

Office of the Army Chief Information Officer/G-6

ARMY NETWORK CAMPAIGN PLAN

IMPLEMENTATION GUIDANCE

MID TERM

2018-22



CIO/G-6
ENABLING SUCCESS For Today and Tomorrow



U.S. ARMY



CIOG6.ARMY.MIL

DISCLAIMER

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 Do not cite this document for the purpose of advertisement.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. This iteration of the *Army Network Campaign Plan Implementation Guidance, Mid Term* refines modernization planning and execution activities across multiple communities of interest and practice, including resource planning, acquisition and policy development, to ensure that investments and the information technology solutions delivered support the Army Vision and Army Operating Concept. As part of these efforts, the Army will synchronize hardware, applications and services that support both warfighting and business operations, using assessments conducted as part of the Army Enterprise Network portfolio management process and the Army Warfighting Challenge process. In fiscal years 2018-22, the Army will maintain and modernize the network through targeted capabilities that are designed to improve network infrastructure, deliver enterprise-level services and manage and secure the network.

The Army is working with key mission partners to implement several initiatives, including cloud-based solutions and services to advance the Army's long-term objective to reduce ownership, operation and sustainment of hardware and other commoditized information technology. This, in turn, will significantly boost IT operational efficiency, increase network security, improve interoperability with mission partners and posture the Army to adopt innovative technology more quickly at lower cost.

By the end of FY17, Army network infrastructure will 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. This will empower garrison-based and Home-Station Mission Command operations, enable distributed live/virtual/constructive/gaming training, and enhance the readiness of deployable network components. The Army will have standard policies and protocols that support initiatives and tools to synchronize cybersecurity and network operations across all organizations. In addition, the Army will use a service-based, integrated, enterprise, access-management framework to identify, authenticate, authorize and account for users accessing enterprise services, and to provide user privilege management.

Network modernization will spur changes across the Army that will require analysis from a doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy perspective. Reexamining these areas for the FY18-22 period will present opportunities for the Army to reassess how it is task-organized, 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, leveraging advances in technology and addressing fiscal realities, 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
Army Chief Information Officer/G-6

UNCLASSIFIED

This page intentionally left blank.

UNCLASSIFIED

Table of Contents

Introduction.....	7
Army Network Campaign Plan (ANCP) Construct.....	7
ANCP, Mid-Term Construct.....	7
The Network in FY17	8
FY18-22 Overview	9
Impacts to the Army.....	12
Appendix 1 – Network Capacity Domain.....	1-1
Domain Overview	1-1
Network Capacity at the End of FY17	1-2
Overview of FY18-22 Capabilities.....	1-2
Mandates Driving Network Capability Modernization.....	1-2
Capability Gaps and Priorities.....	1-3
Capability Progression/Joint Capability Area (JCA) Alignment (FY18, FY19-22)	1-4
Information Transport	1-5
Computing Services	1-6
Dependencies.....	1-7
Summary.....	1-8
Appendix 2 – Enterprise Services Domain.....	2-1
Domain Overview	2-1
Enterprise Services at the End of FY17.....	2-1
Overview of FY18-22 Capabilities.....	2-2
Mandates Driving Network Capability Modernization.....	2-2
Capability Gaps and Priorities.....	2-3
Capability Progression/JCA Alignment (FY18, FY19-22)	2-4
Core Enterprise Services	2-4
Position, Navigation and Timing	2-8
Dependencies.....	2-8
Summary.....	2-9
Appendix 3 – Network Operations and Security Domain	3-1
Domain Overview	3-1
Network Operations and Security at the End of FY17	3-2
Overview of FY18-22 Capabilities.....	3-2
Mandates Driving Network Capability Modernization.....	3-2
Capability Gaps and Priorities.....	3-3
Capability Progression/JCA Alignment (FY18, FY19-22)	3-6
Net Management	3-6

UNCLASSIFIED

Cybersecurity 3-9
Defensive Cyber – Internal Defense Measures 3-12
Dependencies 3-13
Summary 3-13
Appendix 4 – Glossary 4-1
Appendix 5 – Acronyms 5-1

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 Army Enterprise Network (AEN) portfolio management process, the Army will maintain and modernize the network via synchronization of institutional and operational capabilities in fiscal years (FY) 2018-2022. This document begins to reflect the alignment of planning across all Army mission areas (Enterprise Information Environment, Warfighting, Business and Defense Intelligence). *The Army Network Campaign Plan – Implementation Guidance, Mid Term* builds upon the activities in the *ANCP – Implementation Guidance, Near Term*, which covers FY16-17, and 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 that align with the DoD Joint Information Environment (JIE): the *Army Network Campaign Plan*, the *ANCP – Implementation Guidance, Near Term* and the *ANCP – Implementation Guidance, Mid Term*. These documents were originally published in February 2015; the implementation guidance is intended to be updated on a yearly basis. The ANCP is designed to impact network planning activities across the Army. The table below describes the purpose of each document and the associated timeframes.

ANCP Document	Purpose	Timeframe
<i>Army Network Campaign Plan (ANCP)</i>	<ul style="list-style-type: none"> 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
<i>ANCP – Implementation Guidance, Near Term</i>	<ul style="list-style-type: none"> 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. 	2016-2017
<i>ANCP – Implementation Guidance, Mid Term</i>	<ul style="list-style-type: none"> Focuses on network capabilities. Designed to impact resource planning within Program Objective Memorandum venues. 	2018-2022

Table 1: ANCP Construct

ANCP, Mid-Term Construct

The *ANCP – Implementation Guidance, Mid Term* is a living document, updated 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 future network capabilities in FY18-22.

The mid-term guidance is developed along 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 (EIEMA) IT investments, acquisition plans and resourcing plans. Near- to mid-term activities, supported through IT investments, will be aligned, managed and tracked through the CIO/G-6’s five lines of effort (LOE).

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 are the current set of network priorities for the near and mid term. New LOEs will emerge based on the progress achieved in the execution of the near- and mid-term implementation guidance.

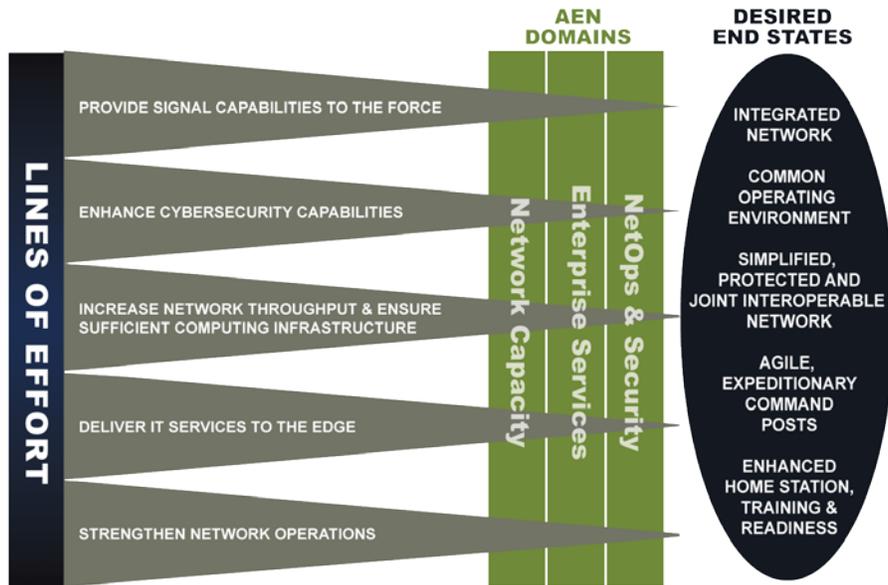


Figure 1: ANCP Operating Construct

The Network in FY17

By the end of FY17, 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. A more robust infrastructure will empower Home-Station Mission Command Center (HSMCC) operations and the Live, Virtual, Constructive Integrating Architecture (LVC-IA) in the Integrated Training Environment (ITE), while also 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. Common Operating Environment (COE) operational and interoperability certification test events are planned for FY16 and early FY17, which will inform key COE implementation decisions.

By the end of FY16, the Army will start providing locations in the continental United States (CONUS) a Unified Capabilities soft-client capability to enable non-assured voice, video and collaboration. Additionally a truly enterprise-wide service desk will begin to support global IT assistance to all Army users.

By the end of FY17, enterprise services will be made available through mobile devices in an efficient, consistent, secure and reliable manner. Standardized policies, protocols, supporting initiatives and tools will allow the Army to synchronize cybersecurity, data center and network operations across all organizations. The Army also will apply more stringent network security, to include vulnerability and patch management, and enhanced encryption to improve the secure exchange of information. Service-based enterprise access management and an integrated access management framework will identify, authenticate, authorize and account for users accessing enterprise resources, as well as manage user privileges. Combined with an integrated directory service capability, it will provide global access to user and resource information on the network.

The Army expects a gap in network modernization funding in FY16-17 that will likely result in an execution shortfall. In FY17, Network Enterprise Technology Command's funding is projected to be less than its FY14 operational budget. With installation IT infrastructure funded below FY16 levels, the Army may experience a slowdown in future network security improvement. Commands could also face a lack of technical support to maintain configuration and management of information assurance tools. Likewise, there may be an inadequate number of tools to secure systems and networks, which would raise the Army's vulnerability. Units' situational awareness may be impacted by a shortfall in funding for Blue Force Tracking in FY17. In addition, the Training Program Evaluation Group did not accept increases in requirements for Iridium/Enhanced Mobile Satellite Service airtime in FY17. All of these efforts will cause a shift in Program Objective Memorandum (POM) planning for FY18-22.

FY18-22 Overview

Using a phased approach, the Army will continue to modernize the network through implementation of multiple, targeted capabilities¹ within the FY18-22 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 FY18-22 timeframe.

POM planning in FY18-22 will provide the Army the capability to operate, manage and defend the network. Army network operations are largely funded to the correct levels, given current priorities, to support operations without creating a year-of-execution issue. Investment accounts are lower than desired but staff continue to realign funds into these accounts. Persistent

¹Targeted 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. This assessment also incorporates other mission area plans to determine end-to-end network impacts.

underfunding of the Army Data Center Consolidation Program (ADCCP) below critical requirements will require the Army to shift to an alternative, cost-reimbursable approach with customers. The Army expects to redirect Defense Information Systems Agency-provided savings from restructured long-haul communications service rates to modernization efforts primarily focused on Installation Campus Area Networks (ICANs).

Installation upgrades, to include fielding of Joint Regional Security Stacks (JRSS) and procurement of network operations tools and a base support communications capability (i.e., the non-tactical Land Mobile Radio network), as well as data center consolidation efforts, will continue in FY18-22. The inability to fully upgrade installation networks, security infrastructure, network operations tools and base support communications infrastructure in FY18-22 would force the retention of legacy infrastructure and associated costs. Routine, systematic evaluation and disposition of excess IT equipment and end items will, over time, reduce overall equipment sustainment costs.

Figure 2 depicts the Enterprise Information Environment Mission Area domain’s alignment with the Army IT Portfolio Management construct. This process reviews network capabilities on a yearly basis to determine gaps in the network capabilities needed to support Army strategy. The main outputs of the portfolio management process are the ANCP near- and mid-term implementation guidance documents. For a more in-depth review of the capabilities within each domain, refer to Appendices 1-3.

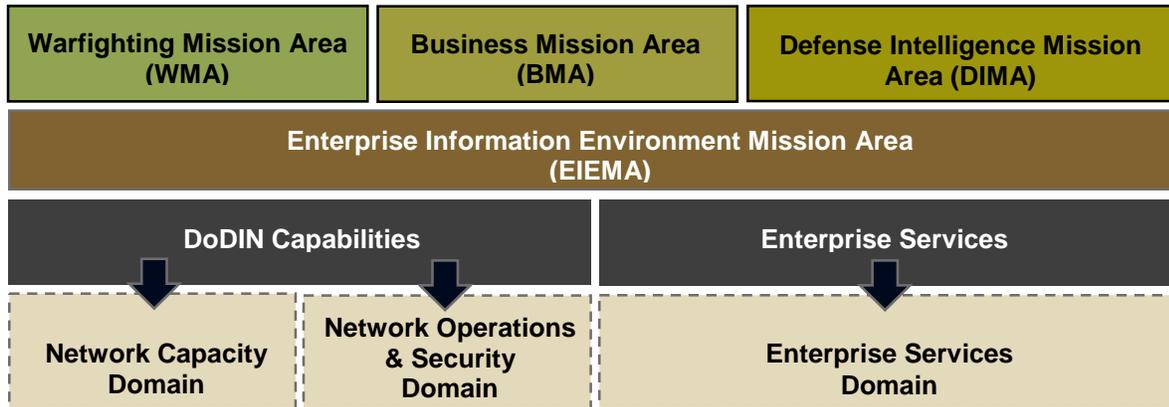


Figure 2: Army IT Portfolio Management Construct

The Network Capacity, Enterprise Services and Network Operations and Cyberspace domains are aligned with the three CIO/G-6 directorates: Architecture, Networks, Operations and Space (AONS), Policy and Resources, and Cybersecurity. The capabilities within each domain are also categorized by Joint Capability Areas.

The following table provides an overview of the AEN domains, capability areas and capabilities for development in FY18-22.

Network Capacity	<p>Information Transport</p> <ul style="list-style-type: none"> • Continue installation infrastructure modernization to improve wired information transport throughput and performance. • Continue implementation of Joint Regional Security Stacks. • Continue modernization to improve 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. <p>Computing Services</p> <ul style="list-style-type: none"> • Consolidate 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 data and information, including authoritative data sources that reside at the enterprise level, from any location and approved device. • Provide fusion and analysis 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 operation and management guidelines to improve operation and sustainment processes based on the streamlined data center and application architectures. • Field Common Operating Environment (COE) Version 3 in FY19. • Implement published standards that define the common software foundation for the Mobile Hand-held Computing Environment in FY19.
Enterprise Services	<p>Core Enterprise Services</p> <ul style="list-style-type: none"> • Consolidate standalone, legacy solutions to enterprise capabilities. • Provide global directory services with contextual search. <ul style="list-style-type: none"> • Provide an enterprise collaboration service enabling synchronous and asynchronous collaboration for users end to end. • Provide a single point of access to information. • Provide a service desk capability that is supported by standardized processes across the institutional and tactical environments. <ul style="list-style-type: none"> • Provide the Army Software Marketplace (ASM) as an enterprise service in FY19.

Network Operations and Security	<p>Net Management</p> <ul style="list-style-type: none"> • Provide a single capability that performs enterprise asset identification. • Standardize network operations across the network. • Provide tools and training that simplify network management. <p>Cybersecurity</p> <ul style="list-style-type: none"> • 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 via physical distribution. • Synchronize and integrate continuous monitoring solutions. • 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). <p>Defensive Cyber – Internal Defense Measures</p> <ul style="list-style-type: none"> • Provide cyber defenders near-real-time risk and threat detection. • Implement storage capacity and analysis tools to aggregate and correlate threat indicator data.
---------------------------------	---

Table 2: AEN domains, capability areas and capabilities for development

Impacts to the Army

In FY18, the Army will be at a critical point in network modernization while facing a landscape of changing missions and budgetary constraints. To build on the current network modernization momentum, the Army will continue to gain efficiencies and reduce costs through divestiture of legacy systems and maximization of enterprise capabilities. Rigorous assessments through the AEN process will continue to balance network capability investments. The Army will be positioned to drive down operating and sustainment costs by more actively pursuing and leveraging advances in technology.

The Army will continue to modernize the network from the tactical edge to the installation, enabling the transition to a regionally aligned, expeditionary fighting force. Soldiers and units will experience enhancements and improvements to capabilities across the network, specifically, more direct and transparent access to enterprise-level services utilizing HSMCC, Installation as a Docking Station, the Integrated Training Environment and authoritative data sources. Operating and generating forces’ network access will bring dynamic computing power to the Soldier level, facilitating 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 2022, the agility and versatility needed by the Army to meet mission requirements and mitigate an ever-evolving threat landscape will be further enhanced by the network.

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 within 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’s objectives are to provide a resilient transport network, an optimized, responsive computing and storage capability, and a range of user device options that promote continuous advantage across all operational phases.

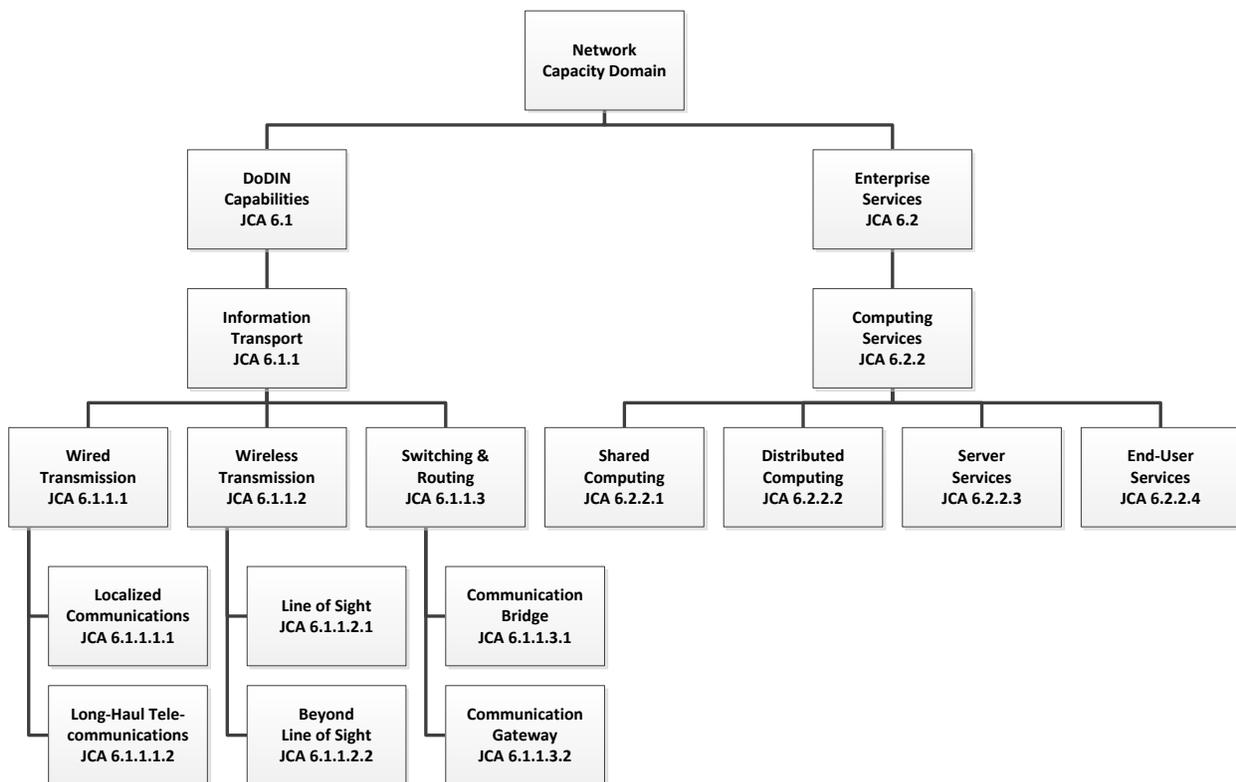


Figure 3: NCD Capability Taxonomy

Network Capacity at the End of FY17

By the end of FY17, the Army network will be significantly upgraded to provide the increased throughput and computing power necessary to extend current and projected enterprise services and capabilities to the point of need in all mission environments. The infrastructure will support rapid evolution and deployment of applications to meet changing user needs, and the staging of information to ensure access to it at the point of need as users (Army and other Services) transition between mission environments. The current Army network backbone connecting installations to the DoD Information Network (DoDIN) will be increased to 100 gigabits per second (gbps), with the on-site installation capacity increased from 1 gbps to 10 gbps at the majority of priority Army locations. Also trending toward a joint environment by the end of FY17, a significant portion of the Army's computing and data storage will be moved into approved DoD enterprise hosting facilities (EHF)^{2,3,4,5} to meet ever-changing computing and storage requirements while making data far more accessible to end users.

Overview of FY18-22 Capabilities

Within the FY18-22 timeframe, the Army will continue to migrate enterprise-ready applications and systems to the cloud while exploring advanced data storage techniques to more efficiently accommodate ever-increasing data maintenance needs. The computing infrastructure will be modernized to support cloud and distributed Big Data analytic 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 will initiate implementation of live, virtual and constructive (LVC) Integrated Training Environment (ITE) concepts, and extend enterprise business systems and enterprise capabilities. The Army will employ centralized management and decentralized fielding of end-user devices (EUDs), to include identifying and implementing a standard suite of devices, increasing efficiencies (e.g., Bring Your Own Device (BYOD)) and improving network security.

Mandates Driving Network Capability Modernization

FY18-22 NCD efforts are driven by Army guidance and external mandates, and reflect the need to provide a robust transport infrastructure; sufficient, modern, resilient and reliable computing

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 IPN per DoD installation but each IPN 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 become 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 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.

and storage capacity; and EUDs and mobile capabilities. Three major legislative and DoD mandates, listed below, are driving network capacity modernization activities.

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 (FY13 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 FY18 (DoD CIO memorandum, 11 July 2013). This remains an Army objective; however, due to technical complexities and fiscal constraints, efforts will continue through FY21.
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).

Table 3: Major Legislative and DoD Mandates Driving Network Capacity Modernization

The above 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 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 Orders (EXORDs), Concepts of Operations (CONOPS), policy changes, etc.).

Capability Gaps and Priorities

Using, but not limited to, the Universal Joint Task List (UJTL), the LandWarNet Initial Capabilities Document (ICD) and the Army Equipment Modernization Strategy, NCD conducted an analysis to identify and prioritize network capacity gaps for the FY18-22 timeframe. Comparing the FY17 NCD portfolio to mandates and requirements, such as network capacity-related UJTL and LandWarNet ICD elements and Mission Command Concept 2020-2040, led to the identification of several capability gaps. The number of UJTL and LandWarNet ICD elements aligned to each gap informed the prioritization effort. The table below shows the prioritized NCD FY18-22 capability gaps.

Priority	Gap	Gap Description	Capability
1	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 Internet (TI).	Information transport
2	Network reach	The network reach for lower-echelon tactical units is insufficient to conduct distributed operations. Lower TI reach in an environment without SATCOM is not enough to support cross-enclave and cross-unit communications in cases where the 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.

Priority	Gap	Gap Description	Capability
3	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	Wireless local communications	Installation wireless infrastructure is not mature enough to support increasing demand for local/installation computing and services.	Information transport
5	Installation network throughput	Current, aging installation wired/copper cable infrastructure does not adequately support emerging IP-based demands, such as VoIP, Voice over Secure IP and/or implementation of Installation as a Docking Station (IaDS).	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

Table 4: NCD Prioritized Capability Gaps

Capability Progression/Joint Capability Area (JCA) Alignment (FY18, FY19-22)

The table below shows the NCD capabilities that are targeted for modernization in FY18 and FY19-22.

Initiatives	Joint Capability Area 6 Communications and Computers									
	6.1 DoDIN Capabilities						6.2 Enterprise Services			
	6.1.1 Information Transport						6.2.2 Computing Services			
	6.1.1.1 Wired Transport		6.1.1.2 Wireless Transmission		6.1.1.3 Switching and Routing		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
	6.1.1.1.1 Localized Communications	6.1.1.1.2 Long-Haul Telecommunications	6.1.1.2.1 Line of Sight	6.1.1.2.2 Beyond Line of Sight	6.1.1.3.1 Communication Bridge	6.1.1.3.2 Communication Gateway				
FY17 Targeted Capability	•	•	•	•	•	•	•	•	•	•
FY18-21 Targeted Capability			•	•	•	•	•	•	•	•

Table 5: NCD Capabilities Aligned to JCAs

Information Transport

Wired Transmission

Localized Communications & Long-Haul Telecommunications

- In FY18, 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 FY19-22, as the end of the current wired infrastructure's life cycle approaches, the Army will begin to transform information transport on targeted installations from wired to wireless. Wired transmissions will be phased out while wireless transmissions will grow, 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 FY22, the Army will be in a position 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 FY18, the NCD will continue modernizing the throughput and performance of wireless information transport for deployable units. The goal is more reliable and versatile on-the-move tactical communications, as well as better connectivity between the lower and upper TI, which will improve the ability of commanders at all levels to collaborate with their forces.
- In FY19-22, the NCD will continue modernizing the throughput and performance of wireless information transport. Better connectivity between the lower and upper TI will enhance collaboration across the operating force, with wireless transmission improvements enabling lower-echelon tactical formations to support all forms of communication (voice, video and 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 greater demand for wireless information transport capabilities, which is tied to the exponential growth of mobility services and mobile devices.
- By the end of FY22, the NCD will provide more reliable and versatile on-the-move tactical communications for the force by increasing network throughput and reach, and improving unified action partners' connectivity. Wireless installation infrastructure at prioritized locations will provide information transport support for end-user mobility services.

Switching and Routing

Communication Bridge & Communication Gateway

- In FY18, the Army will continue to deploy Multi-Protocol Label Switching (MPLS) capabilities to maximize network capacity globally in alignment with G-3/5/7 priorities (as available resources allow).
- In FY19-22, the Army will optimize the benefits of information transport improvements in wired and wireless capabilities by synchronizing switching and routing enhancements.
- By the end of FY22, switching and routing enhancements will include nearly 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. The Army will have dual-path physical diversity at the lowest possible life-cycle cost while meeting performance specifications that provide scalability to 100 gigabit per second speeds and improve network performance and survivability at key installations.

Computing Services

Shared Computing, Distributed Computing & Server Services

- In FY18, the Army will continue executing the Federal Data Center Consolidation Initiative and DoD mandates to close, consolidate and standardize data centers. The Army anticipates closing or consolidating 139 data centers in FY18. This will enable centralized hosting of systems, applications and data storage, and will improve holistic enterprise operation and management processes. The Army intends to establish on-demand computing and data for the generating force if sequestration resources are restored. The Army Application Migration Business Office (AAMBO) will assist Commands with application migration to an authorized enterprise hosting environment.
- The Army will assess progress and, by FY19, adjust cloud migration efforts as necessary to improve cloud enablers, such as Unified Capabilities, common services, security (JRSS/MPLS), standardized hosting platforms (Infrastructure as a Service), the Army Software Marketplace and cloud access points. The Army will continue to focus on utilizing a COE that is software-based and hardware-agnostic.
- During FY19-22, necessary data center closure, consolidation and standardization tasks will continue as the number of closures increases across Army installations and applicable joint bases. The Army anticipates closing or consolidating four data centers in FY19 and one data center in 2021, when the final human resource applications are subsumed by the Integrated Personnel and Pay System-Army. Holistic enterprise operation and management processes will be refined, based on the streamlined data center architecture. Following an assessment, the Army will adjust cloud migration efforts in FY18 to improve cloud enablers by FY19.

- In FY18 the Army will continue to establish the Army Private Cloud Enterprise (APCE), which is a two- to five-year pilot that will systematically test, evaluate and define the acquisition, management and operations approaches to an on-premises, contractor-owned, contractor-operated (COCO) private cloud. Initially, the Army Private Cloud will serve Army customers (enterprise application users) around the world only; eventually, it will be open to other DoD and federal agencies as the capability matures.
- By the end of FY22, the NCD will enable the rapid and more efficient evolution of applications, minimizing cost and speeding dissemination of application enhancements through automated processes. The Army will complete the consolidation and standardization of data centers and centralized hosting of systems, networks and applications. The Army data center and applications landscape will be drastically smaller and cloud-enabled. The examination of data center operations and the associated DOTMLPF will further improve unified operations. Aligned with a software-based 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 Army Software Marketplace for applications in all computing environments (CE) that support the enterprise and tactical users, to include the Data Center/Cloud/Generating force CE, the Command Post CE, the Mounted CE, the Mobile-Handheld CE, the Sensor CE and the Real Time/Safety Critical/Embedded CE. Collectively, this will maximize automation potential.

End-User Services

- In FY18, the NCD will enable end users to utilize a standardized single suite of government-approved devices that deliver multiple capabilities (voice, video and computing). End users will be able to acquire and utilize these services through mobile devices in an efficient, consistent and reliable manner.
- Across FY19-22, the NCD will implement a hybrid or BYOD strategy for end users to utilize government and non-government computing devices that deliver multiple capabilities (voice, video and computing) as part of the DoD UC Framework, such as soft phone capability with removable microphone, video teleconference-like capability with enhanced image capture and devices with an interactive voice capability.
- By the end of FY22, 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, enterprise services and other mission areas for the entire Army. The integration of information transport mechanisms and consolidation and standardization of computing services enable the NSD to improve network management through the implementation of unified network operations tools and enhanced asset visibility. The consolidation and standardization of computing services, along with modernized information

transport infrastructure, also enhance enterprise services content delivery by enabling enterprise applications to be hosted in a centrally managed location and accessed from anywhere.

The NCD has strong dependencies with external stakeholders, such as 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 shared computing, distributed computing and server services capabilities. The following table describes the high-level dependencies among the NCD, AEN domains and key external stakeholders.

Initiatives	Alignment		Dependencies			
	LOE Objective	JCA	NCD Initiatives	ESD Initiatives	NSD Initiatives	External Stakeholders
Increase Network Throughput	3.1	6.1.1	MPLS, JRSS, Optical, Pathway, ICAN		Joint Management System, Cryptographic Modernization Initiative	DISA, NSA
Computing Storage and Infrastructure	3.2	6.2.2	JRSS, MPLS, COE, CP CE		JRSS	DISA (Cloud Access Point (CAP))
End-User Devices	3.3	6.2.2.4	Wireless	Standards, Apps and Services		DoD
Synchronize deployable and fixed networks' components to provide integrated access to network capabilities	3.4	6.1.1	Operational Capability Sets, HSMCC, MPLS, JRSS, Optical, Pathway, ICAN			DISA, WMA

Table 6: NCD Initiatives' Critical Dependencies

Summary

The NCD portfolio provides a resilient transport network and an optimized, responsive computing and storage capability while offering 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 FY18-22 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 Enterprise Services Domain (ESD) is a collection of IT investments that will deliver an integrated suite of globally available, adaptable solutions that supports the Army and connects it with unified action partners. 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 unified action partners by ensuring an integrated collaborative environment that supports all mission areas. The ESD comprises three major capability areas: information sharing, 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 the other AEN domains and the COE. These efforts will modernize the network, support the Integrated Training Environment, provide support for mobility and enable realization of the Installation as a Docking Station (IaDS) concept.

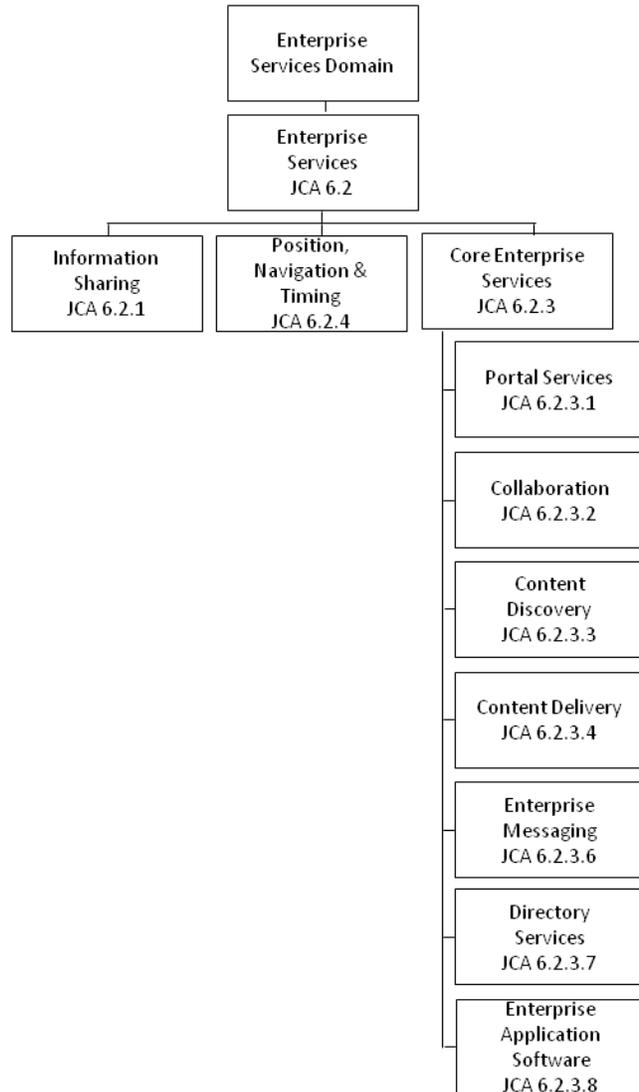


Figure 4: ESD Capability Taxonomy

Enterprise Services at the End of FY17

By the end of FY17, the ESD will be in a strong position to continue making advancements that will save the Army money and enhance the user experience. Many of the NCD and NSD goals accomplished in FY17 also will provide a strong foundation for enterprise services in the out years.

Enterprise services will allow the Army to retire the majority of Army Knowledge Online (AKO) and begin deployment of modernized capabilities by the end of FY16.

The ESD will start 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. At the end of FY16, the AESD will have the ability to use the enterprise ticketing system Army-wide. Additionally, the ESD will have created 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 resource information located on and global access to the network.

By the end of FY17, at least 13 Army and joint enterprise license agreements (ELAs), linked to requirements validated by the Army Enterprise Network Council (AENC) that support both the warfighter and business user, will be in place. ELAs produce cost avoidance, operational efficiencies and asset visibility, and improve maintenance coverage, security threat management and enterprise-level support. As ELAs are created, the Army will focus on discontinuing local purchases of software covered under established license agreements, resulting in additional cost avoidance/savings.

Overview of FY18-22 Capabilities

In FY18-22, Army users will have a single point of access to retrieve the enterprise information needed to complete their missions. The Army will begin the transition to Unified Capabilities as a service. 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. Per direction from the Office of Management and Budget and in coordination with the DoD CIO, the Army will have implemented a records management solution to enable all electronic content to be managed by FY19. The Army will also have solved foundational issues for adopting services from a commercial service provider. Services such as mail and other asynchronous collaboration capabilities will migrate to commercial providers.

An integrated/federated back end will enable more effective search and compliance. A single global directory will allow external applications and enterprise services to filter based on attributes such as name, role, location and organization. Army content delivery will use DoD specifications to discover, search and retrieve content, and will be aligned with DoD and IC initiatives and directives. Discovery tools will utilize attributes of each individual user to return targeted results that are likelier to address his or her needs.

The Army also will have a portfolio of ELAs that provides an Army-wide set of capabilities compatible with the JIE and IC-ITE. Individual commands will no longer purchase enterprise software independently but instead will utilize an application storefront to acquire from a portfolio of approved applications.

The Army Information Technology Service Management (ITSM) policy will be in place, continually increasing the effectiveness of, improving the security of and stimulating efficiency in Army IT services. ITSM will provide a standard approach to monitor, report and evaluate adherence to, built-in governance of and continual service improvement capabilities for every Army Enterprise Service Management Framework (AESMF) process. The architecture will cover the network end to end (institutional through tactical), and Unified Capabilities will be globally available.

Mandates Driving Network Capability Modernization

FY18-22 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 unified action partners 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 in, develop and deliver enterprise services.

Support the Army	DOTMLPF-P solutions 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.

Table 7: Guiding Principles to Enterprise Services

Capability Gaps and Priorities

The primary focus of network modernization is to increase the effectiveness, security and efficiency of the network,⁷ thereby improving the Army’s operational capabilities. 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, which affect the user experience. They are listed in priority order below.

Priority	Gap	Gap Description	Capability
1	Integrated enterprise services (UC, collaboration services, messaging)	Solutions are currently stove-piped 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 FY14.	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 discovery, directory services

Table 8: ESD Priority Capability Gaps

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

Capability Progression/JCA Alignment (FY18, FY19-22)

The table below shows the ESD capabilities that are targeted for modernization in FY18 and FY19-22.

Initiatives	Joint Capability Area 6 Communications and Computers								
	6.2 Enterprise Services								
	6.2.1 Information Sharing	6.2.3 Core Enterprise Services							6.2.4 Position, Navigation and Timing
		6.2.3.1 Portal Services	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	
FY18 Targeted Capability		•	•	•	•	•	•	•	
FY19-22 Targeted Capability		•	•	•	•	•	•	•	•

Table 9: ESD Capabilities Aligned to JCAs

Core Enterprise Services

In FY18-22, the primary goal of enterprise services is to ensure that information is available at the point of need. The value of enterprise services will be better understood by users and resource managers by providing an integrated, holistic IT service delivery framework, the AESMF. Many enterprise services will undergo formal assessments to ensure that they are delivering the expected value to Army users, meeting security standards and cost-efficient.

By providing a continuous, adaptive, device-agnostic user experience, enterprise services will enable users to work in changing environments. While mobile devices 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 FY18-19, 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 FY20-22, the focus will shift to simplifying and standardizing the user experience across core enterprise services, moving training resources onto the network and ensuring availability to the Army and unified actions partners 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. Users will receive ample information and training to ensure that these processes are well understood and user-friendly.

Portal Services

- In FY18, 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 must 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 FY19-22, a validated requirements definition, CONOPS and joint strategic plan will inform device availability. Efforts to field devices that 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. Users will reach joint information through an attribute-based access control (ABAC) point of entry, with an individual data set that is uniform across the participant population. Additionally, ABAC will govern the management and sharing of joint information sets to improve collaboration. SSO dependencies and requirements will be established and policy-based; certificate and password/pin regulations will be validated.
- By the end of FY22, users will have a single point of access to retrieve the enterprise information needed to complete their missions. Authorized users will no longer be required to seek information from multiple locations, simplifying information sharing and collaboration across the Army and with unified action partners.

Collaboration

- In FY18, 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 end-to-end testing of a single, standard, integrated solution for asynchronous and synchronous collaboration will continue.
- In FY19-22, the ESD will focus on implementing a joint, integrated, enterprise collaboration and enterprise messaging service, as well as a solution for assured communications. The Army also expects to approve a model for extending collaboration solutions to unified action partners.
- By the end of FY22, Army 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 FY18, data consumers in the tactical environment will be able to execute limited discovery queries, guided by industry and data interoperability standards that align to DoD and intelligence community (IC) initiatives and 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 content providers, as bandwidth allows. 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 FY19-22, 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. The Army will continue to emphasize compliance with standards in order to achieve interoperability, effectiveness and efficiency. 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 and 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. 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 FY22, content discovery will be provided to users through core enterprise services. Data analytics executed against common (or mediated) metadata will transform content discovery into information discovery. Discovery tools will utilize attributes of each individual user to return targeted results that are likelier to address his or her needs. Additionally, records of previous searches from across the Army will be used to provide criteria for suggested content and similar search terms.

Content Delivery

- In FY18, data consumers in the tactical community will be able to access content in a more responsive manner based on a publish-and-subscribe model that exploits DISA's Global Content Delivery Service (GCDS) for larger files and for disconnected, intermittent and low-bandwidth (DIL) conditions. GCDS's forward staging will also make content delivery via websites, web-based applications and video streaming more responsive.
- In FY19-22, content delivery will expand to geospatial foundational content so that the data consumer is no longer dependent on network bandwidth for that information. 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 while

untethered from 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 enterprise hosting facilities. 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 FY22, 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 FY18, planning for an integrated enterprise service that delivers both collaboration and messaging will continue. Simultaneously, services will continue to be brought online to provide a centralized service desk.
- In FY19-22, 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 that centralized service desk. 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 FY22, enterprise messaging will be part of an integrated and collaborative solution, eliminating some of the Army's disparate initiatives. The Army also will improve customer support, to include bringing additional services to the enterprise service desk.

Directory Services

- In FY18, the Army will continue to identify and integrate attributes for directory-services filtering and to synchronize directories to achieve a standard Army directory.
- In FY19-22, the Army will have an authoritative directory service that provides enhanced attribute filtering. It will reduce the need for local directory service solutions at installations, leading to lower directory maintenance costs across the Army. In order for directory services to realize their full potential and operational efficiency by 2021, the Army must implement and enforce a policy that ensures personnel (i.e., military, civilians and contractors) are providing accurate and reliable data to authoritative data sources (Army Human Resources Command and the Defense Manpower Data Center) on a regular basis.
- By the end of FY22, 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 FY18, 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 evolving JIE and IC-ITE parameters, and will be consolidated and centrally managed. (Current ELAs and their details are available at <https://chess.army.mil/>.)
- In FY19-22, the enterprise application software capability will be improved by implementing an application storefront and additional ELAs and joint ELAs.
- By the end of FY22, the Army will have an enterprise portfolio of ELAs that provides a standard set of capabilities Army-wide 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. Individual users will have the ability to choose from a portfolio of approved applications for a variety of platforms. The storefront will manage 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

In the mid term, Army systems will continue to have a critical dependency on PNT information. Assured PNT is an Army-led and DoD-supported effort to provide PNT data to the warfighter in a contested/denied environment. The Army's assured PNT approach consists of a set of products that provide a cumulative effect to enable the assured PNT capability. The objective over the mid-term period is to begin M-code transition in FY18 and to deliver the assured PNT system-of-systems capability to Army forces at the brigade and lower levels beginning in FY20.

Dependencies

Many of the enterprise services that fall into the ESD have direct dependencies on the capabilities being provided by the NCD and the NSD. While enterprise services rely on the infrastructure and security that the other domains are working to develop, many services within this domain also serve as drivers for NCD and NSD activities. The chart below describes the high-level dependencies among the ESD, the other domains and external stakeholders.

Initiatives	Alignment		Dependencies			
	LOE Objective	JCA	NCD Initiatives	ESD Initiatives	NSD Initiatives	External Stakeholders
Network Modernization; JRSS	2, 3	6.1.3.2 / 6.3.1	MPLS, Installation Information Infrastructure Modernization Program, Installation Information Infrastructure – Communications and Capabilities.		JRSS	DISA
Computer Network Defense Service Provider / Certification Authority	2	6.1.2.1			JRSS	ARCYBER and Second Army, DISA
Directory Services	2	6.1.3.1			IdAM	DISA
Cloud Access Point	2	6.1.3.2			JRSS	DISA, ARCYBER, Second Army and NETCOM

Table 10: ESD Initiatives’ Critical Dependencies

Summary

Enterprise services provide adaptable solutions that support global, seamless collaboration for the Army and unified action partners. The Army will focus on the seven core enterprise service areas during FY18-22 while developing and maintaining a consistent user experience to bridge the gap between near-term activities and the desired 2022 capabilities.

Appendix 3 – Network Operations and Security Domain

Domain Overview

In order to accomplish mission requirements in an ever-growing and changing threat environment, the Army must be able to operate and defend mission-critical systems and

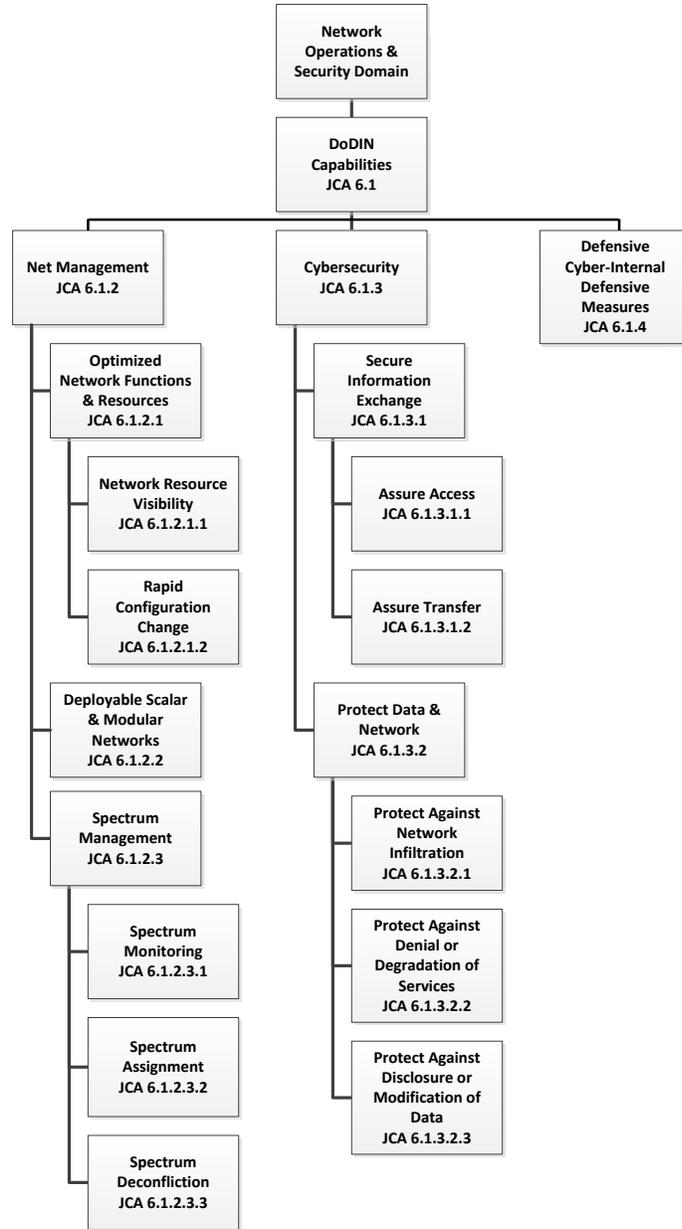


Figure 5: NSD Capability Taxonomy

capabilities and 10 Tier 5 capabilities, as depicted in Figure 5. In an effort to align with the JIE and the other Services, the NSD has updated capabilities to follow the JCA Framework.

ensure the continuity of network functions. The Network Operations and Security Domain (NSD) is responsible for ensuring that cybersecurity is addressed and visible in all capability portfolios, IT life-cycle management processes and investment programs that incorporate IT, in accordance with DoD Instruction 8500.01 (Cybersecurity). The NSD will ensure that organizational cybersecurity objectives developed via the Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group process are implemented when possible.

The Army will conduct network defense measures that are directed, integrated and synchronized in accordance with the DoD Unified Command Plan. Cyberspace operations, enabled by cyber and cryptologic intelligence, shall inform the operation, maintenance and security of the network, as well as shape acquisition efforts and the design of a defensible architecture. Army cybersecurity efforts will be closely nested with the DoD Cyber Mission Force, enabling the Army to more effectively counter traditional threats and address increasingly sophisticated threats, including the insider threat and the advanced persistent threat (APT).

The NSD is composed of three JCA Tier 3 capabilities, five JCA Tier 4

Network Operations and Security at the End of FY17

By the end of FY17, the NSD will have enhanced network operations, management and defense capabilities, as well as updated policies to ensure that all organizations understand, implement and execute cybersecurity best business practices. The Army will achieve full implementation of the JRSS architecture, which replaces individual Top-Level Architecture security stacks, in the Continental United States, Southwest Asia and Europe, 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. Enhanced encryption capabilities will support over-the-network keying (OTNK) and secure data transmission. Government-furnished mobile communication devices will be used to access classified knowledge centers and websites, and securely share information. The Army will have enabled the 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 FY18-22 Capabilities

In the FY18-22 timeframe, the NSD will focus on capabilities that shape the security environment, mitigate cybersecurity deficiencies and address operational gaps to provide a secure, seamless and continuous network environment with protected critical data and information for the Army and unified action partners. The network must be dynamic, assured and managed to offer robust capabilities that improve the Army’s ability to protect information and systems, detect and respond immediately to threats and incursions, and restore any lost capability. 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 will have transitioned to a fully operational Key Management Infrastructure capability that provides an automated secure service to account for and distribute cryptographic products and services in a net-centric environment utilizing an OTNK capability. 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 FY18-22 timeframe.

<p>Identity and Access Management</p>	<ul style="list-style-type: none"> • 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, 23 Jan 13, subject: Mandating the Use of Enterprise Directory Services (EDS).
<p>Cryptographic Modernization</p>	<ul style="list-style-type: none"> • Chairman of the Joint Chiefs of Staff (CJCS) Notice 6510.02D. • CJCS Instruction 6510. • Capability Development Document (CDD), Cryptographic Equipment & Services, JROC Jul 10. • Communications Security (COMSEC) requirements identified in USC Title 40.

Key Management	<ul style="list-style-type: none"> • NSA, Electronic Key Management System (EKMS) Notice #242, subject: EKMS Tier 2 End of Life, Feb 12. • CDD ver. 1.02, 15 Aug 06. <ul style="list-style-type: none"> • Headquarters, Department of the Army EXORD, G-3/5/7 LandWarNet/Mission Command Capability Set FY13 Fielding Execution, 27 Jun 12.
Mobility	<ul style="list-style-type: none"> • DoD/national guidance, Mobility Capability Package, 30 Jul 12. • CJCS Notice 6510.2D.
Information Security Continuous Monitoring (ISCM)	<ul style="list-style-type: none"> • 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.
Enterprise Service Management System	<ul style="list-style-type: none"> • DoD CIO memo, 15 May 11, subject: Information Technology Service Management in the Department of Defense. • Chief Information Officer/G-6 memo, 17 Nov 14, subject: Army Information Technology Service Management (ITSM) Policy.
Standardization of Network Operations across the Network	<ul style="list-style-type: none"> • FM 6.02-71 Network Operations, 14 Jul 09. • Joint CONOPS for GIG Network Operations, 4 Aug 06. • CIO/G-6 memo, 12 Nov 09, subject: Army Information Condition 3 Status.
Increase Agility of Spectrum Management Operations	<ul style="list-style-type: none"> • DoD CIO Electromagnetic Spectrum Strategy, Nov 13. • CJCSI 3320.01 Electromagnetic Spectrum Use in Joint Operations, Feb 11. • AR 5-12, Army Use of the Electromagnetic Spectrum, Jun 15. • Joint CONOPS for Electromagnetic Spectrum Operations, Mar 15.

Table 11: Major Legislative and DoD Mandates Driving Network Operations and Security

Capability Gaps and Priorities

The NSD has identified 15 associated gaps binned to five of the seven JCA Tier 3 capabilities. The prioritized gaps are:

Initiatives	Priority	Gap	Gap Description	JCA Capability
Identity and Access Management (IdAM)	1	Identity and Access Management (IdAM)	The Army's Active Directories are not currently populated with user data from the DoD Enterprise Directory Service (EDS).	Secure Information Exchange
Joint Regional Security Stacks (JRSS)	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
Joint Management System (JMS)	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 operating, assuring and defending the network.	Defensive Cyber - Internal Defense Measures

UNCLASSIFIED

Initiatives	Priority	Gap	Gap Description	JCA Capability
Cryptographic Modernization Initiative (CMI)	4	Cryptographic Modernization	Legacy cryptographic capabilities are unable to meet the KMI-aware functionality or to support the Army's requirement to increase bandwidth for secure communications across the Army Enterprise Network to the tactical edge.	Secure Information Exchange
Key Management Infrastructure (KMI)	5	Key Management (COMSEC)	Inability to provide an automated enterprise service to account for and distribute cryptographic products to enable over-the-network keying in a net-centric environment.	Secure Information Exchange
Mobility	6	Secure Mobility	Army legacy wireless technologies are unable to secure mobile handhelds to support enterprise tactical applications.	Secure Information Exchange
Enterprise Service Management System (ESMS)	7	Single, Interoperable IT Service Management (ITSM) System	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
Increase Agility of Spectrum Management Operations	8	Near-Real-Time Spectrum Management	Electromagnetic spectrum (EMS) continues to become congested and contested. Deployed tactical forces may not have full control over the EMS in a particular operating environment due to congestion and/or adversarial use or denial. The ability to manage the spectrum effectively in near-real time and to mitigate interference is critical to maintaining operational effectiveness.	Spectrum Management
Standardization of Network Operations across the network (i.e., converging tools, IES, CONOPS, metadata)	9	Standardize and Simplify Network Operations	The Army currently has multiple redundant and costly tools; some have associated enterprise license agreements and others do not. The Army needs to determine the best way to: integrate existing tools (tactical and enterprise); identify redundant tools for possible elimination; and prioritize bridging capabilities between the tactical and enterprise environments for end-to-end network operations.	Optimized Network Functions and Resources
Enhance Cyber Situational Awareness by Leveraging Big Data/Cyber Analytics	10	Automated Sensing, Reporting & Response	Current network sensors and reporting technologies are manual and not as flexible or portable as the Army needs.	Defensive Cyber – Internal Defense Measures
Enhance Cyber Situational Awareness by Leveraging Big Data/Cyber Analytics	11	Forensic & Threat Analysis Technologies	The Army lacks the capability to remotely and rapidly capture, analyze and exploit forensic evidence, and deploy countermeasures on cyber assets.	Defensive Cyber – Internal Defense Measures

Initiatives	Priority	Gap	Gap Description	JCA Capability
Enhance Cyber Situational Awareness by Leveraging Big Data/Cyber Analytics	12	Intrusion Detection, Response & Recovery Technologies	The Army lacks intrusion detection, response and recovery technologies designed to operate within low-bandwidth tactical environments.	Defensive Cyber – Internal Defense Measures
Information Security Continuous Monitoring (ISCM)	13	Risk Management Approach to Network Security	The Army lacks the ability to integrate current applications and tools that use data standards to provide near-real-time risk visualization, automated configuration management analysis and continuous monitoring capabilities to enable network defense and provide risk awareness.	Protect Data and Network
Army Insider Threat Program	14	Risk Management Approach to Network Security	The Army lacks the ability to identify and mitigate the risk that insider threats pose to the network.	Protect Data and Network
Refining the Cyber Workforce	15	Training Requirements & Work Roles	The Army lacks institutionalized training to acquire and maintain civilian competencies that meet the Joint Cyberspace Training and Certification Standards.	Protect Data and Networks

Table 12: NSD Prioritized Capabilities Gaps

Capability Progression/JCA Alignment (FY18, FY19-22)

The table below shows the NSD capabilities that are targeted for modernization in FY18 and FY19-22.

Initiatives	Joint Capability Area 6 Communications and Computers												
	6.1 DoDIN Capabilities												
	6.1.2 Net Management						6.1.3 Cybersecurity						6.1.4 Defensive Cyber – Internal Defensive Measures
	6.1.2.1 Optimized Network Functions and Resources		6.1.2.2 Deployable Scalable and Modular Networks		6.1.2.3 Spectrum Management		6.1.3.1 Secure Information Exchange		6.1.3.2 Protect Data and Networks				
	6.1.2.1.1 Network Resource Visibility	6.1.2.1.2 Rapid Configuration Change		6.1.2.3.1 Spectrum Monitoring	6.1.2.3.2 Spectrum Assignment	6.1.2.3.3 Spectrum Deconfliction	6.1.3.1.1 Assure Access	6.1.3.1.2 Assure Transfer	6.1.3.2.1 Protect Against Network Infiltration	6.1.3.2.2 Protect Against Denial or Degradation of Services	6.1.3.2.3 Protect Against Disclosure or Modification of Data		
FY18 Targeted Capabilities	•	•	TBD	•	•	•	•	•	•	•	•	•	
FY19-22 Targeted Capabilities	•	•	TBD	•	•	•	•	•	•	•	•	•	

Table 13: NSD Capabilities Aligned to JCAs

Net Management

Network operations is a component of Signal support to warfighters and includes the business operations that establish, operate, manage, protect and defend the network. Network operations enables authorized users to effectively execute their mission by leveraging the following capabilities: optimized network functions and resources; deployable, scalable and modular networks; and spectrum management. Network operations covers enterprise management, net assurance and content management, and 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

Standardization of Network Operations across the Network

In FY18, the Army will continue to optimize network functions and resources through the standardization of network operations. Standardization will extend end to end (institutional through operational) and include the convergence of network operations tools, which will reduce the number of tools and applications residing on the network and allow for more commonality within maintenance, sustainment and training. Additionally, the extension of enterprise-level services to the tactical edge will create efficiencies and result in major cost and time savings. The Unified Trouble-Ticketing System will serve as a model for the extension of enterprise services to the tactical edge. Network operations will be influenced by unique and complex tools that are deployed at multiple echelons. As tools are consolidated, hosted and maintained at the enterprise level, network management processes will be streamlined.

In FY18, standardization of network operations will include:

- Implementation and adherence to the Network Operations CONOPS.
- Implementation of a configuration control process for tools and application that reside on the network.
- Utilization of a Unified Trouble-Ticketing System for the tactical and enterprise domains.
- An on-going Army-wide effort, led by CIO/G-6, to reduce the number of network tools and applications.
- Adoption of information exchange specifications and metadata that mandate standards according to which Army systems and network appliances must operate, creating more effective, useful and timely performance and management data.

In FY19-22, network operations must transform along with the DoDIN to support new warfighting, intelligence and business processes and emerging capabilities. Network operations should enable users to access and share trusted information in a timely manner with advanced technologies.

By the end of FY22, the Army will have situational awareness dashboards configured for installations, Regional Cyber Centers, the Army Cyber Operations Integration Center, Army Cyber Command, Second Army, functional commands and other designated commands. Future network operations must continue to provide commanders the ability to effectively control, manage, defend and operate in and through the cyberspace domain.

Army Enterprise Service Management (ESM)

In FY18 and beyond, all ESM activities are contingent upon the final decision regarding procurement of an Enterprise Service Management System as a Service (ESMSaaS) capability. The CIO/G-6 will decide either to federate the remaining organizational ITSM systems with the Remedy 8.1 upgrade or to operate as is until ESMSaaS migration. The ESMSaaS migration plan will be synchronized with operation and maintenance spending plans to recapture funds that would be allocated to maintenance and equipment refresh in FY18-20.

In FY18, ESMSaaS activities include the integration, development and accreditation of the following: Enterprise System Center, Host-Based Security System, ArcSight, Assured

Compliance Assessment Solution (ACAS) and IT Client Manager Application. Initiation of contract activities will also begin in FY18.

In FY19, ESMSaaS activities include integration of the Joint Management System and the Single Interface to the Field (SIF), which will enable unified tactical trouble-ticketing between strategic and tactical environments. The Army will continue to synchronize the requirements and capabilities associated with data center consolidation and standardization efforts. The Army also will commence regional migration to ESMSaaS, delivering services through a commercial cloud service provider or as a service from an Army data center.

In FY20 and beyond, 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, with full integration of tactical and joint ITSM services and platforms. All legacy ITSM instantiations and trouble-ticketing systems will be off the network and retired, or in the process. IT Infrastructure Library 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. Enterprise management dashboards for network operations, computer network defense ticketing, enterprise analytics and trending will be centralized for the SIPRNet and NIPRNet. Combined, these attributes will help the CIO/G-6 to determine the total cost of ownership of Army network IT.

Deployable Scalable and Modular Networks

As part of extending network operations enterprise services, in FY18-22 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

Increase Agility of Spectrum Management Operations

In FY18, the Army intends to complete the transition to the DoD electromagnetic spectrum standard data format to enable machine-to-machine data exchange to support the Common Operating Environment. The Army will implement the Electronic Warfare Planning & Management Tool (EWPMT) by incorporating comprehensive electromagnetic spectrum operations comprised of electronic warfare and spectrum management operations (SMO) capabilities. SMO functions enable frequency assignment, deconfliction and scheduling. Combined, these capabilities support planning, management and execution of operations within the electromagnetic operational environment during all phases of military operations, and give commanders the ability to shape the electromagnetic operating environment to their advantage.

In FY19-22, the Army will continue implementation of EWPMT by updating electronic warfare operations and spectrum management operations capabilities. Emerging requirements for this period include cyber situational awareness, offensive cyberspace operations planning and Pseudolite planning and management. The Army also will implement capabilities to monitor the electromagnetic spectrum to identify and mitigate electromagnetic interference with the network

and other spectrum-dependent systems. EWPMT will sense congestion and dynamically deconflict and re-assign frequencies according to set parameters.

By the end of FY22, spectrum management operations will provide commanders and staff the tools they need to more effectively and efficiently plan, coordinate and use spectrum throughout the mission. Army electromagnetic spectrum data will be validated and transitioned to the DoD XML standard for access and exchange. In addition, spectrum management tools and spectrum assignment and deconfliction capabilities will be integrated into the Command Post Computing Environment. The Army will be able to monitor spectrum, identify and mitigate electromagnetic interference, and dynamically reassign spectrum when congested.

Cybersecurity

Secure Information and Exchange

Identity and Access Management (IdAM)

In FY18, the Army will complete the transition of AKO SSO applications to a common authentication service. The Army intends to implement on-demand selection of identities and privileges to manage user entitlements to enterprise network resources, as well as a protected service for privileged identity credentials. Efforts to institute role-based access control and to audit privileged-user sessions will continue. Strong authentication and single sign-on will allow the Army to achieve fine-grained control over distributed computing capabilities.

During the FY19-22 timeframe, the Army will further enhance IdAM capabilities to provide a family of security services that supports distributed computing through higher security assurance with agility and adaptability. The IdAM enterprise framework will enable robust insider threat awareness through identification of anomalies and potential security risks, and analysis of how data are being utilized based on user context and behavior. The Army will be able to evaluate associations, trends and patterns in user-access privileges that may violate guidelines or present security risks. IdAM also will allow for the automatic discovery of resources as they are created in a hybrid environment and automatic application of policy to maintain control. Using the framework, the Army will assess biometric technologies, as well, based on funding availability.

By the end of FY22, the IdAM framework will allow identification and accounting of all user activity on enterprise network resources. Enterprise services will enable information systems and resources to be accessible across different organization and security boundaries. The enhanced IdAM framework will permit network operations tools to associate user identities with trends, and to detect patterns in privileged accounts that may violate guidelines or present security risks.

Common Access Card/Public Key Infrastructure (CAC/PKI)

During the FY18-22 timeframe, the Army will enhance PKI capabilities to provide a more secure network and greater agility and adaptability for the enterprise. The global CAC program, which covers more than one million users, will continue via DEERS RAPIDS. The Army will maintain round-the-clock support for approximately a quarter-million NIPRNet Alternate Smart Card Logon and SIPRNet users to ensure data integrity, non-repudiation and confidentiality of information, and to uniquely identify each user in accordance with DoD mandates. Development of a medium-assurance solution on the SIPRNet for non-person entities, such as computers,

applications and devices, will proceed in coordination with the DoD PKI Project Management Office. The Army also will develop and implement NIPRNet and SIPRNet PKI capabilities for mobile, tactical and training devices that currently do not support CAC or SIPRNet tokens. Testing and analysis of PKI capabilities will be included in Network Integration Evaluations in order to assess operational capabilities, trends, patterns and potential security risks.

By the end of FY22, PKI will be established in end-to-end environments, ensuring data integrity, non-repudiation and confidentiality for individual users, organizations and groups. The Army will continue to provide 24x7 PKI support to enable secure communication with mission partners, as well as the identification, authentication, authorization and accounting of all user transactions on enterprise resources.

Cryptographic Modernization Initiative (CMI)

In FY18-22, CMI will continue to evaluate and implement innovative technologies to support more stringent security, greater network capacity, and improved network performance and interoperability. The ultimate objective is to enable secure information sharing across the total force and with unified action partners.

The Army must continually enhance and modernize cryptographic capabilities to keep pace with the rapid changes in cyber warfare and network vulnerabilities. The Army will define new standards for and invest in advanced cryptographic capabilities and next-generation cryptographic technologies to protect NSS and NSI from emerging threats, securing the network as enterprise services are extended to the tactical edge. In addition, the Army will pursue application of future upgrades to cryptographic systems via programmable equipment that allows new features and algorithms to be easily uploaded. Wireless and mobile solutions to mission command requirements will be used to increase the real-time dissemination of information via voice, data, secure video teleconference and access to knowledge centers at various security levels (unclassified to TS/SCI).

In order to field modern technology, the Army must eliminate capabilities that are no longer logistically supportable, sustainable or maintainable. This makes the replacement of legacy cryptographic equipment and software a high priority.

In FY22 and beyond, the Army will continue the CMI multiyear effort with the introduction of new algorithms designed to enhance interoperability and information sharing across the Services and with coalition allies.

Key Management Infrastructure (KMI)

In FY18-22, the Army will complete the transition of Electronic Key Management System (EKMS) Tier 2 accounts to KMI, based on unit mission requirements, available technology and the Sustainment Readiness Model (formerly known as Army Force Generation). The NSA and the Services (with direct input from the DoD CIO) will establish the KMI Capability Increment 3 capabilities development document, which will set the framework to incorporate EKMS core operations (key generation, distribution and tracking) into the infrastructure. This capability will also modernize operational key management services for sharing of service/agency COMSEC database device registration information, and provide more support to NATO, allied and coalition partners, resulting in improved identification, authentication and global access for

warfighters. Most importantly, this capability will further reduce warfighter exposure to risks associated with manual distribution of cryptographic keys.

Mobility

In FY18, 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 anytime, 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 FY19-22, the Army will complete ICAN upgrades to enable wireless connectivity for government-furnished equipment operating within installation boundaries.

By the end of FY22, the Army plans 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 device 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 resources.

Protect Data and Networks

Single Security Architecture (SSA) Management

During FY18-22, Joint Management System (JMS) 2.0 capabilities will include the Enterprise Operations Center (EOC) and provide a logical path toward the JIE single security architecture (SSA). JRSS/JMS 2.0 capabilities will support perimeter protection of Core Data Centers, IPNs and installations. In addition, the JIE EOC will evolve to manage the network and the JRSS portion of the SSA, which will provide border protection capabilities for the SSA.

By the end of FY22, JRSS/JMS 2.0 will add the capabilities necessary for the Navy and Marine Corps 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 Security Continuous Monitoring (ISCM)

During FY18-22, the Army will implement Phase 3, Block 3, which will provide the capability to manage information and software assurance by measuring the trustworthiness of software processes and products. At the end of Phase 3, the Army will be able, through ISCM, to maintain situational awareness of all systems across the network; gain an understanding of threats and threat activities; access all system security controls; and collect and analyze security-related information.

Army Insider Threat Program (InT)

In FY18-22, Army will continue to enhance InT capabilities for early identification of current and emerging insider threats that pose the greatest risks to national security, and will enable investigative and Command authorities to reduce the unauthorized disclosure of information and/or loss of information, personnel, assets and equities. The Army Insider Threat Program’s

focus will be on the following lines of effort in order to address the greatest threats to national security.

- Expand employment of Army classified network user activity monitoring (UAM) and analysis. Also, determine whether UAM is needed on select NIPRNet assets.
- Improve and refine security processes, systems and information-sharing procedures for counterintelligence, personnel security, law enforcement and information assurance information indicative of an insider threat.
- Integrate existing capabilities to better detect, analyze and respond to activity and information indicative of an insider threat.

To properly contend with the complexity of insider threats and the constrained resource environment facing the Army, the Insider Threat Program will employ a deliberate, risk-based, multi-phased approach to manage resources and close the critical detection gaps within information systems and information-sharing processes.

Refining the Cyber Workforce

In FY18-22, the Army will continue to assess the framework for identifying, shaping and tracking the civilian cyberspace workforce and aligning it with the military structure of Career Field 17, ensuring that personnel are matched in accordance with the Army's needs and requirements. If any adjustments are necessary, based on roles and responsibilities, then a further deep dive will take place to address the noted concerns.

Defensive Cyber – Internal Defense Measures

Big Data/Cyber Analytics

In FY18, the Army will enhance cyber situational awareness by leveraging Big Data technology and behavioral analytics to address gaps in automated sensing, response, reporting, forensic and threat analysis, intrusion detection and recovery technologies. The Army will provide storage capacity and analytic tools to aggregate and correlate threat-indicator data. This capability will provide cyber defenders near-real-time risk threat detection, thus decreasing the time required to respond and mitigate. Armed with enhanced situational awareness, and an accurate and timely picture of the friendly and enemy environments, the Army will invest in a platform of computing resources from which defensive cyberspace operations forces can draw to maneuver to a threat or target of interest, and deliver tools or payloads to achieve desired effects.

In FY19-22, the Army will invest in these critical capability areas (in accordance with priorities) 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/cyber analytics platform. The Army will complete the deployment to cyber operators of Big Data production systems on all tiers, including but not limited to all JRSS/JMS sites, all classifications with cross-domains solutions and other key terrains as appropriate. These are critical years in which to build upon foundational defensive cyber operations capabilities, rooted in situational awareness.

By the end of FY22, the Army's defensive cyber forces will have unprecedented access to advanced data analytics and substantially enhanced situational awareness of friendly and enemy units. 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, performed in accordance with AESMF to provide IT service delivery, 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 the NCD for the foundational elements that enable Network Operations and Security tools and processes to work. The following table describes the high-level dependencies among the NSD, AEN domains and key external stakeholders.

Initiatives	Alignment		Dependencies			
	LOE Objective	JCA	NCD Initiatives	ESD Initiatives	NSD Initiatives	External Stakeholders
IdAM	2.2	6.1.3.1				DoD (Enterprise Directory Services); DMDC (Identity Web Services)
JRSS	2.2	6.1.3.2	MPLS			DISA (installation, operation and maintenance)
JMS	5.3	6.1.4	MPLS, JRSS			DISA (installation, operation and maintenance)
CMI	2.2	6.1.3.1				NSA, ASA(ALT), DoD, G-3, G-4, G-8, TRADOC (NetMod planning & implementation)
KMI	2.2	6.1.3.1				NSA, ASA(ALT), DoD, G-3, G-4, G-8, TRADOC (NetMod planning & implementation)
Mobility	2.1	6.1.3.1	Wireless Infrastructure	Standards, Apps & Services		DISA (DoD Mobile Unclassified and Classified Capability Service Pilots)
ESMS	5.3	6.1.2.1				PEO EIS (analysis of alternatives)
SMO	5.2	6.1.2.3				DISA (Spectrum Data Repository & SXXIO deployed) ASA(ALT) (Command Post Computing Environment)
SNO	5.5	6.1.2.1				PEO C3T & PEO EIS (Integrated Product Team)
Cyber Analytics	2.3	6.1.4				ARCYBER/ARL/DISA Pilot
ISCM	2.2	6.1.3.2				DoD/DISA (ISCM policy/capability releases)
Cyber Workforce	2.1	6.1.3.2				OSD & OPM (policy development and implementation)

Table 14: NSD Initiatives' Critical Dependencies

Summary

The NSD capabilities provided in the FY18-22 timeframe, coupled with the requisite personnel, tactics, techniques and procedures, will establish the framework to secure the network and protect critical data and information for Army and unified action partner missions. The overall benefits to be realized by the Army are:

UNCLASSIFIED

- Networks and information that are accessible, interoperable and protected against threats.
- Improved secure network capabilities for authorized users to effectively and efficiently execute missions.
- The elimination of standalone access-control mechanisms, which were often insecure and inefficient, for applications, systems and networks.
- Improved network performance and interoperability that enable secure information sharing across the Army and unified action partners.
- Enhanced mission planning and operations through a web-based, net-centric key management infrastructure that significantly decreases the manual distribution of cryptographic keys.
- 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 – Glossary

TERM	DEFINITION
Assure Access	The ability to identify and authenticate individuals, groups and entities, and provide authorization to services and information. (JCA 6.1.3.1.1)
Assure Transfer	The ability to exchange authentic data, information and knowledge among authorized individuals, groups and entities. (JCA 6.1.3.1.2)
Beyond Line of Sight	The ability to exchange data or information via electromagnetic spectrum beyond line of sight. (JCA 6.1.1.2.2)
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)
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)
Communication Bridge	The ability to interface two or more common communications media or networks. (JCA 6.1.1.3.1)
Communication Gateway	The ability to interface two or more disparate communications media or networks. (JCA 6.1.1.3.2)
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)
Content Discovery	The ability to identify searches for, or locate, relevant information. (JCA 6.2.3.3)
Core Enterprise Services	The ability to provide awareness of, access to and delivery of information on the DoDIN via a small set of CIO-mandated services. (JCA 6.2.3)
Cybersecurity	The ability to provide the measures that protect, defend and restore information and information systems. (JCA 6.1.3)
Data Center / Cloud / Generating Force (DC/C/GF)	Provides IT service capabilities in four environments that, within a security classification level, are able to share the same data center and non-server infrastructure. The environments are: 1) Cloud environment, which shares hardware resources through contemporary virtualization technologies, and automates provisioning and management of resources using modern cloud technologies. 2) ERP enclave environment, which contains ERP technologies that use virtualized and dedicated servers. 3) Legacy environment, which contains dedicated, system-specific physical servers that should not be virtualized, though legacy applications may share the network and potentially network-attached storage. 4) Development and test environment, which provides cloud-based development and test services and can lower costs by giving capabilities to authorized developers on demand and facilitating early integration testing.
Defensive Cyber - Internal Defensive Measures	The ability to dynamically reestablish, re-secure, reroute, reconstitute and/or isolate degraded or compromised local networks, ensuring sufficient cyberspace access for joint forces. (JCA 6.1.4)
Deployable Scalable and Modular Networks	The ability to design, assemble, transport and establish mission-scaled networks from adaptable component network modules. (JCA 6.1.2.2)
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)
Distributed Computing	A virtual computing capability for end users and applications achieved through the federation of distributed, location-independent computing resources. (JCA 6.2.2.2)
End-User Services	The ability to provide client computing devices that enable access to information, applications and services, and the management of those devices. This includes mobile voice, data and video devices (pagers, cell phones, wireless/cellular-enabled personal data assistants), and other end-user devices used by individuals. (JCA 6.2.2.4)

UNCLASSIFIED

TERM	DEFINITION
Enterprise Application Software	The ability to provide productivity enhancement software to all users. (JCA 6.2.3.8)
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)
Information Sharing	The ability to provide physical and virtual access to hosted information and data centers across the enterprise and with mission partners, based on established data standards. (JCA 6.2.1)
Information Transport	The ability to transport information and services via assured end-to-end connectivity across the net-centric environment. (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, installation, headquarters or federal building). (JCA 6.1.1.1.1)
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 locations (e.g., command post, installations or federal buildings). (JCA 6.1.1.1.2)
Line of Sight	The ability to exchange data or information via electromagnetic spectrum within line of sight. (JCA 6.1.1.2.1)
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 6.1.2)
Network Resource Visibility	The ability to determine the real-time status and effectiveness of network services and resources. (JCA 6.1.2.1.1)
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 6.1.2.1)
Position, Navigation and Timing (PNT)	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)
Portal Services	The ability to access enterprise data and services through a single entry point. (JCA 6.2.3.1)
Protect Against Network Infiltration	The prevention of unauthorized access. (JCA 6.1.3.2.1)
Protect Against Denial or Degradation of Services	Preventing and/or containing activities that may degrade or deny authorized use of network resources. (JCA 6.1.3.2.2)
Protect Against Disclosure or Modification of Data	Preventing and/or containing activities that may expose or modify data. (JCA 6.1.3.2.3)
Protect Data and Networks	Anticipating and preventing successful attacks on data and networks. (JCA 6.1.3.2)
Rapid Configuration Change	The ability to rapidly configure and reconfigure enterprise services and resources in concert with the established CONOPS. (JCA 6.1.2.1.2)
Secure Information Exchange	The ability to secure dynamic information flow within and across domains. (JCA 6.1.3.1)
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)
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)
Software Marketplace	The marketplace will deliver web-based and downloadable applications to all devices approved for use within the Army's Common Operating Environment.

UNCLASSIFIED

TERM	DEFINITION
Spectrum Assignment	The ability to identify spectrum requirements, evaluate electromagnetic environmental effects, and dynamically plan, allot and modify frequency assignments to exploit available spectrum. (JCA 6.1.2.3.2)
Spectrum Deconfliction	The ability to dynamically predict, detect and mitigate frequency interference. (JCA 6.1.2.3.3)
Spectrum Management	The ability to synchronize, coordinate and manage all elements of the electromagnetic spectrum through engineering and administrative tools and procedures. (JCA 6.1.2.3)
Spectrum Monitoring	The ability to monitor and characterize the electromagnetic environment. (JCA 6.1.2.3.1)
Switching and Routing	The ability to move data and information end to end across multiple transmission media. (JCA 6.1.1.3)
Wired Transmission	The ability to transfer data or information with an electrical/optical conductor. (JCA 6.1.1.1)
Wireless Transmission	The ability to transfer data or information without an electrical/optical conductor. (JCA 6.1.1.2)

Appendix 5 – Acronyms

ACRONYM	DEFINITION
AAMBO	Army Application Migration Business Office
ABAC	Attribute-Based Access Control
ADCCP	Army Data Center Consolidation Program
ADMP	Army Data Management Program
AEN	Army Enterprise Network
AESD	Army Enterprise Service Desk
AKO	Army Knowledge Online
APCE	Army Private Cloud Enterprise
APT	Advanced Persistent Threat
ANCP	Army Network Campaign Plan
AESM	Army Enterprise Service Management
AESMF	Army Enterprise Service Management Framework
AONS	Architecture, Networks, Operations and Space
ASM	Army Software Marketplace
BCT	Brigade Combat Team
BMA	Business Mission Area
B/P/C/S	Bases/Posts/Camps/Stations
BYOD	Bring Your Own Device
CAP	Cloud Access Point
CDC	Core Data Center
CDD	Capability Development Document
CDS	Cross-Domain Solution
CIO	Chief Information Officer
CMI	Cryptographic Modernization Initiative
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COCO	Contractor-Owned, Contractor-Operated
COTS	Commercial Off the Shelf
CP CE	Command Post Computing Environment
DCO	Defensive Cyber Operations
DEE	Defense Enterprise Email
DIMA	Defense Intelligence Mission Area
DIL	Disconnected, Intermittent And Low-Bandwidth
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
ELA	Enterprise License Agreement
EOC	Enterprise Operations Center
ESD	Enterprise Services Domain
ESMSaaS	Enterprise Service Management System as a Service
EUD	End-User Device
EWPMT	Electronic Warfare Planning & Management Tool
EXORD	Execute Order
FY	Fiscal Year
Gbps	Gigabits per Second

UNCLASSIFIED

ACRONYM	DEFINITION
GCDS	Global Content Delivery Service
HSMCC	Home-Station Mission Command Center
IaaS	Installation as a Docking Station
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
L/V/C/G	Live/Virtual/Constructive/Gaming
LOE	Line of Effort
LTE	Long-Term Evolution
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
POM	Program Objective Memorandum
SATCOM	Satellite Communications
SIF	Single Interface to the Field
SIPRNet	Secure Internet Protocol Router Network
SMO	Spectrum Management Operations
SSA	Single Security Architecture
SSO	Single Sign-On
SPPN	Special Purpose Processing Node
TS/SCI	Top Secret/Sensitive Compartmented Information
UAM	User Activity Monitoring
UAP	Unified Action Partner
UC	Unified Capabilities
UJTL	Universal Joint Task List
VoIP	Voice over Internet Protocol
VTC	Video Teleconference