional Army. The robust infrastructure will empower garrison-based and distributed mission command (MC) operations and distributed live, virtual, constructive and gaming (L/V/C/G) training while enhancing the readiness of deployable network components. Modernization and centralization of network security stacks will provide a logical starting point for integration into the future Joint Information Environment (JIE) and Intelligence Community Information Technology Enterprise (IC-ITE) technical and operational constructs. The JIE Single Security Architecture (SSA) will provide centralized network

management and defense, and better command and control. Command Post Computing Environment (CP CE) version 2.0 will go into testing with a fielding decision in early FY 17.

By FY 16, the Army will provide:

- Continental United States (CONUS)-based unified capabilities soft-client bridging capability.
- Enterprise-wide service desk support for global IT assistance to all Army users.
- Global access to user and resource information on the network through an integrated directory service capability.
- Standardized policies, protocols, supporting initiatives and tools to synchronize cyber security, data center and network operations across all organizations.
- Service-based enterprise access management and an integrated access management framework to identify, authenticate, authorize and account for users accessing enterprise resources. This centralized service will manage user privileges to access resources across the Army.
- Increased network security, to include vulnerability and patch management, as well as enhanced encryption to improve the secure information exchange capability.

FY 17-21 Overview

Using a phased approach, the Army will modernize the network through implementation of multiple, targeted capabilities[1] within the FY 17-21 timeframe. Although not all network-related capabilities were assessed and included in this document, the expectation is that those capabilities not addressed are in a legacy/sustainment phase or will be assessed and addressed in future versions of the *ANCP – Implementation Guidance, Mid-Term*. This document only focuses on capabilities that are targeted for modernization/upgrade in the FY 17-21 timeframe. Figure 2 depicts the Enterprise Information Environment Mission Area (EIEMA) domain alignment with the Army IT Portfolio Management construct. For a more in-depth review of the capabilities within each domain, refer to Appendices 1-3.

[1]Targeted capabilities are derived through assessments conducted within the AEN Portfolio Management Process, led by the CIO/G-6 in coordination with the AEN stakeholder community. This process identifies gaps, validated by the AEN stakeholder community, which are developed through review of the current end-to-end network, the level of capability the network must achieve in order to meet Army strategic requirements and the current and planned posture of information technology investments within the Enterprise Information Environment Mission Area (EIEMA). This assessment also incorporates other mission area plans to determine end-to-end network impacts.

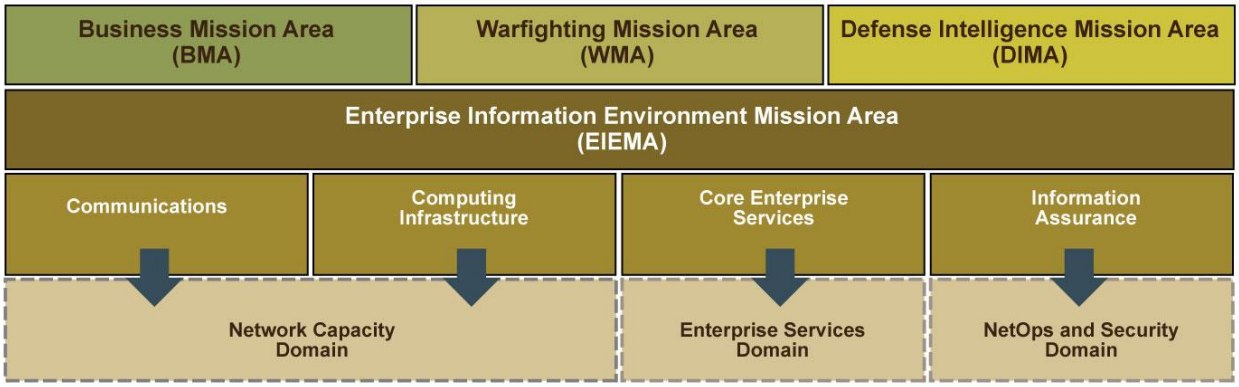

Figure 2: Army IT Portfolio Management Construct

The following table provides an overview of the AEN domains, capability areas and capabilities for development.

Network Capacity	**Information Transport** • Continue installation infrastructure modernization to improve wired information transport throughput and performance. • Continue Joint Regional Security Stack (JRSS) modernization. • Continue modernizing the throughput and performance of on-the-move tactical communications for the deployable force. • Begin the transformation to a wireless infrastructure on Army installations. • Production and fielding of cellular, 4G/Long-Term Evolution (LTE) wireless (WiFi). • Production and fielding of commercial coalition equipment. • Convergence of TS/SCI transport supporting Brigade Combat Teams (BCTs). • Production and fielding of data radios to support Company and below key leaders (four BCTs per year). **Computing Services** • Consolidate the computing and storage infrastructure to support the migration of Army enterprise systems, applications and data into approved enterprise hosting facilities (excluding deployable data centers). • Enable access to authoritative data sources, data and information that reside at the enterprise level from any location and approved device. • Provide fusion and analytics of Army data across Army functional communities to support operational, business and decision-making processes. • Centrally manage a standardized suite of devices. • Enable decentralized access to Army data and enterprise services. • Continue to implement standard enterprise operations and management guidelines to improve operation and sustainment processes based on the streamlined data center and application architectures. • Fielding of CP CE version 2 in FY 17. • Fielding of CP CE version 3 in FY 19. • Fielding of mounted CE with a common software foundation and software development kit for Common Operating Environment (COE) version 3 with interoperable apps and widgets in FY 19. • Establishing and publishing standards that define the common software foundation for the Mobile Hand-held CE in FY 19.

Enterprise Services	**Common Core Enterprise Services** • Consolidate standalone, legacy solutions to enterprise capabilities. • Provide global directory services with contextual search. • Enable content discovery services with contextual awareness. • Provide a single point of access to information. • Provide a service desk capability that is supported by standardized processes across the institutional Army.
Network Operations and Security	**Net Management** • Provide a single capability that performs enterprise asset identification. • Synchronize and integrate continuous monitoring solutions. • Standardize network operations across the network. **Information Assurance** • Provide enterprise service-based access management utilizing user identity attributes and associated privileges. Begin to establish the foundational elements for incorporation of biometrics to support user identity and access management. • Modernize cryptology capabilities for critical command, control and communications systems and establish the foundational elements to leverage and integrate commercial capabilities. • Enable enterprise key management capability "over the network" instead of physical distribution. • Provide security components to allow users to leverage and utilize enterprise services on the Army network with their own devices (i.e., bring your own device [BYOD]).

Impacts to the Army

In FY 17, the Army will be at a critical point in network modernization while facing a landscape of changing missions and budgetary constraints. To build on current network modernization momentum, the Army will continue to gain efficiencies and reduce costs through divestiture of legacy systems and maximization of enterprise capabilities. Conducting rigorous assessments through the AEN process will balance network capability investments. By leveraging advances in technology, the Army will be positioned to drive down operating and sustainment costs.

Capability fielding will modernize the network from the tactical edge to the installation, enabling the Army to transition to a regionally aligned, expeditionary fighting force. Soldiers and units will see enhancements and improvements to capabilities across the network, specifically, more direct and transparent access to enterprise-level services utilizing Installation as a Docking Station (IaaDS), the Integrated Training Environment (ITE) and authoritative data sources. Operating and generating forces will have network access that will bring dynamic computing power to the Soldier's level, enabling decision making with reliable data. As resilient capabilities are developed and provided at the enterprise level, the Army may also experience changes across the DOTMLPF-P spectrum, such as force redesign. By 2021, the network will provide the Army the agility and versatility necessary to meet mission requirements and mitigate an ever-evolving threat landscape.

Appendix 1 – Network Capacity Domain

Domain Overview

The Network Capacity Domain (NCD) portfolio manages the physical infrastructure necessary for all services and information-based activities to pass through the network. It encompasses the foundation upon which the Enterprise Services Domain (ESD) and the Network Operations and Security Domain (NSD) are built. The NCD will leverage existing capabilities and implement the Army's Network 2020 and DoD's Joint Vision 2020 architectures. The goal is to manage the transport and computing infrastructure of a modernized, global and versatile network that gives Regionally Aligned Forces and unified action partners (UAPs) the full range of military and business advantages across all joint operational phases.

As depicted in Figure 3, the domain is comprised of two major capability areas: Information Transport and Computing Services. These capability areas support moving data and extending services in and between the institutional component and deployed units; storing and processing data; and delivering the devices utilized by Soldiers and others to send, receive and process data. The NCD capability area objectives are to provide a resilient transport network, an optimized, responsive computing and storage capability, and a range of user device options that provide continuous advantage across all operational phases.

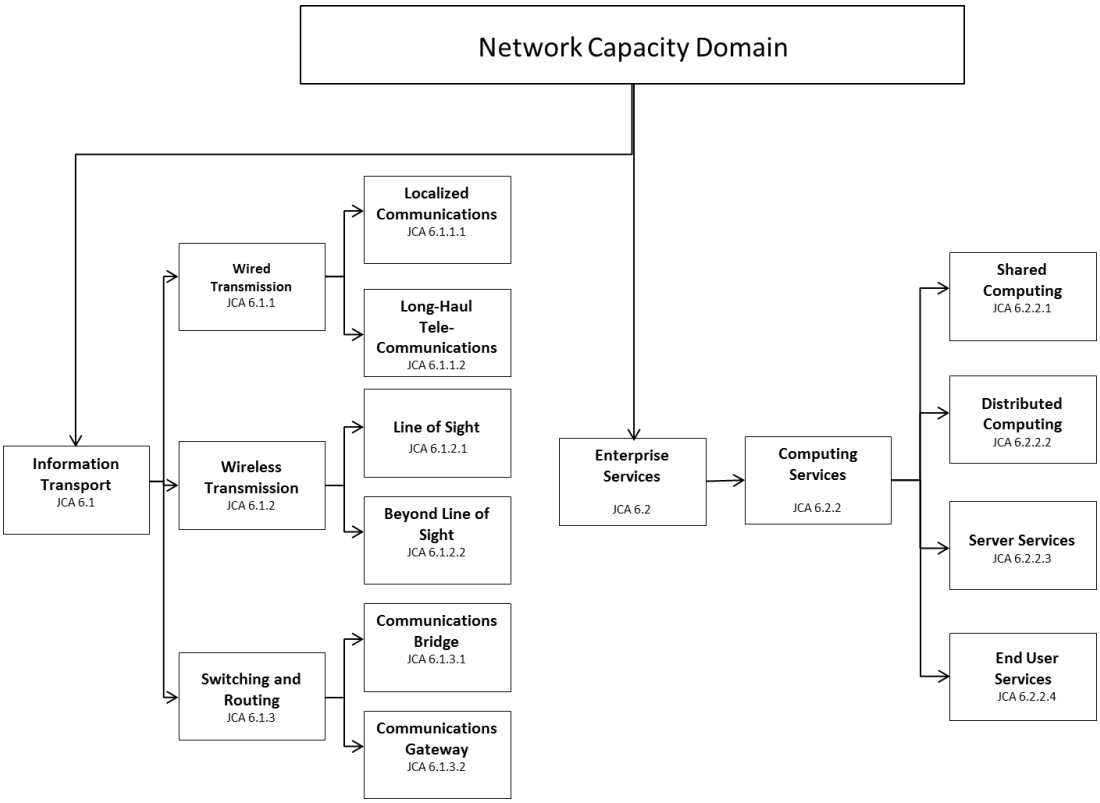

Figure 3: NCD Capability Taxonomy

Network Capacity at the End of FY 16

By the end of FY 16, the Army network infrastructure will be upgraded to provide the throughput and computing power necessary to extend enterprise services and UC to the point of need across a majority of the institutional Army. The infrastructure will support rapid evolution and deployment of applications to meet changing user needs, and the staging of information to ensure connectivity to critical information at the point of need as users transition between mission environments. The Army network backbone, connecting installations to the DoD Information Network (DoDIN), will be increased to 10 gigabits per second (Gbps) with the capacity to increase to 100 Gbps in the future. A significant portion of the Army's computing and data storage will be consolidated in approved DoD enterprise hosting facilities (EHF)[2,3,4,5] located around the world to meet the computing and storage requirements of most installations.

Overview of FY 17-21 Activities

Within the FY 17-21 timeframe, the Army will continue consolidation of applications and data storage to approved enterprise hosting facilities in order to support external mandates and Army senior leader goals and objectives. The computing infrastructure will be modernized to support cloud and distributed Big Data analytics capabilities, providing decision support to all users. Garrison-based and distributed operations from CONUS will become the standard, helping to reduce the footprint of forces deployed in the threat environment. The Army also will initiate implementation of L/V/C/G training concepts, as well as the extension of business systems and capabilities to the enterprise. The Army will employ centralized management of end-user devices (EUDs), to include identifying and implementing a standard suite of devices as part of the COE, which will increase efficiencies (i.e., BYOD) and improve network security.

Mandates Driving Network Capability Modernization

FY 17-21 efforts are driven by Army guidance and external mandates. This implementation guidance is based on the need to provide a robust transport infrastructure; sufficient, modern, resilient and reliable computing and storage capacity; and EUDs and mobile capabilities.

Three major legislative and DoD mandates, listed below, are driving network capacity modernization activities.

---

[2] Core Data Center (CDC): Provides standardized hosting and storage services to the enterprise, serving as consolidation points for computing and storage services currently hosted across hundreds of component facilities.

[3] Installation Processing Node (IPN): A fixed DoD data center serving a single DoD installation and local area (installations physically or logically behind the network boundary) with local services that cannot (technically or economically) be provided from a CDC. There will be no more than one lPN per DoD installation but each lPN may have multiple enclaves to accommodate unique installation needs (e.g., joint bases).

[4] Installation Service Node (ISN): A facility containing the localized equipment necessary to provide the minimum basic functionality to an installation should it becomes disconnected from the DoD Information Network (DoDIN). There is no application hosting or data processing in an ISN. Potential services include read-only Active Directory (AD) servers, DNS servers, Assured Compliance Assessment Solution servers, Host-Based Security System servers and print servers. ISNs may also host UC that must remain on the installation in order to enable emergency services even when the connection to the DoDIN is interrupted.

[5] Special Purpose Processing Node (SPPN): A fixed data center supporting special-purpose functions that cannot (technically or economically) be supported by CDCs or IPNs due to association with infrastructure or equipment (e.g., communications and networking, manufacturing, training, education, meteorology, medical, modeling and simulation, test ranges, etc.). No general purpose processing or storage can be provided by or through an SPPN. SPPNs do not directly connect to the DoDIN; they must connect through a CDC or lPN.

Auditability	Congress requires DoD to have audit-ready financial statements by 2017. Former Secretary of Defense Leon E. Panetta assured Congress that all of the Services would have auditable Statements of Budgetary Resources by 2014 and would achieve audit readiness for all financial statements by 2017 (FY 13 Army Audit Readiness Strategy)[6].
Application, System and Data Migration	The DoD Chief Information Officer (CIO) directed components to migrate all applications and systems supporting users across installation boundaries to DoD CDCs by the end of FY 18 (DoD CIO memorandum, 11 July 2013). This remains an Army objective; however, due to technical complexities and fiscal constraints, efforts will continue through FY 21.
Mobile Devices	DoD guidance provides a phased approach for the development and use of mobile, non-tactical applications on EUDs (DoD Commercial Mobile Device Implementation Plan, 13 February 2013).

The listed mandates require an aggressive modernization approach across NCD capability areas to provide the transport, computing and EUD infrastructure necessary to support the mass migration of Army data into consolidated data hosting facilities and the enterprise management of EUDs. Specific capabilities required to modernize the Army's robust infrastructure will be addressed with key stakeholders through various means (e.g., Execute Order (EXORDs), Concept of Operations (CONOPS)).

Capability Gaps and Priorities

Utilizing the Universal Joint Task List (UJTL) and the LandWarNet Initial Capabilities Document (ICD), NCD conducted an analysis to identify and prioritize network capacity gaps for the FY 17-21 timeframe. Comparing the FY 16 NCD portfolio to mandates and requirements (e.g., network capacity-related UJTL and LandWarNet ICD elements) led to the identification of capability gaps. The number of UJTL and LandWarNet ICD elements aligned to each gap fed the gap prioritization effort. The table below shows the prioritized NCD FY 17-21 capability gaps.

Priority	Gap	Gap Description	Capability
1	Deployed network throughput	Network transport bandwidth cannot support voice transmission (e.g., voice over internet protocol (VoIP)), video transmission (e.g., video teleconference) and data transmission for all deployed mobile forces across both the lower and upper tactical edge (TI). Network transport throughput for lower-echelon tactical units is not sufficient to support mission requirements, to include information operations, and enterprise hosting of data and applications.	Information transport
2	Deployed network reach	The network reach for lower-echelon tactical units is insufficient to conduct distributed operations. Lower TI reach is not long enough to support cross-enclave and cross-unit communications in cases where upper TI is not available.	Information transport

[6] Auditability requires the consolidation of data into approved enterprise hosting facilities, the transport infrastructure to support virtual data access and computing, and end-user devices for end users to analyze the data.

3	Deployed network computing services	Lower-echelon tactical units lack sufficient data storage and processing power to support mission requirements. Deployed forces do not have the necessary computing and processing power to provide automated services to commanders.	Shared computing, distributed computing, server services
4	Cellular/ wireless local communications	Installation wireless infrastructure is not mature enough to support the increasing demand for cellular/mobile computing and services.	Information transport
5	Installation network throughput	Network transport bandwidth cannot support voice transmissions (i.e., VoIP, Voice Over Secure Internet Protocol) to all users.	Information transport
6	UAP connectivity	Deployed network lacks infrastructure plug-in points to facilitate UAP connectivity in theater.	Information transport
7	IP-based VTC	VTC over IP capability is limited and relies on non-standard equipment.	Information transport
8	EUD environment	EUD implementation and use are neither standardized nor efficient.	End-user services

Capability Progression/Joint Capability Area (JCA) Alignment (FY 17, FY 18-21)

The table below shows the NCD capabilities that are targeted for modernization in FY 17 and FY 18-21.

Initiative	**Joint Capability Area** 6 Net-Centric									
	6.1 Information Transport						6.2 Enterprise Services			
	6.1.1 Wired Transmission		6.1.2 Wireless Transmission		6.1.3 Switching and Routing		6.2.2 Computing Services			
	6.1.1.1 Localized Communications	6.1.1.2 Long-Haul Telecommunications	6.1.2.1 Line of Sight	6.1.2.2 Beyond Line of Sight	6.1.3.1 Communication Bridge	6.1.3.2 Communication Gateway	6.2.2.1 Shared Computing	6.2.2.2 Distributed Computing	6.2.2.3 Server Services	6.2.2.4 End-User Services
FY 17 Targeted Capability	●	●	●	●	●	●	●	●	●	●
FY 18-21 Targeted Capability			●	●	●	●	●	●	●	●

Information Transport

Wired Transmission

Localized Communications & Long-Haul Telecommunications

- In FY 17, the NCD will continue installation infrastructure modernization to improve wired information transport throughput and performance. Network efficiency and effectiveness will be achieved by consolidating, standardizing and expanding the network to facilitate faster data transfer.
- Across FY 18-21, as the end of the current wired infrastructure's life cycle approaches, information transport on targeted installations will begin to transform from wired to wireless. Wired transmissions will be phased out while still providing the installation a network that is always on and always available, with limited single points of failure and more network diversity.

- By the end of FY 21, the Army will be positioned to support future enterprise business systems, the universal adoption of enterprise services, cloud computing and Big Data analytics. NCD efforts will increase installation network throughput, standardization, efficiency, reliability and availability to support the growing network demand associated with distributed operations, L/V/C/G training and heavier utilization of enterprise services. These modernization activities will also empower installation networks with the resiliency and flexibility to scale up or down, as needed.

Wireless Transmission

Line of Sight & Beyond Line of Sight

- In FY 17, the NCD will continue modernizing the throughput and performance of the wireless information transport for deployable units. The goal will be more reliable and versatile on-the-move tactical communications, as well as improved connectivity between the lower and upper TI, which will increase the ability of commanders at all levels to collaborate with their forces.
- In FY 18-21, the NCD will continue modernizing the throughput and performance of the wireless information transport. The improved connectivity between the lower and upper TI will enhance collaboration across the operating force, while wireless transmission improvements will enable lower-echelon tactical formations to support all forms of communication (voice, video, data). The NCD will begin implementation of a standard wireless infrastructure at prioritized installations (in lieu of upgrading wired infrastructure at the end of its life cycle) to meet the increased demand for wireless information transport capabilities tied to mobility services and mobile devices
- By the end of FY 21, the NCD will provide more reliable and versatile on-the-move tactical communications for the force by increasing deployed network throughput and reach, and improving unified action partners' connectivity. Implementation of wireless installation infrastructure at prioritized locations will provide information transport support for end-user mobility services.

Switching and Routing

Communication Bridge & Communication Gateway

- In FY 17, the Army will continue to deploy Multi-Protocol Label Switching (MPLS) capabilities to build network capacity globally in alignment with G-3/5/7 priorities.
- In FY 18-21, the Army will optimize the benefits of information transport improvements in wired and wireless capabilities by synchronizing switching and routing enhancements. These network infrastructure upgrades will ensure that the Army is positioned to support future enterprise business systems, the universal adoption of enterprise services, cloud computing and Big Data analytics.
- By the end of FY 21, switching and routing enhancements will include full implementation of MPLS globally in synchronization with DoDIN modernization guidance. Satellite communication (SATCOM) gateways and teleports will be modernized to extend long-haul transport to the tactical edge, connecting tactical networks that operate beyond the Defense Information Systems Network (DISN) point of presence to the DISN backbone.

Computing Services

Shared Computing, Distributed Computing & Server Services

- In FY 17, the Army will continue executing the Federal Data Center Consolidation Initiative and DoD mandates to close, consolidate and standardize data centers. This will enable centralized hosting of systems, applications and data storage, aligned with improved holistic enterprise operations and management processes. The plan is to establish on-demand computing and data for the generating force if sequestration resources are restored.
- During FY 18-21, necessary data center closure, consolidation and standardization tasks will be repeated as the number of closures increases across posts, camps, stations, and applicable joint bases. Holistic enterprise operations and management processes will be refined based on the streamlined data center architecture. Optimum project management and engineering techniques will be achieved based on prior-year lessons learned and process refinements.
- By the end of FY 21, the NCD will enable the rapid and more efficient evolution of applications, minimizing cost and speeding dissemination of application enhancements through automated processes. The consolidated computing environment will support the processing of large amounts of data regardless of location, aiding knowledge discovery and improving both deployed network computing services and IP-based video teleconference (VTC). The Army will complete the consolidation and standardization of data centers, centralized hosting of systems, networks and applications. The Army data center and applications landscape will be drastically reduced and cloud-enabled. The examination of data center operations and associated doctrine, organization, training, materiel, leadership, policies, plans and facilities will further enable unified operations. Based on the COE and JIE guidelines, data centers will have a standardized scalable computing, storage, software, security and communications environment. The Army will establish the data center COE library to enable the Software Marketplace for applications supporting the enterprise and tactical users in the Data Center/Cloud/Generating Force, Command Post, Mounted and Handheld Computing Environments. Collectively, this will maximize automation potential.

End-User Services

- In FY 17, the NCD will enable end users to utilize a standardized single suite of devices that deliver multiple capabilities (voice, video and computing). End users will be able to acquire and utilize end-user services through mobile devices in an efficient, consistent and reliable manner.
- Across FY 18-21, the NCD will implement a hybrid or BYOD strategy for end users to utilize a single suite of computing devices (e.g., soft phone capability with removable microphone, video teleconference-like capability with enhanced image capture and devices with a voice interactive capability) that deliver multiple services (voice, video and computing) as part of the DoD UC Framework.
- By the end of FY 21, the NCD will enable collaboration across the Army, seamless access to the right information, identification of authoritative data sources and sharing across functional communities and centers of excellence, thus mitigating gaps in the EUD environment. It also will automate business processes to improve management of workflows, task tracking, personnel and organizations.

Dependencies

The NCD will provide the foundational elements that enable other domains to execute network operation oversight, network security and enterprise services for the entire Army. Below is a description of high-level dependencies among the NCD, AEN domains and key external stakeholders.

- Network Operations & Security: The integration of information transport mechanisms and consolidation and standardization of computing services enable the NSD to improve network management through the implementation of standardized, end-to-end network operations tools and enhanced asset visibility. Network infrastructure standardization facilitates improved cybersecurity by reducing the network attack surface and enabling the utilization of standardized, enterprise-level cybersecurity tools. Network management is required for successful data migration. The NSD needs to ensure that the selected standardized family of EUDs is able to support data protection on all devices, to encrypt data on devices and to conduct vulnerability and patch management on network and mobile devices.
- Enterprise Services: The consolidation and standardization of computing services, along with the modernized information transport infrastructure, enhance enterprise services content delivery by enabling enterprise applications to be hosted in a centrally managed location and accessed from anywhere. This expedites the routing of information, allowing faster data transfer and collaboration. The NCD relies on the Enterprise Services Domain (ESD) to provide guidance on structure and configuration of data storage and associated pathways that enable data migration. The ESD must also ensure that the selected standardized family of EUDs is able to support enterprise applications and services; these capabilities must be synchronized to ensure that the desired level of computing services can be achieved.
- The NCD has strong dependencies with external stakeholders, such as the Defense Information Systems Agency (DISA) and commercial service providers. The NCD is relying on DISA to provide the facilities, personnel, maintenance and management of the consolidated data centers that support the shared computing, distributed computing and server services capabilities. Enterprise-level service level agreements (SLAs) need to be orchestrated with commercial EUD providers, as the Army will leverage commercial off-the-shelf (COTS) devices to set a standardized suite of EUDs for users to select.

Summary

The NCD portfolio provides a resilient transport network, an optimized, responsive computing and storage capability, and a range of user device options. Combined, these elements create continuous advantage across all operational phases. Network capacity modernization will ensure that the Army is positioned to support future enterprise business systems, the universal adoption of enterprise services, decentralized computing and Big Data analytics. Capability progression in FY 17-21 will support moving data and extending services to and from the institutional component to deployed units; storing and processing data; and delivering the devices utilized by Soldiers and others to send, receive and process data.

Appendix 2 – Enterprise Services Domain

Domain Overview

The Army ESD is a collection of IT investments that will deliver an integrated suite of globally available, adaptable solutions that supports the Army (Active, Guard, Reserve, civilian, contractor) and connects them with UAPs. These services, both user-facing and enabling, provide the Army awareness of and access to information.

The ESD's primary goal is to continuously deliver value to the Army and UAPs by ensuring an integrated collaborative environment that supports all mission areas. The ESD is comprised of two major capability areas: common core enterprise services and position, navigation and timing, as described in Figure 4. The ESD will play a supporting role in achieving outcomes under the purview of other AEN domains (Network Capacity and Network Operations and Security) and the COE. These efforts will modernize the network, support the ITE, provide support for mobility and enable realization of the IaaDS CONOPS.

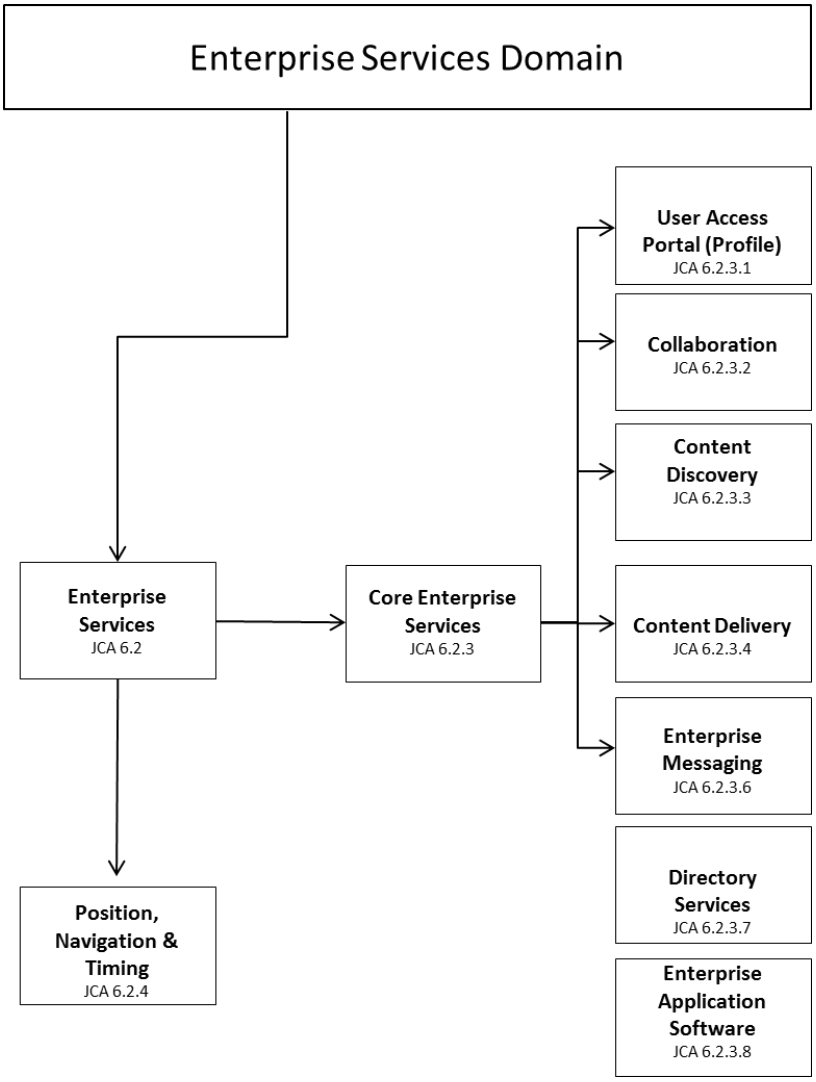

Figure 4: ESD Capability Taxonomy

Enterprise Services at the End of FY 16

By the end of FY 16, the ESD will be in a strong position to continue making advancements that will save the Army money and enhance the user experience. Some of the goals accomplished in FY 16 will lay a strong foundation for the ESD to build upon in the upcoming years to the benefit of the user community.

Enterprise Services will have retired the majority of Army Knowledge Online (AKO) 1.0 and begun deployment of modernized capabilities by the end of FY 16. The ESD will begin to introduce a single sign-on (SSO) feature for users to help minimize the inconvenience of

multiple password checks, and to enable them to get the information they want more quickly. The ESD will initiate plans for on-boarding to the Army Enterprise Service Desk (AESD), which will provide global assistance for Tier 0 (self-help) and Tier 1 IT support. The AESD will have the ability to use the enterprise ticketing system, which will be implemented Army-wide. The ESD will also create a single source for directory information across the network and will continue to look for attributes for future incorporation into directory services. This will allow the Army to provide users global access and resource information on the Army network.

By the end of FY 16, at least 13 agreements (Army enterprise and Joint) linked to Army Enterprise Network Council (AENC)-validated requirements will be in place. ELAs produce cost avoidance, operational efficiencies, asset visibility, improved maintenance coverage, security threat management and enterprise-level support. ELAs are driven by validated DoD and Army requirements that support both the warfighter and business user. As ELAs are created, the Army will focus on discontinuing local purchases of software covered under the established license agreements, resulting in additional cost avoidance/savings.

Mandates Driving Network Capability Modernization

FY 17-21 efforts are driven by both Army guidance and external mandates. *The ANCP – Implementation Guidance, Mid-Term* has defined two expected outcomes for the ESD:

1. Enterprise applications and services are used by the Army, enabling global collaboration with UAPs on any trusted device.
2. Enterprise applications and services provide a consistent user experience to any authorized user through simplified and standardized global delivery.

The Army will use the following guiding principles to invest, develop and deliver enterprise services:

Support the Army	The DOTMLPF-P solutions that are developed should account for all Army components.
Go Joint First	The Army will use Joint solutions before pursuing Army-only solutions. The default approach for investments will be to share services across Joint forces whenever reasonably possible.
Simplify, Standardize and Integrate	Following DoD's lead, the Army must shift from mission-specific sets of systems, processes, governance and controls to a more seamless, coordinated, unified and integrated data-centric enterprise environment.
Build for Change	The dynamic environment in which the Army operates requires solutions that evolve, based on changing requirements. Solutions will be developed incrementally in order to ensure that services evolve with the changing environment.

Capability Gaps and Priorities

These efforts are focused on increasing network effectiveness, security and efficiency[7]. As new enterprise services are brought online, funding for standalone, redundant solutions will be re-directed to fill gaps. The ESD has identified several gaps based on a subjective assessment of the portfolio and senior leader priorities. The gaps that enterprise services target to ensure a better experience for all users are listed in priority order below.

Priority	Gap	Gap Description	Capability
1	Integrated enterprise services (UC, collaboration services, messaging)	Solutions are currently stovepiped and not properly integrated.	Collaboration, enterprise messaging
2	Assured voice	Assured voice currently relies on Time-Division Multiplexing technology, which the Army began to retire in FY 14.	Collaboration
3	Mobile apps	Enterprise services are not currently available on mobile devices.	Enterprise application software
4	Enterprise search	A content discovery service to search across enterprise services does not exist.	Content discovery
5	Duplication of data	Authoritative data sources are not clearly established.	Content delivery, directory services

Capability Progression/JCA Alignment (FY 17, FY 18-21)

The table below shows the ESD capabilities that are targeted for modernization in FY 17 and FY 18-21.

Initiative	Joint Capability Area 6 Net-Centric							
	6.2 Enterprise Services							
	6.2.3 Core Enterprise Services							6.2.4 Position, Navigation and Timing
	6.2.3.1 User Access (Portal)	6.2.3.2 Collaboration	6.2.3.3 Content Discovery	6.2.3.4 Content Delivery	6.2.3.6 Enterprise Messaging	6.2.3.7 Directory Services	6.2.3.8 Enterprise Application Software	
FY 17 Targeted Capability	●	●	●	●	●	●	●	
FY 18–21 Targeted Capability	●	●	●	●	●	●	●	

Core Enterprise Services

In FY 17–21, the primary goal of enterprise services is to ensure that information is available at the point of need. By providing a continuous, adaptive, device-agnostic user experience, enterprise services will enable users to work in changing environments. While mobile devices

[7]See Department of Defense Information Technology Enterprise Strategy and Roadmap (2011)

and their operating systems may have specific design limitations, services should generally offer a consistent user experience that can be customized based on user preferences. In the near term, the enterprise services team will work to better understand and develop a comprehensive picture of the future user experience while moving to the COE. In the mid term, the focus will shift to simplifying and standardizing the user experience across common core enterprise services, moving training resources onto the network and ensuring availability to the Army and UAPs as required.

It is imperative that users have the correct access across all IT services. Updated user in-/out-processing procedures will provide the opportunity to manage and update the access needed to accomplish the mission from the moment a change is implemented (e.g., role, location, organization). Creating and adopting this process will require close collaboration with the NSD and a comprehensive understanding of which attributes affect user access to each service. A clearer picture of which user access changes can occur will emerge as those attributes are defined, allowing the process to be engineered and applied across all core enterprise services. Strategic communications and training will be provided to users to ensure that these processes are well understood and user-friendly.

User Access (Portal)

- In FY 17, the ESD will emphasize gathering and analyzing enterprise and user requirements, as well as lessons learned from previously completed efforts. In order to provide user access (portal) services, the Army will need to build a foundation that includes identified data sources, consistent data standards and operational policies. The Army will determine whether memoranda of agreement are necessary to access information, and will determine the impact of additional or changed security requirements and architectures.
- In FY 18-21, a validated requirements definition, CONOPS and Joint strategic plan will inform device availability. Efforts to field that capability, which will provide relevant information to the user (right information, right personnel, right time, securely), should be under way. This service will be DoD-aligned with support from DISA for data consolidation and storage, and will still enable work offline. The point of entry to Joint information is provided through an Attribute-Based Access Control (ABAC) point of entry with an individual data set that is uniform across the participant population. Additionally, ABAC should govern the management and sharing of Joint information sets for collaboration. The determination of SSO dependencies and requirements should be near completion and policy-based, certificate and password/pin regulations will be validated.
- By the end of FY 21, users will have a single point of access to retrieve the enterprise information needed to complete their missions. Users will no longer be required to seek information from multiple locations. Users will be linked to U.S. Army information and relevant information from UAPs.

Collaboration

- In FY 17, the collaboration capability will be improved by continuing efforts to converge or retire standalone solutions as enterprise services become available. Implementation of a Joint enterprise service for assured voice will be under way and planning for a single, standard and integrated solution for asynchronous and synchronous collaboration will continue. As the initial effort, in FY 17 the Army will begin the transition to Unified

Capabilities as a Service. Joint planning for cross-domain collaboration is required to ensure that the Joint community avoids duplicating solutions and can collaborate effectively with UAPs.

- In FY 18-21, the ESD will focus on implementing a Joint, integrated, enterprise collaboration and enterprise messaging service. Additionally, a solution for assured communications will be implemented. A model for extending collaboration solutions to UAPs will be approved.
- By the end of FY 21, users will no longer have to know a phone number to communicate with other Army users; they will be able to reach intended parties based on either identity (e.g., SGT Smith) or role (S3, 1/4ID). Collaboration services will integrate with newly available information and filtering within directory services to provide the ability to find other users by name, role, organization, location, skills or expertise.

Content Discovery

- In FY 17, data consumers in the tactical community will be able to execute limited discovery queries, guided by industry and data interoperability standards that align to DoD and intelligence community (IC) initiatives/directives. Traditional keyword, geospatial coverage and temporal coverage queries will be available. Content discovery queries will be executed against metadata cached from tactical sources in the CP CE and will be brokered to federated, non-disconnected, intermittent, low bandwidth content providers. Data producers will provide minimum discovery and security metadata with their content to inform content discovery and retrieval. Content cataloging capabilities will derive discovery and security metadata from selected content formats. To improve understandability of retrieved content, program managers will register and manage information exchange specifications for structured and semi-structured content (e.g., XML) in the DoD Data Services Environment. All available metadata will be provided to the content consumer on request.
- In FY 18-21, the Army Data Management Program (ADMP) will continue to align with and implement Joint and DoD initiatives and direction, such as JIE, IC-ITE and the DoD Data Framework. Emphasis on compliance to standards, in order to achieve interoperability, effectiveness and efficiency, will continue. ADMP will also continue to mature to cover more areas of the Data Management Association's Data Management Body of Knowledge and to evolve with technology advances and innovations. Data consumers across the Army enterprise will be able to execute expanded discovery queries, guided by industry and data interoperability standards that align to DoD and IC initiatives/directives. In addition to traditional keyword, geospatial, and temporal coverage queries, data consumers will be able to include subject coverage, based on community of interest taxonomies registered in the DoD Data Services Environment. Content discovery brokers will mediate queries to content providers within a limited version range. Data stewards will register and manage data dictionaries and taxonomies for their subject areas to be used for content discovery. These dictionaries and taxonomies also will be leveraged by data scientists developing Big Data analytics. Content cataloging will expand the content formats and metadata fields to be derived and included for discovery. Content providers will be queried periodically to assess metadata quality and content availability, and they will publish access control requirements, citing specific policies for restricted content.

- By the end of FY 21, content discovery will be provided to users through core enterprise services. Data analytics executed against common (or mediated) metadata will transform content discovery to information discovery. Content discovery will utilize attributes of each individual user to return targeted results that are more likely to address his or her needs. Additionally, records of previous searches will be used to provide criteria for suggested content and similar search terms based on queries from across the Army.

Content Delivery

- In FY 17, data consumers in the tactical community will be able to access content in a very responsive manner based on a publish-and-subscribe model that exploits DISA's Global Content Delivery Service (GCDS) for larger files and for DIL conditions. GCDS' forward staging will also make content delivery via web sites, web-based applications and video streaming more responsive.
- In FY 18-21, improved content delivery will expand to geospatial foundational content so that the data consumer is not dependent on network bandwidth for the foundation content. Data consumers will be able to synchronize their geospatial foundational content while connected to the CP CE, yet be able to use the applications on their devices untethered to the network. The Army will consistently implement the policy and guidance for methods of securing personal health information and sensitive transactional and other data with special requirements. Content will be delivered via a dynamic network to approved EHFs. This network will use a standards- and service-based approach to prioritize data delivery and meet customer needs, such as timeliness, sensitivity and volume.
- By the end of FY 21, the goal is for content delivery to be provided to users through core enterprise services. Army content delivery will use DoD/content discovery and retrieval specifications to discover, search and retrieve content, and will be aligned with DoD and IC initiatives and directives.

Enterprise Messaging

- In FY 17, planning for an integrated enterprise service that delivers both collaboration and enterprise messaging will continue. Simultaneously, services will continue to be brought online to provide a centralized service desk.
- In FY 18-21, users will be offered a self-service portal with access to an enterprise-level service desk. In order to support customers, all core enterprise services will be on-boarded to a common service desk. In order to manage incoming requests with a consolidated solution, Defense Enterprise Email (DEE) 2.0 will provide integrated email, collaboration, UC and messaging as a suite of services.
- By the end of FY 21, enterprise messaging will be part of an integrated and collaborative solution, eliminating some of the Army's disparate initiatives. Additionally, the Army will improve customer support, to include bringing additional services to the enterprise service desk.

Directory Services

- In FY 17, the Army will continue to identify and integrate attributes for directory services filtering and will continue to synchronize directories to achieve a standard Army Directory.
- In FY 18-21, the Army will have an authoritative directory service that will provide enhanced attribute filtering. Implementation of the Army enterprise directory service will

reduce the need for local directory service solutions at installations, constituting an overall reduction in directory maintenance costs across the Army. In order for directory services to realize its full potential and operational efficiency by 2021, a policy must be implemented and enforced that ensures Army personnel (i.e., military, civilians and contractors) are providing accurate and reliable data to authoritative data sources (Army Human Resources and the Defense Manpower Data Center) on a regular basis.

- By the end of FY 21, a single global directory will enable external applications and enterprise services to filter based on attributes such as name, role, location and organization. These filters will ensure that users are connected with the right person, even when the name is unknown, by allowing them to search by skill set or role. These attributes will also act as a mechanism for grouping directory records, ensuring that expertise from around the world can be accessed.

Enterprise Application Software

- By FY 17, the enterprise application software portfolio will be enhanced with additional ELAs that support the Army Enterprise Architecture. ELA requirements will be identified by Army Commands and the evolving JIE and IC-ITE requirements. ELAs will be managed at the enterprise level.
- In FY 18-21, the enterprise application software capability will be improved by implementing an application storefront and continuing to implement additional ELAs and Joint ELAs.
- By the end of FY 21, the Army will have an enterprise portfolio of ELAs that provides a standard set of capabilities across the Army that are compatible with the JIE and IC-ITE. Individual commands will no longer purchase enterprise software independently but instead will utilize an application storefront to request the applications they need. Individuals will have the ability to choose from a portfolio of approved applications for a variety of platforms. The storefront will manage the delivery of the applications to the user by ensuring that the most economical fulfillment method is utilized. License sharing and leasing of specific titles (by metered usage) will be the norm, whether by managing a pool of Army-owned licenses or via subscription models.

Position, Navigation and Timing

Position, Navigation and Timing (PNT) belongs to the ESD, but it is not currently a focus area for the domain. Assured PNT starts development in FY 16, with an operational test scheduled in FY 20 and fielding in FY 21.

Dependencies

As delivering enterprise services is a main driver for many Army initiatives, the ESD will play a supporting role in achieving outcomes led by the other two domains, NCD and NSD. Because the ESD has a hand in targeted Army goals, it is important to show which dependencies occur between the domains to ensure that overall Army goals are achieved on time (e.g., are not delayed due to secondary and tertiary effects of stopping certain initiatives/activities without seeing the bigger picture). Below is a description of high-level dependencies between the ESD and the other domains.

- Network Capacity Domain: Without the ability to transmit information, or handle a requested task, enterprise services would not be able to meet the intended outcomes

described above. Software agreements will save the Army money but, if the EUD cannot support the software, it is a wasted purchase. Collaboration depends heavily on the NCD, from EUDs to the ability to communicate with other locations. The amount of data that can be passed between these locations is important. Additionally, if the network or supporting functions are not well enough established to handle requirements, collaboration cannot occur.

- Network Operations & Security Domain: Enterprise services depend on the NSD in multiple ways. If the Army network is not secure, there is no guarantee that any of the enterprise services will perform as expected. Every core enterprise service depends heavily on assured access and assured transfer capabilities to provide communication across the Army Enterprise Network and enable authorized personnel to access data anytime and anywhere. The NSD is essential for the ESD to be able to create the services and perform the activities the Army needs.
- Content delivery, as defined by the JCA, is highly reliant on other capability gaps identified within this domain, including deployed network throughput, deployed network reach and deployed network computing services. Filling these capability gaps will accelerate the delivery of enterprise content and services. The provision of more core data centers and Installation Processing Nodes (IPNs) and the use of a tactical cloud will also improve the reliability of content delivery.

Summary

Enterprise services provide adaptable solutions that support global, seamless collaboration for the Army and UAPs. The Army will address seven areas of focus during FY 17-21 while developing and maintaining a consistent user experience to bridge the gap between the FY 15-16 near-term activities and the desired 2021 capabilities. These efforts include targeted improvements that provide a clear and comprehensive roadmap to achieving the desired ESD end-state capabilities.

Appendix 3 – Network Operations and Security Domain

Domain Overview

In order to accomplish mission requirements in an ever-increasing and changing threat environment, the Army must be able to operate and defend mission-critical systems and ensure the continuity of network functions. For the FY 17-21 timeframe, the NSD will manage capabilities focused on mitigating cybersecurity deficiencies and addressing operational gaps to provide a secure, seamless and continuous network environment with protected critical data and information for the Army and UAPs. The domain is composed of two JCA Tier 2 capabilities, seven JCA Tier 3 capabilities and 13 Tier 4 capabilities, as depicted in Figure 5. In an effort to align with the JIE and the other Services, the NSD has updated the capabilities to follow the JCA construct.

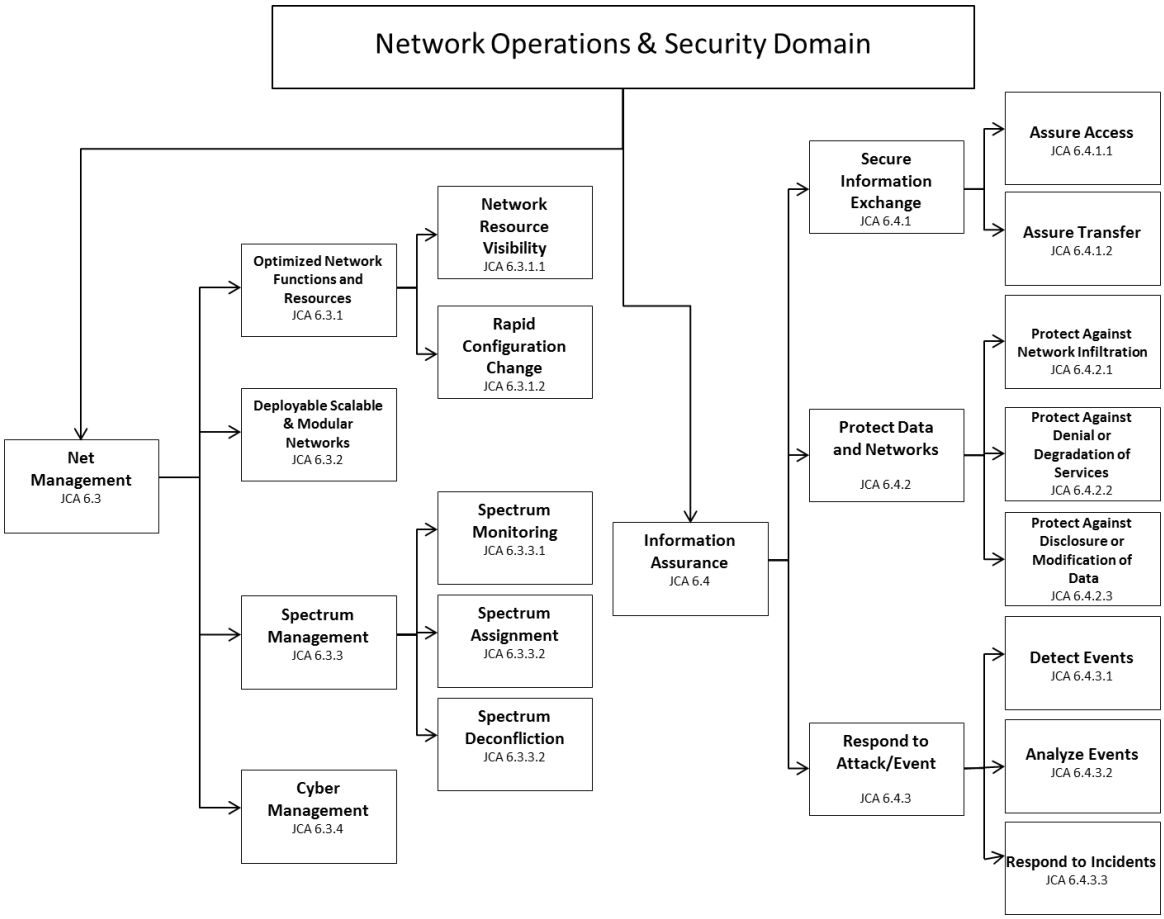

Figure 5: NSD Capability Taxonomy

Network Operations and Security at the End of FY 16

By the end of FY 16, the NSD will enhance network operations, management and defense capabilities, as well as update policies to ensure that all organizations understand, implement and execute cybersecurity best business practices. The Army will achieve full implementation of JRSS architecture in the Continental United States, Southwest Asia and Europe, replacing individual top-layer architecture security stacks and resulting in improved security. The Identity and Access Management (IdAM) framework will be implemented, enabling the Army to provide user access at the point of need and decreasing the time Soldiers are disconnected from the network while transitioning between installations. The Army will implement fully operational Key Management Infrastructure capabilities, including the ability to access key management services and products via the Non-Secure Internet Protocol Router Network (NIPRNet). Enhanced encryption capabilities will support over-the-network keying (OTNK) and provide secure data transmissions. Government-furnished mobile communication devices will be used to access classified knowledge centers and websites, and securely share information. The Army will enable synchronization of information security and user and device activity, as well as data auditing across all networks to detect insider threat activities. Simplified and standardized tools for both operational and institutional environments will assure seamless network operations functions from the enterprise to the tactical edge.

Overview of FY 17-21 Activities

To meet global demands and strategic objectives, data and information critical to both the Army and UAPs must be protected. The network must be dynamic, assured and managed to offer robust capabilities that will improve the Army's ability to protect, detect, respond, restore and manage information and systems. The Army will continue to improve its ability to detect threats and incursions, respond immediately and restore any lost capability via dynamic, 24/7/365 management of its information and systems. The Army will pursue enhanced situational awareness and command and control capabilities that support the management of the underlying physical assets that provide end-user services. The Army also will establish and manage stringent cybersecurity policies and standards, and prepare the workforce for the cybersecurity environment.

Mandates Driving Network Capability Modernization

Mandates for the NSD are derived from several sources, including federal, DoD, Joint and Army documents. The following table depicts the mandates specific to the activities identified in the FY 2017-2021 timeframe.

Identity and Access Management	DoD Instruction 8520.2. Public Key Infrastructure (PKI), Public Key Encryption Enabling, 1 Apr 04 Target PKI Operational Requirement, 20 Aug 01 JTF-GNO CTO 070015 (PKI) Phase 2, 11 Dec 07 DoD CIO memorandum, subject: Mandating the Use of Enterprise Directory Services (EDS), 23 Jan 13
Cryptographic Modernization	Chairman of the Joint Chiefs of Staff (CJCS) Notice 6510.02D Chairman of the Joint Chiefs of Staff (CJCS) Instruction 6510 Capability Development Document (CDD), Cryptographic Equipment & Services, JROC Jul 10

	Communications Security (COMSEC) requirements identified in USC Title 40
Key Management	NSA, Electronic Key Management System (EKMS) Notice #242, subject: EKMS Tier 2 End of Life, Feb 12 CDD ver. 1.02, 15 Aug 06 Headquarters, Department of the Army (HQDA) EXORD, G-3/5/7 LandWarNet/Mission Command Capability Set FY13 Fielding Execution, 27 Jun 12
Mobility	DoD/national guidance, Mobility Capability Package, 30 Jul 12 Chairman of the Joint Chiefs of Staff (CJCS) Notice 6510.2D
Information Security Continuous Monitoring (ISCM)	DoD CIO, Operations Order 12-1016, 31 Aug 12 NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations NIST SP 800-39, Managing Information Security Risk
IT Asset Management (ITAM)	Clinger-Cohen Act of 1996 (CCA-96) AR 25-1, Army Information Technology, 25 Jun 13 AR 25-2 Information Assurance, 24 Oct 07 FY 2013 National Defense Authorization Act, Section 937, Software Licenses of the DoD
Enterprise Service Management System	DoD CIO memo, subject: Information Technology Service Management in the Department of Defense, 15 May 11
Standardization of Network Operations across the Network	FM 6.02-71 Network Operations, 14 Jul 09 Joint CONOPS for GIG Network Operations, 4 Aug 06 Army CIO/G-6 memo, subject: Army Information Condition 3 Status, 12 Nov 09

Capability Gaps

The NSD has identified 13 associated binned to five of the seven JCA Tier 3 capabilities. The prioritized gaps are:

Priority	Gap	Gap Description	Capability
1	Identity and access management technologies	No united Army PKI certificate validation architecture and implementation to ensure that services are available at all echelons.	Secure information exchange
2	Enterprise-level security stack architecture	Inability to “see” into the network due to multiple layers of redundant and non-standardized security controls. Computer network defense tools and resources are inconsistently deployed and inefficiently used.	Protect data and network

Priority	Gap	Gap Description	Capability
3	Unified network management system	Network management and/or enterprise service management capabilities are not fully interoperable nor integrated vertically and horizontally across the force. The Army lacks the ability to provide a single network management capability to manage the entire spectrum of network operations activities within the context of the operating, assuring and defending the network.	Optimized network functions and resources
4	Cryptographic modernization	Enable crypto capabilities to be key management infrastructure (KMI)-aware and support the requirement to increase bandwidth for secure communications across the Army Enterprise Network to the tactical edge.	Secure information exchange
5	Modernization of enterprise key management services	Transition to an enterprise Key Management capability to provide an automated service to account for and distribute cryptographic products to enable OTNK across the NIPRNet and Secure Internet Protocol Router Network (SIPRNet).	Secure information exchange
6	Secure mobility	Phase out legacy 2G to 4G wireless technology and leverage commercial capabilities to enhance secure mobile handhelds to support enterprise tactical applications.	Secure information exchange
7	IT service management (ITSM)	With disparate ITSM/trouble ticketing tools and processes, the Army lacks the capability to deliver an easy-to-use, reliable and secure ITSM capability as a managed service.	Optimized network functions and resources
8	Asset visibility	Army IT resource management suffers due to discontinuities in the network and incomplete visibility of all network assets. The Army lacks enterprise visibility of IT assets, the ability to use data automatically and persistently collected by network operations capabilities, and the ability to track data exposure to Army and external authorized organizations.	Optimized network functions and resources
9	Spectrum management	Electromagnetic (EM) spectrum continues to become more and more congested. Deployed tactical forces will not have full control over the EM spectrum in a particular operating environment, which could be poorly regulated by the host country. The Army itself is fielding more systems that depend on EM spectrum to function. The ability to manage the spectrum effectively and to minimize interference is critical to maintaining operational effectiveness.	Spectrum management
10	Standardize and simplify network operations	Gaps and inconsistencies in existing Army systems and services prevent use of industry best practice standards, management processes, data sharing and common situational awareness views.	Optimized network functions and resources
11	Automated sensing, reporting & response	Current network sensors and reporting technologies are manual and not as flexible or portable as needed by the Army.	Respond to attack/event

Priority	Gap	Gap Description	Capability
12	Forensic & threat analysis technologies	The Army requires the capability to remotely and rapidly capture, analyze and exploit forensic evidence, and deploy countermeasures on cyber assets.	Respond to attack/event
13	Intrusion detection, response & recovery technologies	Available COTS and open-source individual data set systems were not designed to operate within low-bandwidth tactical environments.	Respond to attack/event

Capability Progression/JCA Alignment (FY 17, FY 18–21)

Initiative	Joint Capability Area 6 Net-Centric													
	6.3 Net Management						6.4 Information Assurance							
	6.3.1 Optimized Network Functions and Resources	6.3.2 Deployable Scalable and Modular Networks	6.3.3 Spectrum Management			6.3.4 Cyber Management	6.4.1 Secure Information Exchange		6.4.2 Protect Data and Network			6.4.3 Respond to Attack/Event		
	6.3.1.1 Network Resource Visibility		6.3.3.1 Spectrum Monitoring	6.3.3.2 Spectrum Assignment	6.3.3.3 Spectrum Deconfliction		6.4.1.1 Assure Access	6.4.1.2 Assure Transfer	6.4.2.1 Protect Against Network Infiltration	6.4.2.2 Protect Against Denial or Degradation of Services	6.4.2.3 Protect Against Disclosure or Modification of Data	6.4.3.1 Detect Events	6.4.3.2 Analyze Events	6.4.3.3 Respond to Incidents
FY 17 Targeted Capabilities	•	•	•	•	•	•	•	•	•	•	•	•	•	•
FY 18-21 Targeted Capabilities	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Net Management

Network operations is a component of Signal support to warfighters and provides the business operations that establish, operate, manage, protect and defend the network. Network operations will enable authorized users to execute effectively their mission by leveraging the following network capabilities: optimized network functions and resources; deployable scalable and modular networks; cyber management; and spectrum management. Network operations includes, but is not limited to, enterprise management, net assurance and content management. Network operations provides commanders situational awareness to make informed command and control decisions. Cyberspace situational awareness will be achieved through the operational and technical integration of enterprise management with defense actions and activities across all levels of command.

Optimized Network Functions and Resource

- In FY 17, the Army will continue to optimize network functions and resources through the standardization of network operations. Standardization will extend across the institutional and operational environments, which will support the defense, health and maintenance of the network. Additionally, network operations may be influenced by unique and complex tools that are deployed at multiple echelons. For example, as solutions are procured to support requirements (such as MC systems), often a network operations tool, or tools, accompanies each solution. As tools are consolidated, hosted and maintained at the enterprise level, network management personnel and processes will be streamlined. Concurrently, the Army will focus on enhancing Army-wide network resource visibility with phase one of a cloud-based commercial enterprise ITSM capability. Current ITSM processes and services across the Army and DoD are managed in a decentralized manner, which has resulted in attempting to conduct asset visibility operations through a decentralized approach. Second Army and Network Enterprise Technology Command (NETCOM) will begin delivering high-quality, standard and reliable ITSM as a service to network consumers via repeatable processes using commercially managed and owned enterprise cloud-based capabilities. DoDIN and Army asset visibility and network operations will integrate with ITSM to provide commanders a real-time view of all assets.

- In FY18-21, network operations must transform along with the DoDIN to support new warfighting, intelligence and business processes. Network operations should enable users to access and share trusted information in a timely manner with advanced technologies. Enterprise ITSM will be implemented globally across the Army network. Within this global ITSM capability, the Army will deploy asset visibility services fully designed, developed and delivered to meet the strategy of receiving services from a commercially managed cloud-based system.

- By the end of FY 21, the Army will have situational awareness dashboards configured for the installation, Regional Cyber Centers, the Army Cyber Operations Integration Center, Army Cyber Command, Second Army, functional commands and other designated commands. These dashboards will draw their data from a single capability that performs asset visibility across the network. Establishing an enterprise ITSM will improve the Army’s ability to make IT investment decisions through the automatic and routine collection of information on network capabilities (e.g., systems, applications, software and devices). ITSM will aggregate and publish select network asset information automatically collected by the NIPRNet and SIPRNet environment of specific network operation tools. It will serve as an authoritative source for consolidated asset data, making this data available to end users via web services. Approved organizations may utilize ITSM for a range of activities, including but not limited to: supporting Army business requirements, such as acquisition and life-cycle replacement; enabling enhanced reporting and analysis for the general command, control and compliance of IT assets; and enhancing commanders' situational awareness of asset inventory. The completion of asset visibility will help drive down costs by removing legacy software and systems from the Army network. Finally, future network operations must continue to provide commanders the ability to effectively control, manage, defend and operate in and through the cyberspace domain.

Deployable, Scalable and Modular Networks

- Continuing in FY17-21, as part of extending network operations enterprise services, commanders on the ground will have the capability to manage their element of the network as the mission dictates. The Army will continue to tailor network operations capabilities to ensure that tools are adaptable and responsive to the commander's needs in a mature theater or austere environment, and to allow adjustments to the network in response to ever-changing cyber threats.

Spectrum Management

- In FY 17, the Army will continue to implement the Electronic Warfare Planning & Management Tool (EWPMT) by incorporating comprehensive electromagnetic spectrum operations comprised of electronic warfare (EW) and spectrum management operations (SMO) capabilities. EW capabilities consist of electronic attack, electronic protection and electronic warfare support. SMO functions deliver the capabilities to perform frequency assignment and host-nation coordination, and develop policy. Combined, these capabilities enable planning, management and execution of operations within the electromagnetic operational environment during all phases of military operations, and give commanders the ability to shape EW operational environments to their advantage.
- In FY 18-21, the Army will continue implementation of EWPMT by updating EW operations and SMO capabilities. Emerging requirements will include cyber situational awareness, offensive cyberspace operation and Pseudolite planning and management.
- By the end of FY 21, EWPMT will provide the commander and staff the tools to more effectively and efficiently plan, coordinate and synchronize EW throughout the operations process.

Cyber Management

Enterprise Service Management:

- In FY 17, the Army will begin implementing a standard ITIL 2011 ITSM approach and conducting enterprise service management by delivering services through a commercial cloud service provider. This enterprise service management approach is called Enterprise Service Management System as a Service (ESMSaaS). ESMSaaS will be a globally distributed network operations software component of the larger ITSM implementation.
- In the FY 18-21 timeframe, the Army will be fully capable of managing the IT enterprise as a service, driving down cost and creating high value for network consumers and operators. ESMSaaS will be executed globally across the Army network, and tactical and Joint ITSM services/platforms will be integrated with ESMSaaS. All legacy systems' tools should be off the network and retired, or in the process.
- By the end of FY 21, ITIL 2011 processes will be in place for incident management, problem management, change management, service asset and configuration management, request fulfillment (self-service), service catalog management and financial management. Also, enterprise management dashboards for network operations, computer network defense ticketing, enterprise analytics and trending will be centralized Army-wide for the SIPRNet and NIPRNet.

Single Security Architecture (SSA) Management:

- In FY 17, JRSS will continue to provide a logical path to the JIE SSA on CONUS and OCONUS bases, posts, camps and stations (B/P/C/S). JRSS/Joint Management System

(JMS) 1.0 will implement a hubs-and-spokes configuration to provide capabilities to manage network operations. As part of this process, the Army will remove its top-level architecture (TLA) and the Air Force will take down its gateways. EUCOM will migrate its TLA to Wiesbaden's JRSS. Marine Corps and Navy boundaries will be peered and their traffic will pass through JRSS. JRSS/JMS 1.5 will deploy multiple new tools and capabilities, such as Cyberspace Situational Awareness Analytic Cloud analytical capabilities, and integrate them with Service and DISA DoDIN Operations and defensive cyberspace operations internal defensive measures (DCO-IDM) tactics, techniques and procedures. Service network operations and DCO-IDM cyberspace operations centers will use the JMS to fulfill their Title 10 responsibilities. DISA will provide JRSS operation and maintenance.

- In FY 18 and beyond, JRSS/JMS 2.0 capabilities will include the Enterprise Operations Center (EOC) and which will provide a logical path toward the JIE single security architecture (SSA) on CONUS and OCONUS B/P/C/S. JRSS/JMS 2.0 capabilities will support perimeter protection of Core Data Centers, IPNs and the B/P/C/S perimeter. When fully deployed, they will support all current and future stakeholders within Combatant Commands, Services and agencies. The JIE EOC will evolve to manage the network and the SSA. JRSS will also evolve and provide border protection capabilities for the SSA. JMS will be absorbed into the EOC to manage selected SSA capabilities.
- By the end of FY 21, JRSS/JMS 2.0 will add additional capability necessary for the Navy and USMC to remove their boundary stacks, migrate to JIE EOC capabilities, integrate the JIE out-of-band network and implement the Global Emergency Operations Center concept.

Information Assurance

Secure Information and Exchange

Assure Access

Identity and Access Management:

- In FY 17-21, the Army will continue to implement an enterprise service-based access management capability, building on the integrated IdAM framework. This framework will provide seamless network access for identification, authentication, authorization and accountability for personnel (military, civilian, contractor, etc.) accessing logical and physical resources. It will allow the Army to eliminate the standalone access control mechanisms for applications, systems and networks that are often insecure, inefficient and redundant. In FY 17, the framework will conduct the following actions for all Army logical and physical resources.
    - Transition all applications from using Army SSO to direct PKI, DoD Self-Service Logon or a common authentication service access management-based capability using Common Access Card-embedded metadata in conjunction with authoritative attributes from the Defense Manpower Data Center.
    - Decouple applications from existing active directories to enable users to access IT resources across different security and organizational boundaries.
- During the FY 18-21 timeframe, the Army will further enhance IdAM capabilities to provide a family of security services that supports a distributed computing capability

through higher security assurance, with agility and adaptability for the enterprise. The enterprise framework will:

- Enable on-demand selection of identities and privileges for dynamic access controls in enterprise applications.
- Provide strong authentication and SSO, and fine-grained control over distributed computing capabilities.
- Enable robust insider threat awareness through identification of anomalies, potential security risks and exposure by analyzing how data are being utilized based on user context and behavior.
- Identify the ability to evaluate associations, trends and patterns in user-access privileges that may violate guidelines or present security risks.
- Create a protected service for privileged identity credentials that retains role-based access control and monitors and records privileged user sessions.
- Provide the ability to automatically discover resources as they are created in a hybrid environment and to automatically apply policy in order to maintain control.
- Assess biometric technologies within the Army in accordance with guidance received, based on the availability of funding.

- By the end of FY 21, the Army will have established an enterprise IdAM framework to oversee policies, standards, requirements and technologies that use digital identities for identification, authentication, authorization and accountability for logical and physical access controls (e.g., to applications, networks, systems, buildings, rooms, etc.) required for the full range of military and business operations. This framework will align with DoD, JIE and federal identity, credential and access management requirements and regulations, and ensure full interoperability with UAPs.

Assure Transfer

Cryptographic Modernization Initiative:

- In FY 17, the Army's Cryptographic Modernization Initiative (CMI) will continue to modernize through innovative technologies to enhance network capacity, performance (reliability, availability and confidentiality) and interoperability, with the objective of enabling secure information sharing across the Army and UAPs. Cryptographic modernization efforts will provide the required technology, ensuring that it is interoperable with KMI net-centric capabilities that enable OTNK for secure distribution of cryptographic keys across the Warfighter and Business Mission Areas. This modernized cryptographic technology is mandatory to support the Army's requirement to build network capacity and improve network performance on Army installations.

- In FY 18-21, the Army will continually enhance and modernize cryptographic capabilities in order to adjust to the rapid changes in cyber warfare and network vulnerabilities and protect sensitive information as enterprise services are extended to the tactical edge. The following efforts are critical to successfully implementing modern technology and eliminating capabilities that are no longer logistically supportable, sustainable or maintainable.

    - More-capable cryptographic protection through the replacement of legacy algorithms with modern ones.

  - Support operations in the JIE through cryptographic interoperability and releasability.
  - Capacity for future upgrades of cryptographic systems via programming new features and algorithms.
  - Enable net-centric and transparent key and equipment management to ease logistical burdens and enable enhanced flexibility and interoperability, thus eliminating manual processes.
  - Support on-the-move command and control to dramatically increase real-time information flow through voice, data and secure VTC; and access classified knowledge centers at various security levels (unclassified to top secret/ sensitive compartmented information).
  - CMI will ensure compliance with national-level directives to improve network security through the divestiture of legacy devices that place National Security Systems (NSS) and National Security Information (NSI) at grave risk. The Army will also adapt policies and procedures to provide oversight and guidance as we implement new technologies, modernize and prepare for transformation.
- By the end of FY 21, the Army will have complied with all required DoD and NSA mandates for modernization of cryptographic capabilities to protect our NSS and NSI. The Army will continue to leverage emerging and innovative technologies in accordance with DoD, NSA and the JIE to ensure security, interoperability and appropriate protection for the exchange of authentic data between authorized individuals, groups and entities.

Modernization of Enterprise Key Management Services:

- During FY 17, the Army will transition the 92 remaining EKMS Tier 2 accounts to KMI for web-based, net-centric key management and software provisioning technologies, which will enhance network mission planning and operations in accordance with EKMS Notice #252 End of Life (20 Aug 12).
- In FY 18-21, the Army will continue to implement KMI technology for the secure delivery of communications security (COMSEC) products and services, which enable cryptographic and cybersecurity devices across the network. After the completion of the Tier 2 transition, KMI will be able to utilize all networks (SIPRNet, NIPRNet and Joint Worldwide Intelligence Communications System) as a backbone for accessing key management services for net-centric key delivery and OTNK. This capability will further reduce warfighter exposure to risks associated with manual distribution of cryptographic keys. It also will modernize operational key management services for the sharing of Service/agency COMSEC databases' device registration; and provide greater support to NATO, allied and coalition partners, resulting in improved identification, authentication and global access for warfighters.
- By the end of FY 21, all EKMS Tiers (0-2) will have transitioned to KMI, ensuring net-centric capability and operations within a trusted key management architecture. This, in turn, will improve the availability, operation and management of COMSEC products and services, enabling secure end-to-end communications. The Army also will be able to switch from manual to secure automated distribution of keys across the force and UAPs.

Protect Data and Networks

Mobility:

- In FY 17, the Army will achieve significant advancements in unclassified and classified mobile services. Mobile device capability will provide the Army user the ability to perform work functions over a secure network at any time, from anywhere. The Army is targeting derived credentials and thin client as the primary methods for accessing enterprise resources and authenticating users. Users leveraging mobile devices will be properly identified and verified, and measures will be established to ensure that data are appropriately protected depending on the classification.
- In FY 18-21, the Army will build Installation Campus Area Networks to enable wireless connectivity for government-furnished equipment while operating within the boundaries of the post, camp and station.
- By the end of FY 21, the Army's plan is to enable the use of personal commercial mobile devices, commonly known as "bring your own device" (BYOD). Authorized, authenticated and validated mobile users will provision the BYOD for DoD/Army use, with the authorized user retaining responsibility for the hardware and cellular voice and data plans. The Army will be responsible for the connections into DoD- and Army-protected network recourses.

Respond to Attack/Event

- In FY 17, the Army will enhance cyber situational awareness by leveraging Big Data technology and behavioral analytics to address gaps in automated sensing; response and reporting; forensic and threat analysis technologies; and intrusion detection, response and recovery technologies. The Army will provide storage capacity and analytics tools to aggregate and correlate threat indicator data. This capability will provide cyber defenders near-real-time risk threat detection, thus reducing the time required to respond and mitigate. Armed with enhanced situational awareness, and an accurate and timely picture of the friendly and enemy environments, we will also invest in a platform of computing resources from which defensive cyberspace operations forces can draw to maneuver to a target of interest or threat, and deliver tools or payloads to achieve desired effects.
- In FY 18-21, the Army will proportionately invest in these critical capability areas to ensure that defensive cyber forces can operate decisively against the most sophisticated adversaries. The Army will continue to engineer the network such that all requisite data populate a distributed Big Data analytics platform. These are critical years in which to build upon foundational DCO capabilities, rooted in situational awareness.
- By the end of FY 21, the Army's DCO forces will have unprecedented access to advanced data analytics and substantially enhanced red and blue situational awareness. Similarly, with the inevitable growth of cyber operations as a force multiplier, Army units will be empowered to remotely access critical targets and terrain, deliver advanced payloads and measure the effectiveness of their operations.

Dependencies

Network management is required for successful data migration. The NSD must ensure that the selected standardized family of EUDs is able to support data protection on all devices, to encrypt data on devices and to conduct vulnerability and patch management on network and mobile devices. Cybersecurity is required for the proper functioning of enterprise services.

The NSD relies heavily upon NCD for the foundational elements that enable Network Operations and Security tools and processes to function. Below is a description of high-level dependencies among the NCD, AEN domains, and key external stakeholders.

- Network Capacity Domain: The integration of information transport mechanisms and consolidation and standardization of computing services enables the NSD to provide improved network management through the implementation of standardized, end-to-end network operations tools and enhanced asset visibility. Network infrastructure standardization facilitates improved cybersecurity by reducing the network attack surface and enabling the utilization of standardized, enterprise-level cybersecurity tools. NCD also creates the network capacity necessary to deliver encryption keys over the network thereby reducing Soldiers' exposure to the hazards of the battlefield.
- Enterprise Services Domain: The consolidation and standardization of computing services along with the removal of legacy applications and systems enhances network operations and cybersecurity by enabling asset visibility and centrally managed hosting accessible from anywhere on the network. The ESD must ensure standards and specifications for enterprise services enable access to ESMSaaS at all echelons.
- The NSD has strong dependencies with external stakeholders, including DISA for implementation of Joint Management System. In addition, the establishment and enforcement of COE standards and specifications will shape the modernization of network operations and cybersecurity tools and processes.

Summary

The NSD capabilities provided in the FY 17-21 timeframe, coupled with the requisite personnel, tactics, techniques and procedures, establish the framework to secure the network and protect critical data and information for Army and UAP missions. The overall benefits to be realized by the Army are:

- The elimination of standalone access control mechanisms for applications, systems and networks which were often insecure and inefficient.
- Improved network performance and interoperability that enable secure information sharing across the Army and UAPs.
- Enhanced mission planning and operations based on a web-based, net-centric key management infrastructure.
- Improved security due to fewer ingress and egress points on the network and greater asset visibility.
- Improved security of mobile devices and a reduction in the number of mobile devices per user.
- Improved information sharing and reliability, and lower command, control, communications, computers and information management service delivery costs.

Appendix 4 – Capability Taxonomy by Domains

Network Capacity Domain

Information Transport – The ability to transport information and services via assured end-to-end connectivity across the network. (JCA 6.1)

Wired Transmission – The ability to transfer data or information with an electrical/optical conductor. (JCA 6.1.1)

Localized Communications – The ability to disseminate, transmit or receive voice, data, video and integrated telecommunications via wire or optical means within the confines of a platform or an installation (e.g., command post, post, camp, station, base, installation, headquarters or federal building). (JCA 6.1.1.1)

Long-Haul Telecommunications – The ability to disseminate, transmit or receive voice, data, video and integrated telecommunications via wire or optical means to, from and between platforms and/or installations (e.g., command post, post, camp, base, stations or federal buildings). (JCA 6.1.1.2)

Wireless Transmission – The ability to transfer data or information without an electrical/optical conductor. (JCA 6.1.2)

Line of Sight – The ability to exchange data or information via electromagnetic spectrum within the line of sight. (JCA 6.1.2.1)

Beyond Line of Sight – The ability to exchange data or information via electromagnetic spectrum beyond the line of sight. (JCA 6.1.2.2)

Switching and Routing – The ability to move data and information end to end across multiple transmission media. (JCA 6.1.3)

Communication Bridge – The ability to interface two or more common communications media or networks. (JCA 6.1.3.1)

Communication Gateway – The ability to interface two or more disparate communications media or networks. (JCA 6.1.3.2)

Computing Services – The ability to process data and provide physical and virtual access to hosted information and data centers across the enterprise based on established data standards. (JCA 6.2.2)

Shared Computing – The ability to provide computing processing and storage resources that can be used by more than one component, community of interest, program or DoD user. (JCA 6.2.2.1)

Distributed Computing – The ability to provide a virtual computing capability to an end user or application through federation of distributed, location-independent computing resources. (JCA 6.2.2.2)

Server Services – The ability to compute, process, host and control information within the network to provide client services at the edge of and throughout the network. Subcategories include server computing, production and mass storage. (JCA 6.2.2.3)

End-User Services – The ability to provide client computing and mobile voice, data and video devices, to include pagers, cell phones, wireless/cellular enabled personal data assistants (PDAs), and other end-user devices used by individuals to access information, applications and services; and management of those devices. (JCA 6.2.2.4)

Enterprise Services Domain

Core Enterprise Services – The ability to provide awareness of, access to and delivery of information on the DoD Information Network via a small set of CIO-mandated services. (JCA 6.2.3)

User Access (Portal) – The ability to access user-defined DoD enterprise services through a secure single entry point. (JCA 6.2.3.1)

Collaboration – The ability to conduct synchronous and asynchronous communications and interaction across the enterprise, including voice, data, video and manipulated visual representation. (JCA 6.2.3.2)

Content Discovery – The ability to identify, search for and locate relevant information. (JCA 6.2.3.3)

Content Delivery – The ability to accelerate delivery and improve reliability of enterprise content and services, by optimizing the location and routing of information. (JCA 6.2.3.4)

Enterprise Messaging – The ability to perform electronic messaging between users and organizational entities across the enterprise, including providing customer support. (JCA 6.2.3.6)

Directory Services – The ability to provide, operate and maintain a global directory of users, to include directory synchronization with other lower-level systems and information integrity. (JCA 6.2.3.7)

Enterprise Application Software – The ability to provide productivity enhancement software to all users. (JCA 6.2.3.8)

Position, Navigation and Timing – The ability to determine accurate and precise location, orientation, time and course corrections anywhere in the battlespace and to provide timely and assured PNT services across the DoD enterprise. (JCA 6.2.4)

Network Operations and Security Domain

Net Management – The ability to configure and re-configure networks, services and the underlying physical assets that provide end-user services, as well as connectivity to enterprise application services. (JCA 6.3)

Optimized Network Functions and Resources – The ability to provide DoD responsive network functionality and dynamically configurable resources, to include allocation of required bandwidth, computing and storage. (JCA 6.3.1)

Network Resource Visibility – The ability to determine real-time status and effectiveness of network services and resources. (JCA 6.3.1.1)

Rapid Configuration Change – The ability to rapidly configure and reconfigure enterprise services and resources in concert with the established CONOPS. (JCA 6.3.1.2)

Deployable Scalable and Modular Networks – The ability to design, assemble, transport and establish mission-scaled networks from adaptable components' network modules. (JCA 6.3.2)

Spectrum Management – The ability to synchronize, coordinate and manage all elements of the electromagnetic spectrum through engineering and administrative tools and procedures. (JCA 6.3.3)

Spectrum Monitoring – The ability to monitor and characterize the electromagnetic environment. (JCA 6.3.3.1)

Spectrum Assignment – The ability to identify spectrum requirements; evaluate electromagnetic environmental effects (E3); and dynamically plan, allot and modify frequency assignments to exploit available spectrum. (JCA 6.3.3.2)

Spectrum Deconfliction – The ability to dynamically predict, detect and mitigate frequency interference. (JCA 6.3.3.3)

Cyber Management – The ability to assure network support for all DoD missions through the synchronization, deconfliction, coordination and awareness of all elements of computer network operations. (JCA 6.3.4)

Information Assurance – The ability to provide the measures that protect, defend and restore information and information systems. (JCA 6.4)

Secure Information Exchange – The ability to secure dynamic information flow within and across domains. (JCA 6.4.1)

Assure Access – The ability to identify and authenticate individuals, groups and entities, and provide authorization to services and information. (JCA 6.4.1.1)

Assure Transfer – The ability to exchange authentic data, information and knowledge between authorized individuals, groups and entities. (JCA 6.4.1.2)

Protect Data and Networks – The ability to anticipate and prevent successful attacks on data and networks. (JCA 6.4.2)

Protect Against Network Infiltration – The ability to prevent unauthorized access. (JCA 6.4.2.1)

Protect Against Denial or Degradation of Services – The ability to prevent or contain activities that may degrade or deny authorized use of network resources. (JCA 1.4.2.2)

Protect Against Disclosure or Modification of Data – The ability to prevent or contain activities that may expose or modify data. (JCA 6.4.2.3)

Respond to Attack/Event – The ability to maintain services while under cyber attack, to recover from cyber attack and to ensure availability of information and systems. (JCA 6.4.3)

Detect Events – The ability to identify anomalous activities and behavior. (JCA 6.4.3.1)

Analyze Events – The ability to diagnose anomalous activities and behavior by determining cause and characterizing and assessing impact. (JCA 6.4.3.2)

Respond to Incidents – The ability to take action to mitigate the impact of anomalous activities and behavior. (JCA 6.4.3.3)

Appendix 5 – Acronyms

Acronym	Definition
ABAC	Attribute-Based Access Control
ADMP	Army Data Management Program
AEN	Army Enterprise Network
AESD	Army Enterprise Service Desk
ANCP	Army Network Campaign Plan
B/P/C/S	Bases/Posts/Camps/Stations
BYOD	Bring Your Own Device
CDC	Core Data Center
CIO	Chief Information Officer
CMI	Cryptographic Modernization Initiative
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial Off-the-Shelf
CP CE	Command Post Computing Environment
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIN	DoD Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy
EHF	Enterprise Hosting Facility
EIEMA	Enterprise Information Environment Mission Area
EKMS	Electronic Key Management System
ESMSaaS	Enterprise Service Management System as a Service
EUD	End-User Device
EXORD	Execution Order
FY	Fiscal Year
Gbps	gigabits per second
IC	Intelligence Community
ICD	Initial Capabilities Document
IC-ITE	Intelligence Community Information Technology Enterprise
IdAM	Identity and Access Management
IPN	Installation Processing Node
ISN	Installation Service Node
IT	Information Technology
ITE	Integrated Training Environment
ITSM	Information Technology Service Management
JCA	Joint Capability Area
JIE	Joint Information Environment
JRSS	Joint Regional Security Stack
KMI	Key Management Infrastructure

Acronym	Definition
L/V/C/G	Live/Virtual/Constructive/Gaming
LOE	Line of Effort
MC	Mission Command
MPLS	Multi-Protocol Label Switching
NCD	Network Capacity Domain
NIPRNet	Non-Secure Internet Protocol Router Network
NSD	Network Operations & Security Domain
NSI	National Security Information
NSS	National Security System
OTNK	Over-the-Network-Keying
PKI	Public Key Infrastructure
PNT	Position, Navigation and Timing
SATCOM	Satellite Communications
SIPRNet	Secure Internet Protocol Router Network
SSO	Single Sign-On
SPPN	Special Purpose Processing Node
TS/SCI	Top Secret/Sensitive Compartmented Information
UC	Unified Capabilities
UJTL	Universal Joint Task List
VoIP	Voice over Internet Protocol
VTC	Video Teleconference