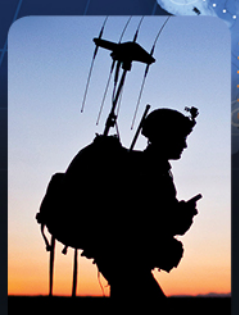
Office of the Army Chief Information Officer/G-6

ARMY NETWORK CAMPAIGN PLAN 2020 & BEYOND

Implementation Guidance

NEAR TERM

2017-2018



CIO/G-6

ENABLING SUCCESS For Today & 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 Do not cite this document for the purpose of advertisement.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-AO), CIO/G-6, ATTN: Mr. Edwin Payne, 107 Army Pentagon, Washington, DC 20310-0107.

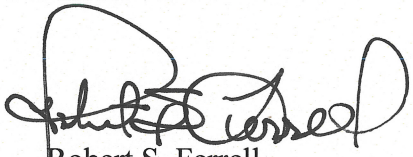
Executive Summary

Over the last decade, the Army invested heavily in augmenting and integrating the network's operational component capabilities. Investments in enterprise and installation capabilities, however, remained relatively stagnant, fostering significant disparities. The goal of the *Army Network Campaign Plan (ANCP) - Implementation Guidance, Near Term* is to address these disparities by synchronizing the hardware, applications and services that enable both warfighting and business operations. In alignment with the *ANCP* and the *Army Operating Concept*, it sets the framework to support the design, development and fielding of a truly end-to-end network capability that supports future mission operations and brings the enterprise to the Soldier.

The FY17-18 near-term implementation guidance aligns the development of enterprise, system-of-systems and solution architectures with Army network strategy and information technology portfolio planning and programming. Using assessments produced through the Army Enterprise Network portfolio management and Army Warfighting Challenge processes, the Army will focus on providing greater tactical and institutional power and efficacy through network convergence, cloud computing, Unified Capabilities, data center consolidation, Windows 10 migration, Home-Station Mission Command Centers, Korea switch upgrades, the Signal Force Pilot and cyber asset visibility. The near-term guidance also sets the conditions for the mid-term implementation guidance, which covers capability modernization and associated activities in FY19-23.

FY17-18 initiatives are informed by what was actually accomplished in FY16, given fiscal realities. The Army expects efficiencies from FY16 network modernization efforts to continue through the Future Years Defense Program.

The Chief Information Officer/G-6 and stakeholders from across the Army are steadily improving the network and the services it provides. This concerted effort will establish a secure end-to-end network that reaches from the home station to the tactical edge, and reliably provides a consistent set of capabilities and services regardless of the user's location and environment. The ultimate objective is to empower Soldiers and decision makers with the information and tools they need to execute their missions as effectively and efficiently as possible. A ready, network-enabled Army is key to winning in a complex world.



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

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Introduction

Building on the momentum of FY16 network-related efforts, the *Army Network Campaign Plan (ANCP) – Implementation Guidance, Near Term* captures the major initiatives within the FY17-18 timeframe. It also sets the conditions for the *ANCP – Implementation Guidance, Mid Term* and informs Program Objective Memorandum (POM) FY19-23.

Army Network Campaign Plan Construct

The ANCP is composed of three documents that align with the Department of Defense (DoD) Joint Information Environment (JIE) and the Army Campaign Plan: the *ANCP*, 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 annually. The ANCP is designed to influence network planning activities across the Army, in the context of budget realities. In addition, *Shaping The Army Network: 2025-2040* (STAN), published in March 2016, serves as a future-looking document to guide ANCP efforts. The table below describes the purpose of each document and the associated timeframes.

ANCP Document	Purpose	Timeframe
ANCP	• Links with relevant Army and DoD strategies. • Describes network-related end states at a high level and outlines lines of effort.	2020 and Beyond
ANCP – Implementation Guidance, Near Term	• Describes execution activities within a two-year timeframe. • Reflects acquisition, resource and mission reality. • Guides the design and development of the next network capability set.	2017-2018
ANCP – Implementation Guidance, Mid Term	• Focuses on future network capabilities. • Designed to impact resource planning within POM venues.	2019-2023
Shaping The Army Network	• Informed by analysis of technology trends and forecasts. • Designed for a commander-focused Army network tailored to formation, echelon and mission. • Supports The Army Plan and builds upon the Army Operating Concept.	2025-2040

Table 1: ANCP Construct

ANCP Near-Term Construct

The near-term implementation guidance is a living document, updated on an annual basis to reflect the realities of Army mission obligations, acquisition planning and resourcing. This is the third iteration; it reflects FY16 accomplishments and describes FY17-18 planned activities. Aligned with the *ANCP* and dependent upon resource constraints, it provides direction for

execution of network initiatives and informs the annual Headquarters, Department of the Army (HQDA) Institutional Network Modernization Execute Order (EXORD).

The near-term implementation guidance is developed in alignment with the Army Enterprise Network (AEN) domains – Network Capacity Domain (NCD), Enterprise Services Domain (ESD) and Network Operations and Security Domain (NSD) – and in coordination with multiple communities of interest, 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, such as Army strategic guidance, senior leader goals and objectives, current Army mission obligations, the status of Enterprise Information Environment Mission Area (EIEMA) IT investments, and acquisition and resourcing plans. Near- to mid-term activities, supported through IT investments, will be aligned, managed and tracked through the Chief Information Office/G-6's (CIO/G-6) five lines of effort (LOEs).

Described below in Figure 1, LOEs link tasks, effects and conditions to the strategic vision and end state, and help define how individual actions contribute and combine to achieve the outcomes desired in 2020 and beyond. These end states align with the six focused end states codified in the 20 February 2015 Chief of Staff of the Army (CSA) memorandum regarding the Mission Command (MC) Network way ahead. The LOEs depicted below, and described in the *ANCP,* are the current set of network priorities for the near and mid terms. New LOEs will emerge based on the progress achieved in the execution of the near- and mid-term implementation guidance. LOE goals are outlined below.

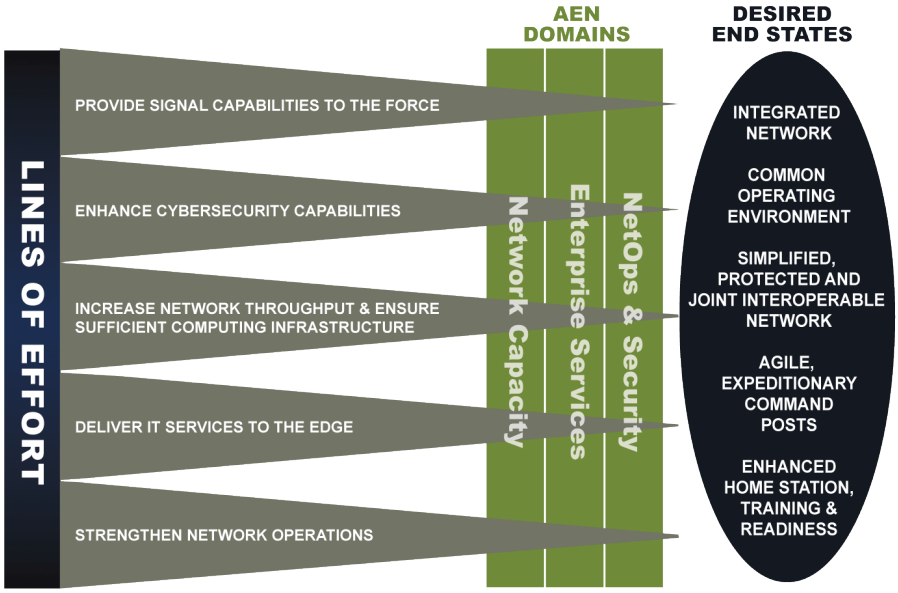


Figure 1: ANCP Operating Construct

LOE 1 – Provide Signal Capabilities to the Force. Optimize the Signal force to synchronize delivery of future capabilities, and to ensure effective operation and defense of a single, end-to-end network, by continually assessing and shaping doctrine, force structure and equipping and training concepts across the operating and generating forces.

LOE 2 – Enhance Cybersecurity Capabilities. Optimize defensive cyberspace operations (DCO) and DoD Information Network (DoDIN) operations by continually assessing and shaping cybersecurity strategy, policy, doctrine and resourcing to enhance the security of the network and information environment.

LOE 3 – Increase Network Throughput and Ensure Sufficient Computing Infrastructure. Lead and integrate Army strategy, policy and resourcing to deliver a robust and secure transport and computing infrastructure that will enable assured warfighting, business and enterprise information environment operations.

LOE 4 – Deliver IT Services to the Edge. Provide a consistent, end-to-end user experience through strategy, policy and resources that effectively, efficiently and securely operationalize and improve IT service delivery.

LOE 5 – Strengthen Network Operations. Optimize end-to-end network operations by leading the development of data and resource strategies and policies, and an integrated architecture that establishes common processes and standards. Simplify and standardize network operations capabilities in support of and integrated with DoDIN operations.

The activities planned for FY17-18 execution enable network advancements to support future mission operations and bring the enterprise to the Soldier anywhere, anytime. They will occur through programs of record (PORs) and other initiatives to ensure that the institutional network infrastructure is proactively modernized and seamlessly integrates with capability set efforts. Near-term initiatives focus on transitioning Army users from disjointed systems to enhanced and centralized services that conform to the Common Operating Environment (COE). These changes will return tangible benefits for Army users, such as greater bandwidth, stronger security and always accessible enterprise services.

The ANCP is consistent with the direction outlined in the DoD Cyber Strategy and the Army Cyberspace Strategy for Unified Land Operations 2025, which formalizes the requirement to build and maintain ready forces and capabilities to conduct cyberspace operations. Moreover, the plan supports Army Warfighting Challenge #7 (Conduct Space and Cyber Electromagnetic Operations and Maintain Communications), specifically learning demand 7.3 ("What is the optimal way to employ cyber capabilities with the elements of traditional combat power to support Unified Land Operations and deliver the effects required by commanders at all echelons?"). Furthermore, the ANCP is consistent with direction from other cyberspace operations directives and documents, such as CSA directives, the Army Cyberspace Strategy, the Army Cyber Materiel Development Strategy (2014-2048), the Army Cyber Command (ARCYBER) and Second Army Strategic Plan (2015), the Army Operating Concept, Army Warfighting Functional Concepts, and the Cyberspace Acquisition, Requirements, and Resourcing (CARR) Annual Plan.

FY17-18 Resourcing Overview

In FY17-18, resources provide the capabilities to operate, manage and defend Army networks against cyber threats, and fund DoD Enterprise Email (DEE), the Army Enterprise Service Desk (AESD), Unified Capabilities (UC), content management and DoD Enterprise Portal Services (DEPS). Army resourcing also supports DoD's Joint Regional Security Stack (JRSS) implementation, the Defense Information Systems Agency's (DISA) European Transport Initiative and U.S. Forces Korea network modernization, which includes replacing legacy

switches. Funding is programmed to sustain upper- and lower-tier transport capabilities and to modernize position, navigation and timing (PNT) and cryptographic capabilities.

FY17-18 Planning Guidance

Enterprise portfolio management (PfM) is the centralized management of one or more mission area portfolios, which includes identifying, prioritizing, authorizing, managing and controlling projects, programs and other related work to achieve specific strategic objectives. Figure 2 below is a graphical depiction of the DoD IT PfM construct and the Army's nested organizational structure.

The EIEMA represents IT investments, as a portfolio, that focus on improving Army Enterprise Information Environment (EIE) capabilities. Elements within the EIEMA provide life-cycle oversight and holistic PfM to applicable Army IT investments (programs, systems and initiatives). As the EIEMA lead, the CIO/G-6 supports the DoD EIE mission lead and ensures that EIE efforts are traceable to, and fully enable, capabilities for the Warfighting, Business and Intelligence Mission Areas.

The DoD IT portfolio capability areas are aligned to DoD's Joint Capability Areas (JCAs). JCAs are collections of similar activities, functionally grouped to support capability analysis, strategy development, investment decision making, capability portfolio management and capabilities-based force development and operational planning. The CIO/G-6's NCD portfolio encompasses DoDIN capabilities related to information transport and computing services; the ESD encompasses information sharing and core enterprise services; and the NSD encompasses network management, cybersecurity and DCO - Internal Defensive Measures (DCO-IDM).

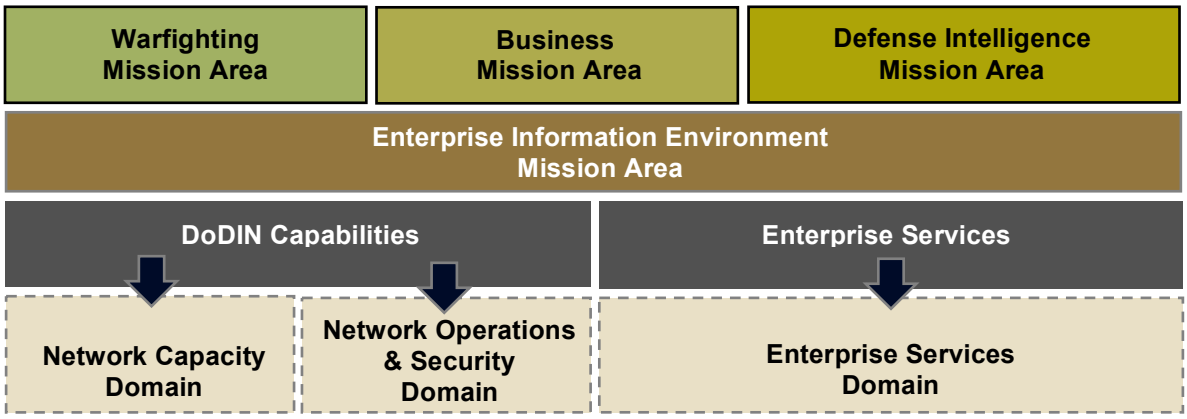


Figure 2: Army IT Portfolio Management Construct

AEN domain efforts have complex relationships and dependencies that are critical to reaching desired end states in the near term and facilitating achievement of end states in the mid and long terms. Network activities, logically grouped as primary and supporting efforts, span the three AEN domains from an IT investment planning and management perspective, and are guided through implementation by the CIO/G-6 LOEs. Primary efforts are critical to enabling the network to achieve end states in the near term and to setting conditions for modernization in the mid term. Supporting efforts bolster planned initiatives or deliver forecasted efficiencies. Primary and supporting efforts can either occur within a specific AEN domain or, due to interdependencies, span multiple domains to achieve a common goal and benefit the network.

Details associated with individual activities are summarized below and addressed in depth in Appendices 1 through 3.

Several strategic resource and environmental factors affect the planning and execution of FY17-18 activities and potential follow-on actions. They include:

- PRINCIPLES, POLICIES AND FRAMEWORKS. Guidance for day-to-day operations in order to achieve strategic goals.
- PROCESSES. Methods and performance measures to achieve specific strategic objectives and produce the outputs that support achievement of strategic goals.
- ORGANIZATIONAL INFLUENCE. Key internal and external stakeholders inform resource decision-making to achieve strategic goals.
- INFORMATION. Critical to providing the right resources to achieve strategic goals.
- PEOPLE, SKILLS AND COMPETENCIES. Required for successful completion of all functions and tasks, making correct decisions and taking corrective action.
- SERVICES, INFRASTRUCTURE AND APPLICATIONS. Provide IT and network processing, systems and services.
- CULTURE, ETHICS AND BEHAVIOR. Critical for the organization to realize strategic goals.
- FINANCIAL. Adopt an efficient financial model for all aspects of information technology modernization efforts.

FY17-18 Primary Efforts

The subsections below describe network activities, responsible supporting domains and expected benefits of the following primary efforts.

- Establishing a COE *
- Delivering UC
- Continuing Operational Unit Modernization
- Establishing Home-Station Mission Command Centers (HSMCCs)
- Achieving Network Infrastructure Modernization and Network Consolidation *
- Reducing the Cyberspace Attack Surface *
- Standardizing Authorized Hosting Environments *
- Migrating to Windows 10 Operating System
- Organizing and Advancing Mobility
- Aligning Army Information Security Continuous Monitoring (ISCM) with the DoD Framework
- Enhancing Cyberspace Situational Awareness by Leveraging Big Data/Cyber Analytics*
- Refining the Role of the Cyberspace Workforce

** These primary efforts combine to support a synergistic approach to cyberspace situational awareness, DCO and other cyberspace capabilities.*

Establishing a Common Operating Environment (COE)

The COE is an approved set of computing technologies and standards to which the network itself and all applications and systems riding the network must adhere. The intent of the COE architecture is to normalize the network environment – that is, to make computer systems, operating systems, databases, security configurations and end-user devices common and interoperable across the entire force.

Computing environments (CEs), which are used to organize the COE, are logical groupings of systems with similar characteristics. A CE comprises the hardware, operating systems, libraries and software required to run applications within the COE. The current CEs are:

- Data Center/Cloud/Generating Force (DC/C/GF)
- Command Post (CP)
- Mounted
- Mobile-Handheld
- Sensor
- Real-Time/Safety Critical/Embedded

The COE will transform the business rules, organizational behavior and engineering basis of the acquisition cycle to produce more agile delivery of future capabilities in the face of changing threats and emerging needs. Properly executed, the COE will enable the Army to design, develop, test, certify and deploy software capabilities rapidly and efficiently while mitigating the introduction of harmful or unexpected consequences. Incorporating Army Special Operations Forces into the COE will improve cross-component mission command and situational awareness during operational planning and execution.

The Army is currently focused on four critical COE objectives:

1. Implement standardized end-user environments.
2. Implement standardized software development kits.
3. Implement streamlined software development, integration, testing, certification and fielding processes that rely on common reusable software components that have already successfully gone through the Army Interoperability Certification process.
4. Develop deployment strategies that provide a more efficient method of updating software within the already fielded baseline.

In FY16, the Army adopted the Army way ahead on COE and computing environment testing.

In FY17, G-3/5/7 and ASA(ALT) decided that no additional work on COE 1.1 or 2.0 would occur in favor of improving interoperability across the Army by reducing the number of fielded COE versions. In FY17-18, ASA(ALT) plans to develop COE 3.0, leveraging Software Block 11/12 baseline as the foundation.

In FY18, CIO/G-6 will conduct interoperability certification testing of the COE 3.0 baseline. As part of the unforeseen requirement to migrate to Windows 10, CIO/G-6 will develop a strategy to integrate the new operating system into COE 3.0. ASA(ALT) intends to begin COE 3.0 deployment in FY19.

Network Activities	LOEs	AEN Domains	Army Benefits
• Develop a set of validated top-level COE requirements, aligned to the JIE and Mission Partner Environment (MPE), to guide the design and architecture of the individual CEs. • Implement open standards within the CE architecture. • Field COE iteratively. Successful Army interoperability testing (Army Interoperability Certification) is required prior to introducing new capabilities into the COE. • In coordination with Training and Doctrine Command (TRADOC), develop communications protocols and data standards mapped to TRADOC-approved information exchange requirements. • Migration to Windows 10.	**1** 3 4 2 5	**NCD** ESD NSD	• Alignment with JIE/MPE will position the Army to achieve mission command interoperability between Army conventional and Special Forces, and with unified action partners. • Facilitate interoperability across environments and foster reuse of common components. • Enable device-agnostic capabilities. • Greater capability agility. • Lower life-cycle costs through standardized applications and unity of effort. • Flexible infrastructure that evolves to match rapidly emerging standards. • Enhanced cyberspace protection.

Table 2: COE Activities and Benefits

Delivering Unified Capabilities (UC)

UC consist of integrated voice, video and data services that are delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to enable universal collaboration and to increase mission effectiveness of the warfighter and business communities.[1] UC will interface with deployed elements of the network and associated mission command capabilities to create a common user experience. A "common user experience" is the idea that employment of the network should not change radically across echelons, formations or operational phases, whether the user is deployed or at home station. It should facilitate the transmission of information that warfighters require at the point of need.

In FY15-16, the conditions were set to transition to Internet Protocol (IP) video teleconference (VTC) and the Army developed requirements for a UC soft client enterprise capability. To support the consumption of a UC soft client from a commercial cloud, the Army and DISA, in partnership with the National Security Agency (NSA), crafted a UC Reference Architecture. The Army also evaluated how cloud-based office automation services could support the Army's UC effort and improve daily business processes. The Army released a request for proposals in early FY17 and expects to award a contract later in FY17 for UC deployment to a select set of users.

By the end of FY17, the Army intends to have a plan to transition from Time Division Multiplexing (TDM) to IP, to complete the migration from Integrated Services Digital Network (ISDN) to IP VTC, and to field a UC soft client to a limited segment of the force. UC initial

[1] *Department of Defense (DoD) Unified Capabilities Master Plan (UC MP), October 2011.*

operating capability (IOC) is expected by the end of FY18. These initiatives will significantly advance consolidation of communications solutions, reducing the reliance on disparate, legacy communication methods and simplifying the user experience.

Network Activities	LOEs	AEN Domains	Army Benefits
• Limited deployment of UC soft client capabilities, to include chat/instant messaging, soft phone, screen sharing, presence and the continuation of Voice over IP (VoIP) and IP VTC either via the Network Enterprise Technology Command theater plan or the DISA Global Video Service. • IP VTC and TDM transition plans that support DoD-wide efforts. • Develop VoIP user framework for assured and non-assured users.	**4** 3 2 5 1	**ESD** NSD NCD	• Better user experience, with timely access to data at the point of need. • Standardization and greater ease of use. • Lower operating and sustainment costs.

Table 3: UC Activities and Benefits

Continuing Operational Unit Modernization

Capability Set (CS) integration is the Army's capstone mission command configuration modernization process for Brigade Combat Teams (BCTs), executed through the Unit Set Fielding model. A Capability Set is an entire package of new and emerging technologies (e.g., network components, associated equipment and software) that provides an integrated and interoperable network capability from the static Tactical Operations Center to the dismounted leader. Capability Sets are tailored to meet operational needs and will differ among types of BCTs. Integration depends on resource constraints, availability of the components to be fielded and availability of unit equipment that is undergoing modernization. In FY16, Capability Set integration was focused on fielding to the maneuver battalions added to CS14/15 units in accordance with Army Structure Memorandum 14-18.

Concerted efforts will continue in FY17-18 to align the operational and institutional components of network modernization through various bodies, such as the Army Enterprise Network Council (AENC), the LandWarNet2 / Mission Command General Officer Steering Committee and the Mission Command Network Modernization Working Group. End-to-end alignment of the network's operational and institutional components will produce a synchronized, interoperable environment that improves readiness and training for commanders, staff and Soldiers, increases interoperability and simplifies mission command capability across Joint and coalition partners.

[2] *While LandWarNet remains the official term for the Army's network infrastructure, it is referred to as DoDIN-Army (DoDIN-A) in Joint Publication 3-12.*

Network Activities	LOEs	AEN Domains	Army Benefits
• Fielding of Warfighter Information Network - Tactical (WIN-T) Increment 2; tech refresh of WIN-T Increment 1B. • Interim en route mission command capability. • Synchronize HSMCC capabilities with network modernization efforts. • Continue Joint Battle Command - Platform fielding. • Handheld Manpack and Small Form Fit full-rate production decision and fielding (FY17). • Field and sustain Army Requirements Oversight Council-validated Transportable Tactical Command Communications bridge.	**1** 3 2 4 5	**NCD** NSD ESD	• Provide more reliable and versatile on-the-move tactical communications, improving collaboration among forces at all levels. • Simplify the network: ease of use, fewer physical components and more agile command posts. • Improve force readiness for no-notice deployments. • Enable deploying forces to develop situational understanding and continue to plan while embarked on strategic airlift. • Ensure that all Army forces are trained and ready prior to deployment. • Reduce Soldier burden by combining the capabilities of two radios – Single Channel Ground and Airborne Radio System and Soldier Radio Waveform – into one.

Table 4: Operational Component Modernization Activities and Benefits

Establishing Home-Station Mission Command Centers (HSMCCs)

The HSMCC, conventionally known as a joint operation center, increases commander flexibility by providing a suite of sustained and standardized technical capabilities, components to operate multiple networks, enhanced audio-visual capabilities, and the physical infrastructure necessary to establish uninterrupted expeditionary mission command through all phases of operations. Divisions, corps and select theater commands require these enduring and fixed operations centers that enable reach-back and reach-forward expeditionary mission command even when tactical operations centers are deployed. Enduring command centers also are necessary to support Regionally Aligned Forces (RAF), military support to civil authorities, homeland defense and other non-traditional missions. The Army will perform a technical refresh of prioritized command centers in FY17 to establish an interim technical baseline while Army requirements are finalized. The Army will then focus on development of a distributed mission command capability, instantiation of the DC/C/GF Computing Environment, integration of VoIP and Secure VoIP, JIE synchronization and network operations integration. By leveraging modernized installation infrastructure, the Army will not have to field additional sets of hardware to enable HSMCCs.

Network Activities	LOEs	AEN	Army Benefits
• Continue deployment of Multi-Protocol Label Switching to installations both within and outside the continental United States. • Continue implementation of Installation Campus Area Networks.	**1** 2 4 5	**NCD** **ESD**	• Simplify the network: ease of use, fewer physical components, more agile command posts. • Distributed mission command provides persistent capability at home station for the commander, and provides a launch platform allowing greater flexibility for forward-echelon warfighting functions. • Improve force readiness for no-notice deployments. • Enable deploying forces to develop situational understanding and continue to plan while conducting distributed mission command through "reach back".

Table 5: HSMCC Activities and Benefits

Achieving Network Infrastructure Modernization and Network Consolidation

In FY16, seven continental United States (CONUS) and three outside CONUS (OCONUS) Non-Secure IP Router (NIPR) JRSS sites became operational. Multi-Protocol Label Switching (MPLS) routers were installed at 30 sites and Installation Campus Area Network (ICAN) upgrades were completed at 14 Defense Information Systems Network Subscription Services (DSS) sites, six non-DSS CONUS sites and one OCONUS site.

In FY17-18, the Army will continue to improve its institutional network infrastructure and consolidation of the following separate networks: U.S. Army Reserve (USAR), Army Corps of Engineers (USACE), Army National Guard (ARNG), Army Materiel Command, Medical Command, Installation Management Command, and Army Test and Evaluation Command. Additionally, the Army will leverage appropriate governance processes to obtain an approved resourcing plan for the 205 non-DSS sites (also known as Army Access Sites). The table below summarizes activities and benefits to the Army.

Network Activities	LOEs	AEN Domains	Army Benefits
• Consolidate Top-Level Architecture Stacks into JRSS. • Continue deployment of MPLS to CONUS and OCONUS installations. • Continue close coordination with the appropriate stakeholders to develop a suitable technical solution, clearly defined and documented, prior to integrating separate networks. • Continue implementation of ICANs. • Set the conditions for integration of deployable network transport solutions into a unified information transport delivery capability.	**3** 2 5	**NCD**	• Enhanced security architecture and improved throughput that support UC and allow users to fully leverage enterprise services. • Greater reliability, availability and flexibility to enable garrison-based mission command operations and live, virtual, constructive and gaming training. • Improved user experience, with timely access to data at the point of need. • Divestiture of legacy systems and equipment.

Table 6: Network Infrastructure Modernization and Network Consolidation Activities and Benefits

Reducing the Cyberspace Attack Surface

In FY17, convergence and consolidation of Top-Level Architecture Stacks into JRSS will continue to be a major priority for the Army. The Army's installation of JRSS NIPR sites and JRSS Secure IP Router (SIPR) sites sets conditions for a more rapid transition to a unified information transport capability. The Army will continue efforts to reduce duplicative legacy security architecture systems. Fewer network ingress/egress points will lower the potential exposure to cyberspace threats and attacks, and simplify network management and network defense.

In FY17, the Army will continue to develop plans, in coordination with DoD and Intelligence Community (IC) stakeholders, to re-provision NIPR and SIPR networks that traverse the Army's Ground Intelligence Support Activities to the operational control and oversight of the Signal community. Known as provisioning convergence, this change will lead to greater efficiency in network operation and maintenance, as well as significant cost savings. Additionally, community of interest networks (e.g., USACE, USAR and ARNG) will continue migration behind the JRSS Single Security Architecture.

Network Activities	LOEs	AEN Domains	Army Benefits
• Network Modernization - JRSS, Joint Management System, MPLS, ICAN • Provisioning Convergence • Network Operations Tools Convergence	**5** 2 3	**NSD** NCD	• Simplify the network, reduce the network attack surface and standardize network security. • Integrated, simplified, protected and interoperable network.

Table 7: Reduced Cyberspace Attack Surface Activities and Benefits

Standardizing Authorized Hosting Environments

To adhere to DoD and Army mandates and lay the foundation for future cloud computing capabilities, the Army will continue to consolidate and transition standalone data center solutions to authorized enterprise hosting environments that enable standard and centralized operations in conjunction with JIE. As of the end of FY16, a total of 425 data centers had been closed.

The Army simultaneously is pursuing a major rationalization effort for current applications and systems to assist commands with their data center transition efforts. The Army Application Migration Business Office reviews requests in preparation for migration to DISA Core Data Centers (CDCs), Army Enterprise Data Centers and the commercial cloud.

Data center consolidation and application rationalization are laying the computing foundation for future data support across the Army enterprise. Enterprise service hosting for capabilities such as email, UC, file sharing and mission applications will be executed through the DC/C/GF Computing Environment. On 9 December 2016, the Secretary of the Army signed Army Directive 2016-38 (Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers), ordering the closure of data centers and migration of enterprise systems and applications to approved enterprise hosting environments.

Network Activities	LOEs	AEN Domains	Army Benefits
• Continue to transition standalone data centers to DoD-authorized hosting environments. • Designate standard Installation Processing Nodes and Installation Service Nodes. Establish service-oriented standard operating procedures. • Rationalize, virtualize and migrate applications to DoD-authorized hosting environments (application migration to NIPRNet enclave in commercial and DoD hosting environments). • Standardize CDCs. • Develop and publish an Army application hosting methodology.	**3** 4 2 5 1	**NCD** ESD NSD	• Robust data storage, on-demand computing, elastic capacity, improved security and more efficient operation and maintenance. • Smaller operating force footprint in theater. • Rapid and more efficient evolution of applications, which will help to minimize costs and speed dissemination of application enhancements. • Enable the processing of large amounts of data to improve decision-support cycles.

Table 8: Standardized Authorized Hosting Environments Activities and Benefits

Migrating to Windows 10 Operating System

In February 2016, the Deputy Secretary of Defense directed all of DoD to migrate to the Microsoft Windows 10 Secure Host Baseline. The objective is to strengthen DoD's cybersecurity posture while concurrently streamlining the IT operating environment. While U.S. Cyber Command leads the overall DoD implementation effort, HQDA CIO/G-6 is managing the Army's transition to Windows 10, in coordination with ARCYBER and Network Enterprise Technology Command.

The enterprise-wide Windows 10 upgrade will be applied to all existing Windows clients on DoD information networks and all unclassified, Secret and Top Secret collateral information systems, to include: desktops, laptops and tablets; Special Access Program systems; mission systems; strategic, tactical, research and development, training and evaluation systems; platform information technology; and weapon systems (to the maximum extent practicable).

When the Secure Host Baseline is fully deployed with all components activated, such as Credential Guard, Device Guard and Secure Boot, network vulnerability will significantly diminish. Credential Guard offers better protection against advanced persistent threats, such as the credential theft attack tools and techniques common in targeted attacks and malware that utilize administrative privileges. Device Guard "locks down" a device so that it can only run trusted applications, which helps to protect against Zero Day and other attacks. Similarly, AppLocker can be used to automatically prevent applications from running by excluding them from the allowed list.

In FY16, the Army conducted a Windows 10 pilot, began inventorying its systems and applications, initiated operating system testing and evaluation in CONUS and OCONUS, and developed a high-level roadmap to set the conditions for wider deployment in FY17. On 21 August 2016, the Army CIO/G-6 issued a one-year Army-wide waiver to the DoD-mandated Windows 10 migration deadline of 31 January 2017. The Army now expects to have implemented Windows 10 on 90 percent of enterprise systems (desktops, laptops, tablets) by

31 January 2018. Enterprise systems that cannot be migrated by this date must submit waiver requests and plans of action and milestones by 31 July 2017.

Programs of record, which include weapon, mission command, logistics and medical systems, will begin transitioning in the FY17-18 timeframe but are not expected to complete migration until the mid-term period (FY19-23).

Network Activities	LOEs	AEN Domains	Army Benefits
• Development of regional/organizational deployment plans and timelines. • Installation of current versions of Host-Based Security System and System Center Configuration Manager. • Deployment of the Global Enterprise Fabric and continued implementation of ICANs. • Life-cycle replacement of hardware to meet DoD Security Technical Implementation Guide requirements. • Application identification, rationalization and remediation. • Deployment of Windows 10 operating system. • Monthly progress reporting to ARCYBER.	**3** 4 2 5 1	**NCD** ESD NSD	• Improve the Army's cybersecurity posture, streamline the IT operating environment and, ultimately, lower the cost of IT/network operation and maintenance. • Common baseline will enable quicker patching, counter certain common cyber intrusion techniques, improve accountability and transparency, and allow cyber defenders to better detect malicious activity. • A DoD-wide common operating system baseline will promote faster and easier implementation of technology upgrades, and allow DoD to leverage common applications and enterprise solutions. That, in turn, ultimately will lower information technology-related costs.

Table 9: Windows 10 Migration Activities and Benefits

Organizing and Advancing Mobility

Mobility is a core Army operational capability required to execute missions effectively. Soldiers and commanders must be able to deploy rapidly from home station to the area of operations, then move through the theater, while retaining full communications and collaboration functionality and access to all information sources and analysis, regardless of where they are. This ability to be "connected" is directly contingent upon modernization initiatives that improve the reliability of network infrastructure, increase network capacity and speed, extend enterprise services to the tactical edge and tighten cybersecurity. True mobility also requires secure end-user devices (EUDs) that are easily integrated into the network and withstand the operational environment.

A key focus in FY17 will be the publication of the Army Mobile Vision document, which will communicate the Army's objectives for performing mission functions and executing tasks anytime, anywhere, on any device. This document will serve as the foundation for Army mobility, completely integrating tactical and strategic elements, to include all forms of IT and the scope of all technical requirements. The ultimate goal is to enable the Army to be flexible and fully capable at all times.

While an optimal enterprise mobility capability will not be fully achieved in FY17-18, efforts across the AEN domains will position the Army to rapidly leverage commercial advances in technology, gain efficiencies through the centralized management and standardization of EUDs, and enable users to access and utilize secure, robust applications from multiple devices.

Network Activities	LOEs	AEN Domains	Army Benefits
• Identify and begin implementing adjustments to the installation and deployable network infrastructure components necessary to support the mobile aspect of EUDs (including services necessary to support control systems). • Develop and publish the Mobile Vision document. • Select, standardize and certify end-user services platforms across the Army, with a focus on commercial devices. • Rationalize commercial contracts that provide devices and transport infrastructure to the Army. • Leverage the DISA effort to establish a mobile device store to centralize the hosting and availability of vetted applications that support Army users. • Leverage the DISA effort to establish a mobile device manager to manage devices and the transport infrastructure. • Identify multifactor authentication technologies, other than Public Key Infrastructure, that meet DoD requirements.	**3** 5 4 2 1	**NCD** ESD NSD	• Ensure that the Army is on a modernization path that keeps pace with the evolving technology environment. • Provide an efficient, consistent, secure and reliable mobile device management process, resulting in cost savings and collaboration. • Standardize and simplify the end-user experience across devices.

Table 10: Mobility Activities and Benefits

Aligning Army Information Security Continuous Monitoring (ISCM) with the DoD Framework

ISCM is a primary effort that includes insider threat activities. DoD defines continuous monitoring as the "ongoing observation, assessment, analysis and diagnosis of an organization's cybersecurity posture, hygiene and operational readiness." As an umbrella of activities, processes and analyses, ISCM will bolster the Army's situational awareness of information security vulnerabilities and threats, and thereby support risk management decisions. ISCM will provide security status information and ongoing insight into security control effectiveness, enabling the Army to move from compliance-driven risk management to data-driven risk management. Consequently, ISCM will decrease vulnerabilities in Army information systems, create a top-down culture of cybersecurity compliance and create efficiencies through automation and processes.

In FY16, much of the Army's focus was on the Insider Threat Program and its associated network actions. The Army developed the FY17-21 deployment strategy for user activity monitoring (UAM) capabilities to observe and record users' computer and network activity; implemented Host-Based Security System (HBSS) capabilities on SIPR; and deployed Assured Compliance Assessment Solution (ACAS) capabilities across the enterprise. Additionally, the Army coordinated with the DoD CIO to shape the final guidance for the ISCM Strategy, and supported DoD CIO efforts to standardize the Secretary of Defense Cybersecurity Scorecard and DISA's deployment of the Continuous Monitoring Risk Scoring (CMRS) solution.

In FY17, TRADOC will conduct a Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities - Policy (DOTMLPF-P) assessment to determine whether capability gaps exist within ISCM. The Army will also continue its multi-year, iterative effort to implement CMRS in accordance with DoD and federal strategies. The Army will ensure its initiatives in confidentiality, integrity and availability remain consistent with the CMRS solution; use best practices; and are reliable and cost-effective. Additionally, the Army will continue to work with the DoD CIO to ensure that the Cybersecurity Scorecard accurately reflects the Army's cybersecurity posture, and will provide stakeholder coordination, oversight, policy and funding to support compliance efforts.

Network Activities	LOEs	AEN Domains	Army Benefits
• Complete HBSS implementation on SIPR. • Complete the deployment of ACAS baseline across the enterprise. • Coordinate with DoD CIO to shape final guidance for the Army's ISCM Strategy.	**5** 2	**NSD**	• Maintain awareness of information security vulnerabilities and threats, which supports organizational risk-management decisions by producing risk scores. • Drive down vulnerabilities in Army information systems. • Create a top-down culture of cybersecurity compliance. • Create efficiencies through automation and processes.

Table 11: ISCM Activities and Benefits

Enhancing Cyberspace Situational Awareness by Leveraging Big Data/Cyber Analytics

One of the Army's challenges is to fully exploit the unprecedented growth of data it collects to enhance cyber situational awareness, protect the network and conduct effective DCO. The Army is addressing the key capability gap of cyber situational awareness by leveraging Big Data technology, including the government off-the-shelf Big Data Platform (BDP) and mission-specific cyber analytics.

BDP provides the capability to collect and analyze the massive volumes of configuration, operations and security data generated across the Army's strategic environments. Analytics within the BDP will enable correlation across multiple data sources to identify anomalies within the environment more rapidly and effectively than has been possible with segmented tools and data sets.

Network Activities	LOEs	AEN Domains	Army Benefits
• Continue enhancing the Army BDP. • Continue development of Big Data / cyber analytics in support of DoDIN operations and DCO.	**2** 5	**NSD**	• Improve cyber workforce effectiveness by providing timely access to data in order to make informed and actionable risk-management decisions. • Analyze cyber data for DCO efforts and provide situational awareness of the battle space. • Provide leadership near-real-time risk information to make informed decisions. • Better integrate all of the Army's Big Data efforts, which are led by several organizations.

Table 12: Big Data/Cyber Analytics Activities and Benefits

Refining the Role of the Cyberspace Workforce

The cyberspace workforce is composed of military, civilian and contractor personnel assigned to cyberspace effects, cybersecurity and cyberspace IT, as well as portions of the IC workforce. The Army must articulate in authoritative documents the cyberspace workforce-related terms and items not adequately defined in Joint Publication 3-12.

In FY16, the Army continued alignment of civilian workforce roles with the military Career Field 17 structure, and focused on gaining approval of changes and codifying policies, strategies and plans. In FY17, the Army will continue to refine its cyberspace workforce activities in the same focus areas.

Network Activities	LOEs	AEN Domains	Army Benefits
• Identify, shape and track the civilian cyberspace workforce. • Define work roles. • Align the cyberspace civilian workforce with the military. • Align training and education opportunities with the COE architecture.	**2** 5 3 1 4	**NSD** ESD NCD	• The development and retention of an exceptional cyber workforce is central to DoD's strategic success in cyberspace.

Table 13: Cyberspace Workforce Activities and Benefits

FY17-18 Supporting Efforts

The subsections below describe network activities, responsible domains and desired benefits for the following supporting efforts.

- Standardizing Network Operations
- Increasing the Agility of Spectrum Management Operations (SMO)
- Cryptographic Modernization Initiative (CMI)

- Providing Army Enterprise Service Management (AESM)
- Enhancing Identity and Access Management (IdAM)
- Establishing and Leveraging Enterprise License Agreements (ELA)

These efforts serve as critical enablers to bolster planned initiatives, with a focus on driving efficiencies.

Standardizing Network Operations

Standardizing network operations across the Army will increase LandWarNet effectiveness, availability and performance. Standardization aims to improve efficiency by divesting redundant toolsets, streamlining operations, and increasing visibility and accountability of network operations tools. The ultimate goal is to provide interoperable DoDIN operations and DCO capabilities, from the generating force to the tactical edge.

In FY16, the Army set the foundational elements for streamlining and standardizing the use of end-to-end (enterprise and tactical) network operations tools across the force. This included establishing the Tools Convergence Working Group to coordinate development, assessment, training and integration of end-to-end network operations tools.

In FY17-18, the Army will formalize the Network Operations Tools Convergence Methodology and Implementation Strategy to support alignment and standardization of network operations capabilities across the force. The Army will also publish information exchange specifications (IESs) for Army DoDIN operations, metadata requirements, interoperability specifications and configuration control processes. The overall intent is to address end-to-end network operations and how the Army will use its assets to detect, react to, report and recover from malicious activities while maintaining cyber situational awareness across the force.

Network Activities	LOEs	AEN Domains	Army Benefits
• Oversee compliance with network operations IESs. • Develop and publish network operations metadata requirements. • Formalize an end-to-end network operations framework that provides the methodology and process to identify redundancies and analyze current tools and new requests for tools. • Implement an end-to-end Network Operations Tools Repository containing technical, cost and license data.	**5**	**NSD**	• Simplified and standardized network operations. • Interoperable end-to-end network operations. • Visibility and accountability of all Army network operations tools.

Table 14: Network Operations Activities and Benefits

Increasing the Agility of Spectrum Management Operations (SMO)

The Army Spectrum Management Program is aligned with DoD guidance and supports the ANCP. Adherence to its precepts will enable effective SMO that meet Army requirements across the range of military operations. Increasing the agility of SMO will further enable net-centric warfare through assured access to the electromagnetic spectrum (EMS) and thereby will extend the enterprise to the Soldier to support mission operations.

In FY16, the Army Spectrum Management Office (ASMO) advanced its pursuit of more agile SMO. In compliance with DoD Instruction 8320.02, ASMO continued its EMS data transition to the Standard Spectrum Resource Format (SSRF) in order to make EMS data interoperable, discoverable and relevant. More than 450 equipment records, containing 15,000 data items, were converted from the legacy EMS data standard to SSRF. ASMO also was actively involved, at the Service and joint levels, in the development of the Electronic Warfare Planning & Management Tool and the Global EMS Information System.

In FY17-18, the Army will continue to simplify and consolidate spectrum management tools, further refine EMS operations doctrine, and engage at the joint, DoD and international levels to ensure that Army EMS needs and interests are met and safeguarded.

Network Activities	LOEs	AEN Domains	Army Benefits
• Transition multiple spectrum management tools to enterprise-level network operations tool solutions. • Implement spectrum data and architecture standards.	**5** 3 1	**NSD**	• Simplify network management. • Provide automated EMS reporting capabilities in near-real time to make informed decisions. • Enable more efficient use of spectrum resources and prioritization in congested bands.

Table 15: Spectrum Management Activities and Benefits

Cryptographic Modernization Initiative (CMI)

CMI is a DoD CIO-led effort, worked in close collaboration with the Services, the NSA and the Joint Staff, to assess and modernize cryptographic capabilities (embedded and standalone) that protect National Security Systems and National Security Information (NSI). Cryptographic modernization must occur continuously in order to address and counter technological obsolescence, adversaries' technological advances in crypto-analytic capabilities, and the cost of concurrently replacing all legacy cryptographic equipment. The Army must ensure that cryptographic requirements, technology, policies and resources are synchronized to maintain confidentiality, integrity and availability of command, control, communications, computers, intelligence, surveillance and reconnaissance capabilities. This effort is therefore spread over multiple Future Years Defense Programs in order to prioritize the most critical initiatives and determine when to accept risk in operating cryptographic solutions beyond the NSA-approved end of life.

In FY17, the Army will implement new encryption standards, revise crypto policies and publish the Cryptographic Modernization Strategy, Implementation Plan and Technology Roadmap to protect the confidentiality, integrity, availability and performance of our networks and information systems. These efforts will set the framework for delivering enhanced cryptographic (embedded and standalone) capabilities, and will enable the divestiture of legacy cryptographic capabilities to ensure that the Army's networks are effectively securing and protecting NSI. The Army will also transition the majority of its communications security (COMSEC) key delivery systems from Electronic Key Management System (EKMS) accounts to Key Management Infrastructure (KMI) accounts. KMI utilizes the latest technology to automate many of the functions within the communications security (COMSEC) key generation, accounting, distribution, destruction and auditing process.

In FY18, as enterprise services are extended to the tactical edge, the Army will utilize cryptographic and key management capabilities to enable the exchange of secure voice, video and data between authorized individuals, groups and entities across the entire Army and among coalition partners. Persistent modernization of these capabilities, which includes replacing legacy technology, waveforms, algorithms and cryptographic equipment, will enhance the confidentiality, integrity and availability of information. These modernization efforts support the Army requirement to improve network performance by reducing the overall burden on the network.

Network Activities	LOEs	AEN Domains	Army Benefits
• Provide an over-the-network key management capability. • Transition from EKMS to KMI. • Modernize cryptographic capabilities (devices, waveforms, algorithms, etc.). • Divest legacy technology, waveforms, algorithms and cryptographic equipment. • Publish the Army Cryptographic Modernization Strategy, which addresses advanced cryptographic capabilities and standards.	**2** 5 1	**NSD**	• Decrease manual key delivery, minimizing the number of Soldiers placed in harm's way. • Enhance programmable and interoperable encryption capability to ensure exchange of authenticated data, information and knowledge between authorized individuals, groups and entities. • Enhance network encryption capability to improve network performance. • Modernize cryptographic equipment and upgrade KMI capabilities in line with the Cryptographic Modernization Strategy.

Table 16: Cryptographic and Key Management Capabilities Activities and Benefits

Providing Army Enterprise Service Management (AESM)

In FY15-16, the Army CIO/G-6 published the first-ever IT service management (ITSM) policy and AESM Reference Architecture. These documents clearly laid out the roles, responsibilities and framework for continually increasing the effectiveness of, improving the security of and gaining efficiencies in Army IT services by standardizing the service delivery process. In support of the Army ITSM policy, Second Army published the AESM Concept of Operations (CONOPS) and AESM Operation Order. Combined, these documents establish the foundation for an integrated, holistic approach to managing IT services based on best business practices.

In FY17-18, the Army will publish various process management plans, complete final service design packages, draft service management plans, and finalize and execute AESM assessment plans. The Army will determine the processes to prepare for implementation, conduct maturity assessments and identify opportunities for improvement. Near-term goals include providing the user additional responsive services, improving automated ticketing and enhancing tracking, management and support analytics to gauge network performance and resolve issues more quickly.

Network Activities	LOEs	AEN Domains	Army Benefits
• Implement the AESM Framework. • Enhance the AESD to improve Tier 0 and Tier 1 services to end users.	**4** 5 3 2 1	**ESD** NCD NSD	• Efficient, effective, secure delivery of IT services to Army users. • Eliminate the time, cost, effort and distraction associated with running local and internal service management platforms.

Table 17: AESM Activities and Benefits

Enhancing Identity and Access Management (IdAM)

The Army is enhancing the enterprise IdAM framework to ensure that it supports the full range of institutional and operational mission requirements. The Army is reviewing life-cycle management policies, standards and technologies that use digital identities for identification, authentication, authorization and accountability for logical and physical access control (e.g., applications, networks, systems, buildings, rooms). The objective is to ensure that mission requirements are met and the Army's IdAM framework aligns with DoD, JIE and federal guidance and regulations.

The Army's enterprise IdAM framework will centrally manage users' digital identity based on authoritative data sources, resulting in improved access, across organizational security boundaries, to required network resources and information services. This capability will enable the Army to extend enterprise services to the tactical edge and provide trusted identity data for the tactical community to leverage in disconnected, intermittent and limited-bandwidth environments. The framework also will allow the Army to manage all users', including privileged users', identity credential services, to audit user access to logical and physical resources, and to utilize role-based access control solutions – thereby ensuring that the right individuals obtain the right information at the right time for the right reasons.

Network Activities	LOEs	AEN Domains	Army Benefits
• Continue IdAM efforts to establish life-cycle management for user identities. • Leverage user identity solutions to support directory services. • Identify non-Public Key Infrastructure, multifactor-authentication technologies that meet DoD requirements.	**2** 4 5	**NSD** ESD	• Stronger security through improved authentication, authorization and accountability of user network transactions. • Decrease the time users are without network connectivity while transitioning between duty stations. • Provide a reliable directory to locate users.

Table 18: IdAM Services Activities and Benefits

Establishing and Leveraging Enterprise License Agreements (ELAs)

In FY17-18, the Army will establish a new Microsoft ELA, identify new opportunities for other ELAs, implement a software asset management (SAM) tool, and fully support and implement DoD-wide plans for the transition of its business systems, platform IT and weapons systems, including PORs, to Windows 10. Windows 10 provides cybersecurity enhancements designed to

counter current cyber exploits and will give the Army a common desktop, laptop and tablet baseline that enables more timely patching of business and warfighter systems.

Network Activities	LOEs	AEN Domains	Army Benefits
• Negotiate and maintain ELAs with vendors that support the network. • Enterprise software management. • Address top initiatives, such as operating system migration, through ELA negotiations. • Implement a SAM tool.	**4** 3 5	**ESD** NSD NCD	• Centralize the Army's purchasing power to potentially provide larger amounts of software/equipment at a lower cost per item.

Table 19: ELAs Activities and Benefits

Summary

To enable the Army of 2020 and beyond to meet the challenges of the 21st century, it is essential that the Army rebalance and unify the network into an end-to-end capability. The *ANCP – Implementation Guidance, Near Term* frames planning to support the design, development and fielding of enhancements in FY17-18 for a resilient, easy-to-use and available network. It is critical that senior leaders across the Army understand the relationships and interdependencies among activities occurring within each of the AEN domains and LOEs. The near-term implementation guidance synchronizes planning with the realities of Army mission obligations, financial resources and changes in acquisition practices, thus ensuring that modernization efforts are coordinated and, when solutions are delivered, they can be utilized to their full potential by Army users.

FY17-18 efforts in infrastructure modernization will dramatically improve network capacity and strengthen network security. Greater capacity and security will enable COE implementation and delivery of UC. They will also allow the operating force to leverage institutional capabilities, such as home-station operations centers and global CDCs that host operational information, to reduce the forward footprint of mission command centers. Mobility initiatives will focus on providing Soldiers the flexibility to connect to information from their mobile devices. CIO/G-6 also will aggressively lead the evolution of the IT workforce's role and proactively strengthen the understanding of cyberspace situational awareness and continuous monitoring, to include leveraging Big Data analytics processes and tools.

Supporting efforts in FY17-18 include the standardization of network operations capabilities to manage more effectively the Army's single network environment. The Army will modernize cryptographic and key management capabilities, enhance IdAM, directory services and Public Key Infrastructure, and increase the agility of spectrum management operations. The Army also will continue to expand enterprise services management and the use of ELAs to optimize economies of scale and ensure Army-wide distribution of the most up-to-date capabilities and tools.

Each AEN domain has an appendix that discusses in detail the activities planned for FY17-18. Additionally, this is the first iteration of the *ANCP Near-Term Implementation Guidance* that includes an appendix of key performance indicator (KPI) tables that capture primary initiatives for each domain. These KPIs will be refined over time. CIO/G-6 also is developing performance metrics, which will be built into and tracked in the Strategic Management System.

Appendix 1 – Network Capacity Domain (NCD)

The NCD portfolio includes the physical information technology (IT) infrastructure over which all data, voice and video services and information-based activities must pass. It provides the essential "information highway" for conducting wartime and traditional business communication operations. Both the Enterprise Services Domain (ESD) and the Network Operations and Security Domain (NSD) require this infrastructure to effectively operate the systems within their portfolios.

The primary goal of the NCD is to optimize the investments necessary to provision the transport and computing infrastructure of a modernized, global, versatile, effective and secure network that gives Regionally Aligned Forces (RAF) and unified action partners (UAPs) the full range of military and business operational advantages across all operational phases.[a]

The NCD will produce three outcomes in FY17-18.

1. A resilient transport network that manages throughput to meet demand.
2. An optimized, responsive computing and storage capability, and the ability to identify opportunities to mitigate demand.
3. Access to a wireless infrastructure that provides unclassified and classified information sharing via voice, video and data regardless of mission environment.

FY17-18 Priority Activities

In FY17-18, there are six network capacity priority activities intended to support the aforementioned outcomes, thereby enabling Soldier access to tailored and timely information at the point of need.

The table below lists FY17-18 NCD activities and shows their alignment to Joint Capability Areas (JCAs).

[a] *NCD efforts are driven by the 11 July 2013 DoD CIO memorandum titled Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration, which identifies the need for a robust transport infrastructure that provides sufficient, resilient, reliable computing and storage capacity, and mobile capabilities. It also mandates migration of applications, systems and data to DoD-approved enterprise hosting facilities by the end of FY18.*

FY17-18 NCD Activities	Joint Capability Area 6 Communications and Computers									
	6.1 DoD Information Network 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					
	6.1.1.1.1 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	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
Network Infrastructure Modernization and Path Diversity	•	•	•	•	•	•				
Integrate Separate Networks	•	•	•	•	•	•				
Improve Transport Capacity for Deployable Forces			•	•	•	•				
Data Center and Application Consolidation; Installation Processing Node/Installation Service Node/Special Purpose Processing Node Standardization							•	•	•	
End-User Services										•
Divestiture Planning	•	•	•	•	•	•	•	•	•	•

Table 1-1: NCD Activities Aligned to JCAs

Network Infrastructure Modernization and Path Diversity

Network infrastructure modernization involves increasing throughput and resiliency on installations; deploying Joint Regional Security Stacks (JRSS), which support the Joint Information Environment (JIE) construct; and installing Multi-Protocol Label Switching (MPLS), which provides more effective virtual traffic management at major installations. Infrastructure modernization also will ensure that installations have dual-path diversity to minimize or mitigate the impact of network transport interruptions on critical user communities.

The U.S. Army Reserve (USAR), Army Corps of Engineers, Army National Guard (ARNG), Army Materiel Command (AMC), Medical Command (MEDCOM), Installation Management Command (IMCOM) and Army Test and Evaluation Command (ATEC) are working to consolidate their networks into the Department of Defense (DoD) enterprise network architecture, thereby improving throughput and connectivity for the ARNG, Joint Force Headquarters, armories, Reserve centers and active component installations. These efforts also

will strengthen network security. FY17-18 targeted priorities are critically dependent upon available resources. The Defense Information Systems Agency (DISA), as lead implementer for a number of capabilities within the NCD portfolio, will play a crucial role in keeping modernization efforts on schedule.

In FY16, network infrastructure modernization projected and actual accomplishments included:

- Projected: Installation of Non-Secure IP Router (NIPR) JRSS at 10 sites.

  Actual: DISA completed installation at seven of 11 continental United States (CONUS) sites, two of two sites in Europe, and one of two sites in Southwest Asia (SWA).
- Projected: Installation of Secure IP Router (SIPR) JRSS at 11 sites.

  Actual: DISA completed installation at four of 11 sites. Also, DISA refined Joint Migration Team and Service Migration Team roles and responsibilities to meet Chief Information Officer/G-6 (CIO/G-6) FY16 migration priorities.
- Projected: Installation of MPLS at 30 of 88 sites.

  Actual: DISA installed MPLS at 14 Defense Information Systems Network Subscription Services (DSS) and six non-DSS sites.
- Projected: Installation of Installation Campus Area Network (ICAN) at 17 of 88 sites.

  Actual: ICAN installed at 14 DSS sites and six non-DSS sites.
- Projected: Upgrade 10 optical pathway links for specified CONUS sites.

  Actual: 17 optical pathway links upgraded/delivered for specified CONUS sites.
- Projected: Replacement of Asynchronous Transmission Mode (ATM) / Synchronous Optical Network (SONET) equipment at 54 sites on the Korean peninsula.

  Actual: Funded Phase 1 (which includes upgrades at 15 sites) in preparation for work to start in FY17.

In FY17, network infrastructure modernization activities, as resources allow and in accordance with G-3/5/7 priorities, include:

- Installing and activating four of 11 NIPR JRSS CONUS sites and the remaining two (of four) Europe and SWA sites.
- Beginning installation of three (of five) Pacific NIPR JRSS sites.
- Installing and activating 25 SIPR JRSS CONUS/outside the continental United States (OCONUS) sites.
- Installing MPLS at 22 DSS sites.
- Continuing to increase throughput for ICANs at 20 CONUS sites, as well as in Europe and the Pacific.
- Continuing optical transport link upgrades at 22 sites.
- Completing Korea ATM/SONET Phase 1 and funding Phase 2 (15 sites).

By the end of FY18, as resources allow, the installation network infrastructure will be sufficiently modernized (i.e., bandwidth increased to 100 gigabits per second (gbps) between installations, and local bandwidth within the majority of prioritized installations increased to 10 gbps). This improvement is necessary to accommodate emerging applications and services offered by DoD-approved enterprise hosting facilities. Priority installations also will have physically diverse access to the DoD Information Network (DoDIN) communications backbone,

tremendously improving reliability and throughput for the user community. Greater network reliability and availability will enable the synchronization and support of garrison-based Home Station Mission Command Center (HSMCC) operations, as well as distributed live, virtual, constructive and gaming (L/V/C/G) training. It will also set the foundation for full integration with the JIE construct, to include the flexibility to scale throughput up or down based on network demand and available resources. Additionally, network infrastructure upgrades will ensure that the Army is positioned to adopt the Data Center/Cloud/Generating Force (DC/C/GF) Computing Environment, cloud-based enterprise business systems and unified capabilities (UC).

Dual-path diversity and infrastructure modernization will enable the removal of legacy switching equipment, thus reducing operating and sustainment costs. Building out the network transport infrastructure ensures that users can connect to requisite information at the point of need.

Consolidate Separate Networks

The consolidation of separate networks unifies the institutional and the tactical into one enterprise network, simplifying network management and reducing operation, maintenance, sustainment and modernization costs. It also ensures that all Army components can connect to enterprise services to access critical information.

A critical element of network consolidation is the migration behind DoD JRSS. Per a 2015 DoD CIO memorandum, the objective is for JRSS to provide security capabilities for all main DoD bases, posts, camps and stations classified as DSS locations by the end of FY19. Currently, the Army has 88 DSS locations. Migration efforts are depicted in Figure 3.

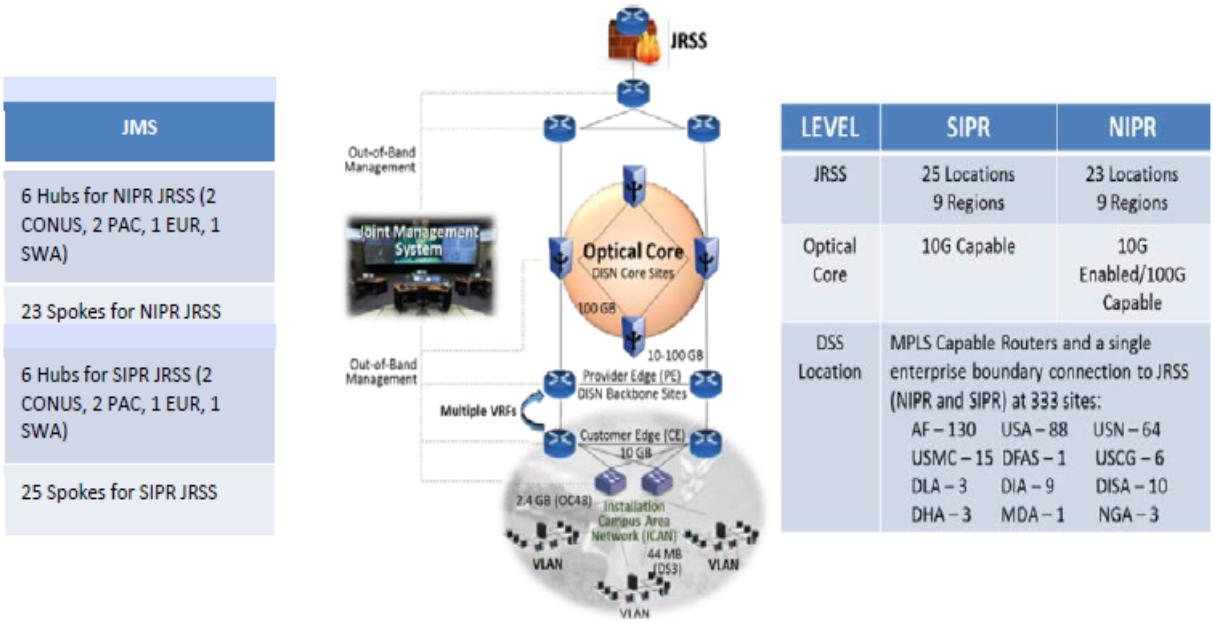


Figure 1-1: JRSS Structure, DSS Locations

In FY16, projected and actual accomplishments related to consolidating separate networks included:

- Projected: Continue to consolidate community of interest networks (e.g., USAR, Corps of Engineers, AMC and MEDCOM networks). Set the conditions for integration of

deployable network transport solutions into a unified information transport delivery capability. Confirm and publish tactics, techniques and procedures (TTPs) for the use of Wideband Global Satellite Communications (WGS) with Warfighter Information Network - Tactical (WIN-T) systems.

Actual: USAR migrated behind JRSS in the third quarter of FY16 and USAR traffic now traverses JRSS. Follow-on migration clean-up actions were completed in the fourth quarter of FY16. ARNG and the Corps of Engineers finished network discovery, and two private IP circuits were connected to JRSS at the Joint Base San Antonio Defense Enterprise Computing Center and the Defense Enterprise Computing Center in Montgomery, AL. Detailed technical procedures for the use of the WIN-T Network-Centric Waveform over the WGS architecture were published. (Funding reprioritization delayed network modernization initiatives, thereby directly impacting integration of separate networks.)

FY17 activities related to integrating separate networks include:

- Complete integration of community of interest networks (e.g., USAR, Corps of Engineers, AMC and MEDCOM networks).
    - Develop and coordinate memorandum of understanding with stakeholders for JRSS operations.
    - Complete coordination with appropriate stakeholders to develop suitable technical solutions, clearly defined and documented, to support integrating AMC, ATEC and IMCOM networks (especially the Defense Research and Engineering Network) in FY18.
- Set the conditions for integration of deployable network transport solutions into a unified information transport delivery capability.
- Transition network modernization efforts for Joint Management System (JMS) implementation from the NCD to the NSD.
- Confirm and publish TTPs for the use of WGS with WIN-T systems.
- Headquarters, Department of the Army (HQDA) G-3/5/7 plans to publish an execute order outlining roles and responsibilities for tactical network transport convergence.

In FY18, the CIO/G-6 and the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)) will complete consolidation of separate networks into the enterprise network and collaborate on Common Operating Environment (COE) implementation. Targeted installations will have one unified transport network, improving network efficiency and effectiveness. This unified network will facilitate faster data transfer, help to establish data standards, standardize network operations and security tools, and improve the cybersecurity posture, thereby ensuring seamless, secure operations from the enterprise to the tactical edge.

Improve Transport Capacity for Deployable Forces

The Army, in synchronization with DISA and joint network initiatives, will continue to enhance tactical network capabilities through the fielding of Capability Sets. Capability Set integration, which will occur in accordance with HQDA Execute Order 244-12, will incrementally enhance the throughput and agility of the tactical network, and extend the network further down into tactical formations. In FY17-18, planned capabilities include mission command on the move and enhanced command and control and situational awareness for the dismounted Soldier.

In FY16, the projected and actual accomplishments to improve transport capacity for deployable forces included:

- Projected: Field modernized Capability Sets to five Brigade Combat Teams (BCTs).

  Actual: In FY16, four BCTs received Capability Sets. The Army also completed WIN-T Increment 1B upgrades to all active and reserve component units (with the exception of two ARNG Expeditionary Signal Battalions (ESBs)).

In FY17, activities to improve transport capacity for deployable forces include:

- Conducting operational testing of WIN-T transportable tactical command communications (T2C2), and WIN-T Increment 2 Tactical Communication Node - Lite (TCN-Lite) and Network Operations and Security Center - Lite (NOSC-L).
- Completing the remaining two WIN-T Increment 1B upgrades (to two ARNG ESBs).
- Conducting initial operational test and evaluation of the Mid-Tier Networking Vehicular Radio.
- Continuing the operational evaluation of transport convergence at the BCT level.
- Finalizing HSMCC network support requirements.
- Continuing Capability Set integration for operational units, with two BCTs.
- Continuing HSMCC technical refresh/modernization and developing a life-cycle sustainment plan, in accordance with emerging requirements.
- Continuing to identify potential technology insertions or waveform enhancements to address emerging requirements (e.g., Net-Centric Waveform-Resilient to improve resiliency, spectrum improvements in Soldier Radio Waveform, Highband Networking Waveform improvements to support the Joint Aerial Layer Network, etc.).
- Completing Training and Doctrine Command (TRADOC) and HQDA staffing of the Regional Hub Node Annex to The Bridge to Future Networks Capabilities Production Document to support execution of programmed funding in FY17. Regional Hub Node upgrades will address the addition of X-band satellite communications, improving modem speed and capacity to support transport convergence efforts, T2C2, commercial gateway and Public Switched Telephone Network access for homeland security and civil support missions, and alignment with JRSS implementation.

In FY18, activities to improve transport capacity for deployable forces include:

- Continuing Capability Set integration in operational units, with two BCTs.
- Continuing to modernize tactical formations with WIN-T Increment 2 and Handheld Manpack and Small Form Fit Rifleman Radios through Capability Set integration.
- Beginning to field WIN-T T2C2, and WIN-T Increment 2 TCN-L and NOSC-L.
- Enabling garrison-based HSMCC operations by refreshing hardware in 26 units, including division, corps and select theater-level commands.
- Continuing to increase the Army's use of and reliance on the WGS and Mobile User Objective System (MUOS) satellite constellations to improve the efficiency of beyond line-of-sight communications. Recent follow-on operational test and evaluation results may delay fielding of MUOS until late FY18 at the earliest.

- Continuing upgrades and modernization efforts at Regional Hub Nodes (RHNs) based on available funding.

Tactical network modernization, along with greater bandwidth and reliability, will ensure that all communication forms (e.g., voice, video and data) are available to support operations, as well as all warfighting functions that include information-based activities. The transport capacity upgrades listed above will ensure more reliable and versatile on-the-move tactical communications in support of expeditionary mission command. They also will improve connectivity between the lower and upper tactical Internet, increasing commander capabilities at all levels to collaborate with units distributed across diverse locations. WGS and MUOS will help reduce the cost of training, while the integration of separate transport networks will expand the reach and agility of the deployable transport infrastructure. Continuing to modernize RHNs as part of the evolution of WIN-T will ensure connectivity between the deployed tactical network and the enterprise cloud, greatly enhancing access to requisite information at the point of need. New capabilities will be integrated within each RHN facility in support of the three phases of Army transport convergence and homeland defense/civil support guidance.

Modernization of deployable units with enhanced Capability Sets will give tactical users greater situational awareness and speed, better inform decision making and enable all aspects of information-based warfighting functions, to include warfighter reach-back to home-station command posts, as needed. As Capability Set integration occurs in accordance with G-3/5/7 priorities, key equipment will be reallocated to units with older systems scheduled for sunset, thereby improving the modernization level of a greater portion of the force.

Data Center and Application Consolidation and Standardization

The Army will implement the Office of Management and Budget's (OMB) Data Center Optimization Initiative (DCOI), dated 1 August 2016, and DoD guidance supporting DCOI. (The August 2016 DCOI supersedes the February 2010 Federal Data Center Consolidation Initiative.) New DCOI objectives include consolidating or closing 25 percent of the Army's tiered data centers and 60 percent of its non-tiered data centers by the end of FY18. In addition, per the 11 July 2013 DoD CIO memorandum titled *Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration*, the Army will continue efforts to reduce the number of Installation Processing Nodes (IPNs) to one per Base/Post/Camp/Station (B/P/C/S) by the end of FY18.

Secretary of the Army Directive 2016-38 (Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers) establishes an implementation plan for a range of actions necessary for the Army to rationalize and modernize IT systems and applications, migrate them to approved hosting environments, and close and consolidate data centers. The directive provides the means for the Army to achieve its FY25 data center end state, including a detailed data center basis of issue plan that identifies the type and number of data centers authorized at each Army installation at the end of FY25. It also provides a data center closure schedule for FY17 and FY18 (and beyond) that supports the Army's achieving DoD data center closure goals. In addition, the directive identifies four CONUS Army Enterprise Data Centers (AEDCs). In FY17 and FY18, the Army will begin to standardize these AEDCs, which will offer an Army-wide enterprise hosting solution. The directive sets application rationalization and migration timelines, as well, to support DoD's FY18 goals.

The directive also establishes the Migration Implementation and Review Council (MIRC) as a senior-level governance framework chaired by the Deputy Chief Management Officer and the Deputy CIO/G-6. The purpose of the MIRC is to ensure Army-wide compliance with the Secretary of the Army directive, including command accountability for meeting specified timelines, schedules and tasks. The MIRC is subordinate and reports to the Army Enterprise Network Council (AENC).

Commands must holistically analyze, prioritize and plan enterprise-hosting resourcing requirements. Resources currently identified for refresh of existing hardware and major software upgrades will serve as the base for covering migration and virtualization costs. CIO/G-6 will continue to assist commands with migration of applications through the Army Application Migration Business Office or similar capabilities in FY17-18. The Acquisition, Logistics and Technology Enterprise System and Services Data Center is designated as a modernization hub for Army commands and is available to facilitate Army application modernization support, as well.

The Army's application and data center consolidation efforts will ensure alignment with the JIE. Through rationalization, modernization and virtualization of applications, Army mission areas will identify unnecessary overlap in IT capabilities and eliminate applications in their portfolios. Shrinking the data center and network footprint will improve the Army's cybersecurity posture, increase efficiency, reduce life-cycle sustainment requirements and simplify IT capabilities.

Also by the end of FY17 the Army will:

- Establish the standard DC/C/GF Computing Environment baseline and plan in accordance with the COE, which enables JIE concepts, supports Installation Service Node implementation, supports Global Enterprise Fabric (GEF) deployment, facilitates cloud capability, enforces Army and DoD guidelines, and reinforces joint force interoperability.
- Begin establishing CONUS AEDCs at Fort Bragg, Fort Carson, Fort Knox and Redstone Arsenal, with a goal of all four accepting enterprise applications in FY17.

The Army continues to adjust its IT infrastructure modernization efforts with a cloud-based computing and storage approach. Transitioning to the cloud environment remains a complex endeavor that requires enterprise-wide planning and coordination in the areas of infrastructure, people and processes. The Army is addressing these complexities by continuing to focus on four strategic imperatives and associated objectives.

- Adopt Cloud Governance and Management Practices
- Instantiate Cloud Computing Capabilities within the Army Network
- Manage the Modernization and Migration of Applications, Systems and Data
- Secure and Manage Cloud Operations

The Army also is participating in two distinct pilots for hosting Army applications through cloud service offerings (CSOs). The first pilot focuses on hosting several applications in off-premises commercial CSOs, while the second focuses on establishing and evaluating an Army private cloud. The Army Private Cloud Enterprise (APCE) pilot, which will continue into the FY19-23 timeframe, is a commercially owned/commercially operated (COCO) CSO on premises in a government facility on Redstone Arsenal, Alabama. The APCE pilot initiative will

systematically test, evaluate and refine the Army's acquisition, management and operations approach to a COCO-based private cloud before Army-wide adoption.

Through these pilots, the Army will be able to determine whether:

- Existing policies, procedures and infrastructure are sufficiently mature to support an easy transition from hosting systems and application in a government enterprise data center environment to either a DISA or commercial off-premises cloud environment.
- The Army, working with its DoD and commercial cloud partners, must continue to refine and align its policies and procedures for network security and establish enabling infrastructure in order to better support the system/application migration associated with data center consolidation and the COE's DC/C/GF Computing Environment.

End-User Services (EUS)

As the Army's interest in and demand for mobility grows, the NCD will focus on development of a robust network infrastructure that complements and supports the overarching Mobile Vision document.

In FY16, projected and actual EUS accomplishments included:

- Projected: Develop an EUS Strategy to define requirements for a common EUS environment. Finalize the End-User Device (EUD) Reference Architecture. Begin implementation of the decisions drawn from Commercial Off-the-Shelf IT Working Group recommendations.

  Actual: Finalized the EUD Reference Architecture, which was signed in January 2016.

In FY17, EUS activities include:

- Supporting development of the Mobile Vision document.
- Identifying and beginning implementation of adjustments to the installation and deployable network infrastructure components necessary to support the mobile aspect of EUS.

By the end of FY18, the Army will standardize procurement of infrastructure that supports unclassified and classified information sharing via voice, video and data. The Mobile Vision document will ensure that the Army is on a modernization path that keeps pace with the rapidly changing technology environment.

Divestiture Planning

Network infrastructure modernization advances the identification and divestiture of unneeded legacy equipment. This will free up life-cycle sustainment resources, which may be made available to help the Army meet its operational and modernization objectives in a resource-constrained environment.

In FY16, projected and actual divestiture accomplishments included:

- Projected: Implement divestiture plans for unneeded legacy circuits, switches and servers through fielding of MPLS and JRSS in CONUS, SWA and Europe. Develop and implement, as new equipment migrates to the enterprise infrastructure, divestiture plans for unneeded command local area networks, wide area networks and transport infrastructure that support dedicated video teleconference (VTC) networks. Develop and

implement divestiture plans for unneeded servers and storage pods as commands migrate and virtualize applications and data to the appropriate hosting facilities. Continue divesting Single Channel Ground and Airborne Radio System (SINCGARS) Models A through D.

Actual: Established a Divestiture Planning and Network Modernization Clean-Up Working Group and drafted a divestiture policy. Developed a matrix of divestiture sources and corresponding triggers.

In FY17, divestiture activities include:

- Implementing divestiture plans for obsolete circuits, switches and servers replaced by MPLS and JRSS in CONUS, SWA and Europe.
- Developing and implementing divestiture plans for unneeded infrastructure that supports VTC networks as commands migrate to the enterprise infrastructure.
- Developing and implementing divestiture plans for unneeded servers and storage pods as commands virtualize and migrate applications and data to appropriate hosting facilities.
- Developing and implementing divestiture plans for unnecessary legacy telephones and Time Division Multiplexing (TDM) network switches as the Army migrates to VoIP.
- Divesting SINCGARS Models A through D (to be completed no later than FY18).

In FY18, divestiture activities include:

- Implementing divestiture plans for unneeded circuits, routers, legacy switches and servers replaced by MPLS and JRSS in Pacific Command, European Command and Africa Command.
- Continuing implementation of divestiture plans for unneeded infrastructure that supports VTC networks.
- Continuing implementation of divestiture plans for unneeded servers and storage pods as commands virtualize and migrate applications and data to appropriate hosting facilities.
- Implementing divestiture plans for the Enhanced Position Location Reporting System, supplanted by fielding Joint Battle Command – Platform to BCTs (to be completed no later than FY18).

Three new factors will enable the start of legacy equipment divestiture, including: activation of the MPLS global network, installation of Voice Local Session Controllers and the enterprise VoIP offering from DISA. The first two Army posts are scheduled to decommission their legacy equipment in FY17, and divestiture activities are now fully initiated for Army organizations in Europe, the Pacific and Africa. By the end of FY17, the Army will start to remove unnecessary equipment from the network in CONUS and SWA.

As enterprise infrastructure and services are operationalized, commands and portfolio managers will identify additional legacy solutions for migration to the enterprise solution.

Appendix 2 – Enterprise Services Domain (ESD)

The ESD's primary goal is to ensure that the Army has the capability to share information, provide core enterprise services and determine accurate position, navigation and timing (PNT). Initiatives supporting this portfolio must be easy to use, integrated, globally available and adaptable, and support all mission areas (Warfighting, Business, DoD Intelligence and Enterprise Information Environment). Figure 4 below shows the major Army imperatives and their associated outcomes, and the three associated Joint Capability Areas (JCAs).

1. Information Sharing (6.2.1) – 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.
2. Core Enterprise Services (6.2.3) – The ability to provide awareness of, access to and delivery of information on the DoD Information Network (DoDIN) via a small set of CIO-mandated services.
3. Position, Navigation and Timing (6.2.4) – 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.

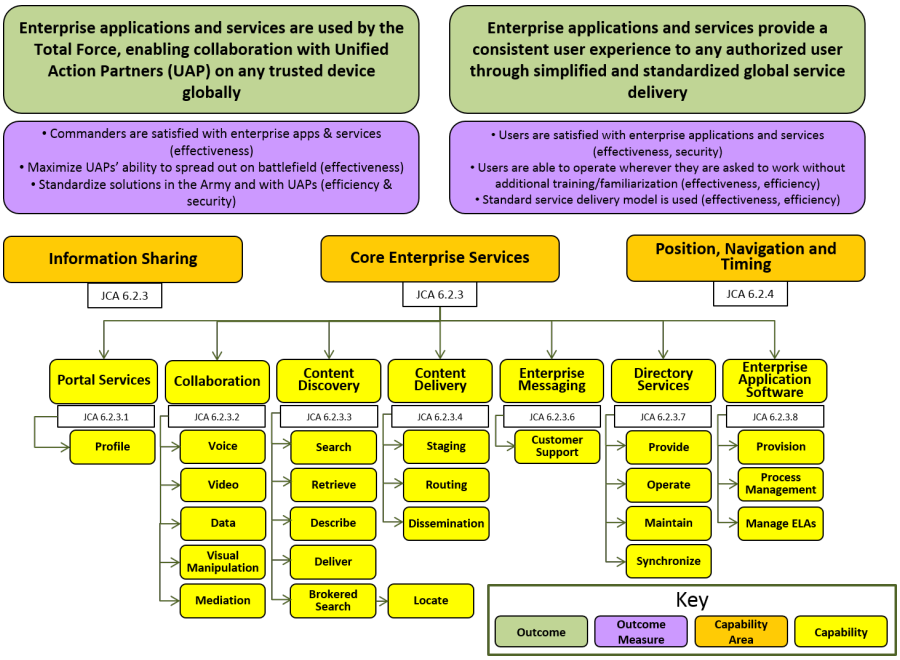


Figure 2-1: Enterprise Service Capability Areas

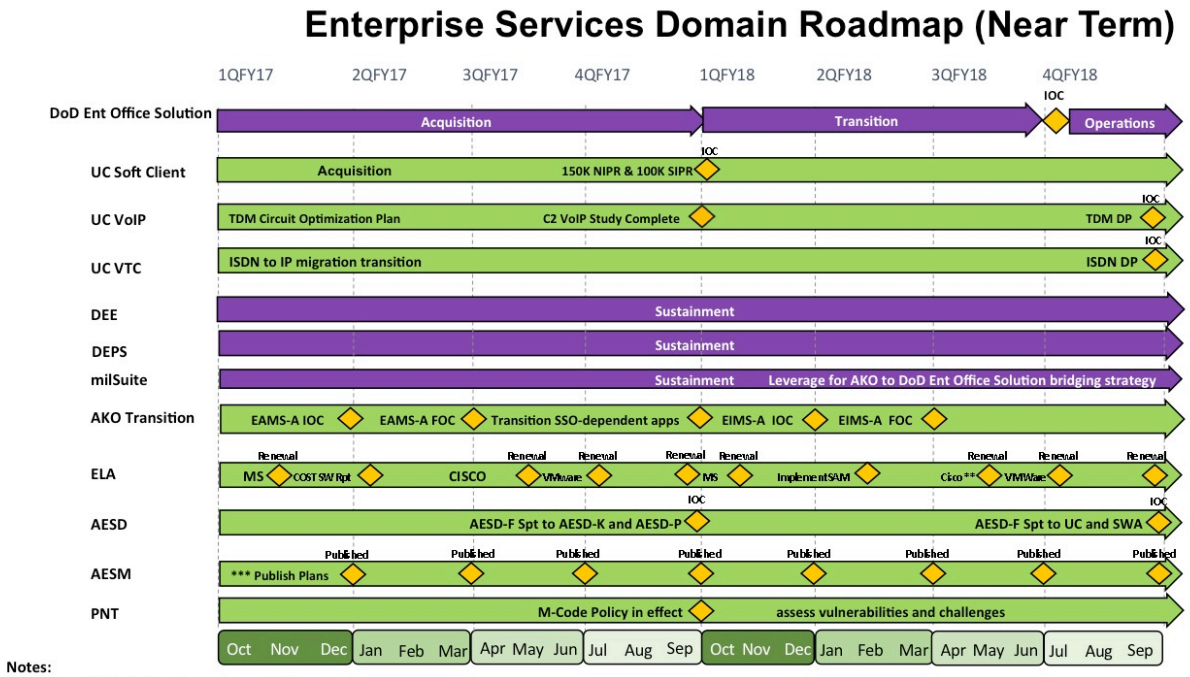
FY17-18 Priority Activities

The ESD will produce five outcomes in FY17-18.

1. Deliver unified capabilities (UC) to the force.
2. Publish a transformation strategy for Army Knowledge Online (AKO).
3. Award contracts for enterprise licenses for several key software products.

4. Improve the quality, lower costs and raise productivity of the Army Enterprise Service Desk (AESD).
5. Mature the delivery of information technology (IT) services.

Figure 2-2 below shows the major ESD portfolio initiatives that support the domain's strategy roadmap for the next two years. These initiatives include UC, DoD Enterprise Email (DEE), DoD Enterprise Office Solution (DEOS), DoD Enterprise Portal Services (DEPS), milSuite, AKO transition, enterprise license agreements, AESD, Army Enterprise Service Management (AESM) and PNT.



Notes:
* Software: BMC, Adobe, Symantec and CA
** Note: FY19 Last option year for Cisco JELA
*** Note: ARCYBER will publish FRAGOs to OPORD 2015-367 specifying which Process and Service Management Plans are to be published

Figure 2-2: ESD Near-Term Roadmap

Unified Capabilities (UC)

UC is the Army's approach to enabling universal collaboration to increase warfighter and business community mission effectiveness. UC will provide integrated voice, video and data services that are delivered ubiquitously across a secure and highly available network infrastructure, "independent of technology."[a] UC will interoperate with deployed elements of the network and associated mission command capabilities to move the Army towards a common user experience. A "common user experience" is the notion that employment of the mission command network should not change radically across echelons, formations or phases of the operation, whether the user is deployed or at home station. It should facilitate the transmission of the information warfighters require, regardless of echelon, at the point of need.

[a] *Department of Defense (DoD) Unified Capabilities Master Plan (UC MP), October 2011.*

ESD has developed three lines of effort (LOEs) for this initiative: deploying a limited UC soft-client institutional solution, transitioning to Voice over IP (VoIP) and transitioning to IP video teleconference (VTC). See Figure 2-3 below.

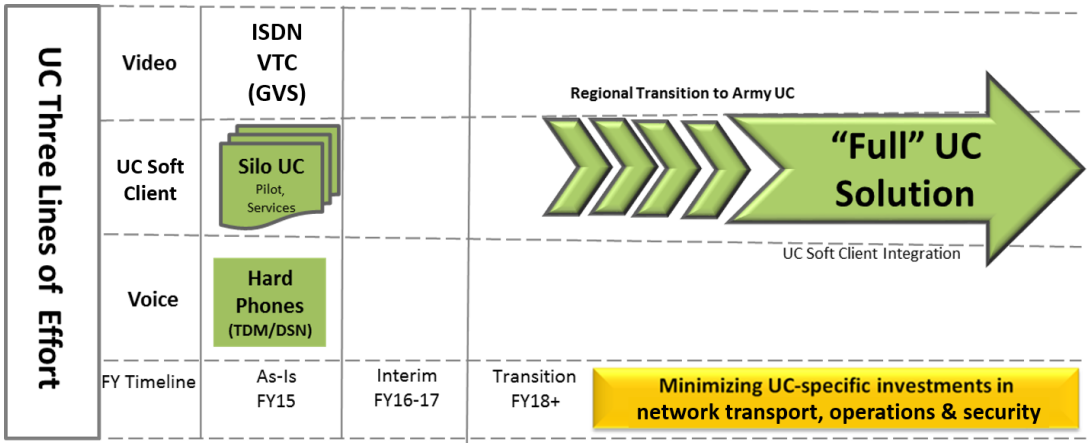


Figure 2-3: UC LOEs

By focusing on these three LOEs, the Army will reduce its reliance on expensive legacy analog telecommunications and disparate collaboration solutions, strengthen its security posture and begin to reap cost savings/avoidance through divestiture.

The Army will not decommission legacy systems, such as Defense Collaboration Services, until soft client and hardware upgrades for voice (e.g., VoIP phones) and IP VTC (e.g., Global Video Services) are fielded.

In FY16, the Army continued materiel solution development by validating requirements, completing the UC Concept of Operations (CONOPS) and conducting an analysis of alternatives. Army commands continued migration of Integrated Services Digital Network (ISDN) circuits to IP VTC. Chief Information Officer/G-6 (CIO/G-6), Network Enterprise Technology Command (NETCOM) and Program Executive Office Enterprise Information Systems (PEO EIS) developed the architecture, requirements and implementation plan to deploy assured voice services in conjunction with the non-assured voice services provided by the UC soft client. This will allow NETCOM to divest Time Division Multiplexing (TDM) switches and migrate services to IP. Based on the UC CONOPS, CIO/G-6 stood up an integrated project team (IPT), and developed and assigned tasks to IPT members for planning the TDM to IP transition. The Army evaluated an office productivity software suite to assess how this solution could support the Army's UC efforts and improve daily business processes. The Army also analyzed, and planned for the consolidation of disparate legacy communications solutions in order to enhance and simplify the user experience. At the end of FY16, the Army released a request for proposals to procure a UC soft client service.

In FY17, the Army intends to award a contract for the UC soft client and begin fielding. Initial operating capability (IOC) will meet threshold requirements for voice, video, instant messaging/chat, presence and desktop (screen) sharing for 150,000 unclassified users and 100,000 classified users. At IOC, the UC soft client service will comply with Level 5 and Level 6 security requirements, as described in the Cloud Computing Security Requirements Guide. The initial 150,000 unclassified users will be located in the southwest region and correspond to the

Network Modernization CONUS (NETMOD-C) schedule. A signed TDM-to-IP transition plan, including a business case analysis and DoD use case analysis report, is anticipated by the third quarter of FY17. Once developed, the Army Mobile Vision document will also help shape the mobility capabilities provided to users by the UC initiative. By the end of FY17, limited deployment of the UC soft client will be under way, and plans will be in place to scale across the remainder of CONUS, Southwest Asia (SWA) and U.S. Army Pacific. UC IOC is expected by the end of FY18.

DoD Enterprise Email (DEE)

DEE is DoD's primary secure email capability for both unclassified and classified networks, and is now in sustainment. Experience with DEE has identified a number of shortfalls, and the Army wants to enhance its email and messaging capabilities. The Defense Information Systems Agency (DISA) is currently engaged in the acquisition cycle to replace DEE with an email capability (and UC) that will be part of the DoD Enterprise Office Solution (DEOS) or another DoD enterprise offering. The rate structure of the replacement offering (the Army pays DISA for its email service) will be a significant driver as the Army looks for newer messaging capabilities.

In FY16, DEE provided unclassified and classified email service to 1.4 million Army customers. In FY17, the Army will closely monitor and participate in preparations for transition from DEE to an alternate (either DoD or commercially provided) solution. The Army must make an informed decision based on the capabilities and costs of all enterprise offerings to determine which, if any, will be used as full or partial solutions. The Army anticipates that DISA will complete its award for DEOS or another DoD enterprise offering in FY18, and will reach IOC prior to the end of the fiscal year. Once IOC is achieved, the Army will conduct an analysis to determine the feasibility of transitioning DEE services.

Army Knowledge Online (AKO) Transition

AKO is the Army's web-based intranet service. Built on an integrated suite of software, AKO provides a secure portal, a global directory, file storage and a single sign-on (SSO) service. In keeping with guidance to decrease spending and tighten security, the infrastructure supporting AKO is being upgraded. As part of these improvements, the Army is leveraging cloud-based hosting solutions, implementing a new bridging strategy, and taking advantage of emerging initiatives. There will be no loss or degradation in services provided to users during the transition.

In FY16, the Army began migrating AKO SSO to a DoD cloud-based service. The Army estimates the migration will be completed by the end of FY17.

After migration of AKO SSO to a DoD cloud-based service is finished, the Army will implement an enterprise identity management service. IOC is expected by FY18.

milSuite

milSuite is a DoD online portal that provides information management, professional networking, asynchronous collaboration, and innovation and search capabilities to all DoD members who have a Common Access Card (CAC), including active duty military, civilians, Army National Guard (ARNG), U.S. Army Reserves (USAR) and contractors. milSuite leverages best-of-breed social business technologies and principles, such as transparency, crowd-sourcing and

innovation, that have enabled more than 750,000 DoD personnel to better execute their missions, solve critical problems, connect with others and manage their information and files.

milSuite's integrated suite of commercial off-the-shelf (COTS) and open source products meets some of the Army's information management requirements, with web-based enterprise information services for team collaboration, content management, Web 2.0, search and discovery, portal and profiles, and asynchronous collaboration (JCA 6.2.2.2).

In FY16, milSuite released a major upgrade in milBook 6.0, which added new features, such as a "Streams" page to showcase custom and global streams (i.e., the new "Bloggers" stream), the "Your View" feature, new "Place" pages, the ability to follow a tag and more tiles to display useful information, all in a mobile-ready package. Major upgrades were made to the milSuite directory for user auto-registration, dynamic account updating upon login, smart time-out session warnings and weekly account updates from milConnect. A new homepage was also added, including an improved user account page supporting quick and easy real-time profile data updating and viewing of others across milSuite. New analytics capabilities were included to provide real-time user stats, and widgets were added to create reporting dashboards. At the infrastructure level, milSuite is currently working with DISA on phase 4, wherein they will expand log management capabilities, caching, login procedures and file storage capabilities.

In FY17, milSuite will offer users the ability to connect to SharePoint, allowing complementary features and shared access to content, such as DEPS and AES. It will also provide lightweight survey capabilities to complement existing polling features, expand milUniversity for wider use and schedule quarterly releases that add functionality to milSuite products. Finally, the milSuite infrastructure will begin preparing for a potential FY18 migration to leverage approved cloud hosting environments.

Enterprise License Agreements (ELAs)

ELAs allow the Army to make bulk purchases, providing a stronger negotiating position and decreasing the cost of productivity-enhancing software solutions. By having a centralized purchasing process and capitalizing on economies of scale, ELAs allow the Army to negotiate additional value-added services, such as training, and reduce the total cost of ownership. The Army will continue to work closely with DoD partners to ensure alignment with JIE strategies and the Better Buying Power initiative.

In FY16, CIO/G-6 analyzed a license inventory data call for Microsoft, Adobe, VMware, BMC Software, Brocade and Veritas. The Army renewed ELAs for Microsoft, Cisco, VMware, BMC Software, Adobe, Symantec and CA Technologies products. (These ELAs are renewed annually until all option years are executed unless determined otherwise.) Additionally, non-ELA contracts were established, including Microsoft customer support agreements, a Microsoft Premier Support Contract and Gartner Research. A Windows 10 consulting contract also was awarded.

In FY17, the Army will establish a new ELA with Microsoft and will identify opportunities for other new ELAs. The Army also will implement a software asset management tool to ensure a successful audit of internal use software, as directed in the Fiscal Year 2016 National Defense Authorization Act.

In FY18, the Army's Cisco ELA will be in its final option year, requiring a re-compete of the contract.

Army Enterprise Service Desk (AESD)

Commanders and staffs of both operating and generating force units lack sufficient access to critical network outage and trend analysis data to effectively execute missions while maintaining reliable communications. The Army is burdened with standalone installation, organization and service desk solutions that provide Tier 0 and Tier 1 support functions. This situation has impeded interoperability, process normalization, information sharing, cost accounting and centralized analysis of call center metrics, incidents and problems (where there are multiple points of contact for service support).

AESD was initiated to solve these issues by creating a single designated point of contact for IT support across the Army network. AESD is the Army's premier Tier 1 service desk, providing desktop support to users 24 hours a day, seven days a week, 365 days a year. It is an essential part of LandWarNet and supports enterprise service provisioning, including services provided by NETCOM, AKO and others. AESD began with CONUS-based support for initial enterprise services, such as AKO, DEE and local command, control, communications, computers and information management services for 7th Signal Command. This chartered AESD organization is currently known as AESD-Worldwide (AESD-W), with a Secure IP Router (SIPR)-based support element known as AESD-W-SIPR.

In order for the AESD program to provide additional theater-level service desk functions and centralize the reporting and analysis of incidents and performance metrics, the service desks aligned to the five Regional Cyber Centers (RCCs) in CONUS, Europe/Africa, SWA, the Pacific and Korea, as well as select command service desk functions, were joined into the AESD Federation (AESD-F) in 2015. AESD-F currently has 13 members (12 service desk members and the Program Office); it supports 568,000 DEE users and more than 1.9 million AKO end users worldwide.

The AESD-F (see Figure 2-4 below) currently consists of the following.

- AESD-Program Office (AESD-PO), which supports AESD and conducts acquisition activities.
- Desks operated by NETCOM.
    - AESD-Europe (AESD-E), which supports organizations in Europe and Africa under 5th Signal Command (Theater) (SC(T)). It is closely aligned with RCC-Europe.
    - AESD-SWA (AESD-S), which supports organizations in SWA under 335th SC(T). It is closely aligned with RCC-SWA.
    - AESD-Pacific (AESD-P), which supports organizations in the Pacific under 516th Signal Brigade, 311th SC(T). It is closely aligned with 4th RCC (PAC). This desk has been virtualized across the three major Network Enterprise Centers (NECs) within 516th. AESD-PO will establish a centralized AESD-P capability starting in FY17.
    - AESD-Korea (AESD-K), which supports organizations in Korea under 1st Signal Brigade, 311th SC(T). It is closely aligned with 6th RCC (Korea). This desk has been virtualized across the two major NECs within 1st Signal Brigade. AESD-PO will establish a centralized AESD-K capability in FY17.

- Desks operated by other commands.
  - Joint Service Provider, which supports organizations in the National Capital Region.
  - AESD-Guard (AESD-G), which supports the ARNG.
  - AESD-Reserve (AESD-R), which supports the USAR.
  - AESD-MEPCOM (AESD-MP), which supports the Military Entrance Processing Command.
  - AESD-USAREC, which supports Army Recruiting Command.
  - AESD-MEDCOM (AESD-M), which supports Army Medical Command and the Defense Health Agency (DHA).
  - AESD-Tactical (AESD-T), which supports tactical requirements for fielded systems and tactical users.
  - AESD-W, operated by PEO EIS, which supports enterprise services worldwide and local NEC services within CONUS for 7th SC(T).

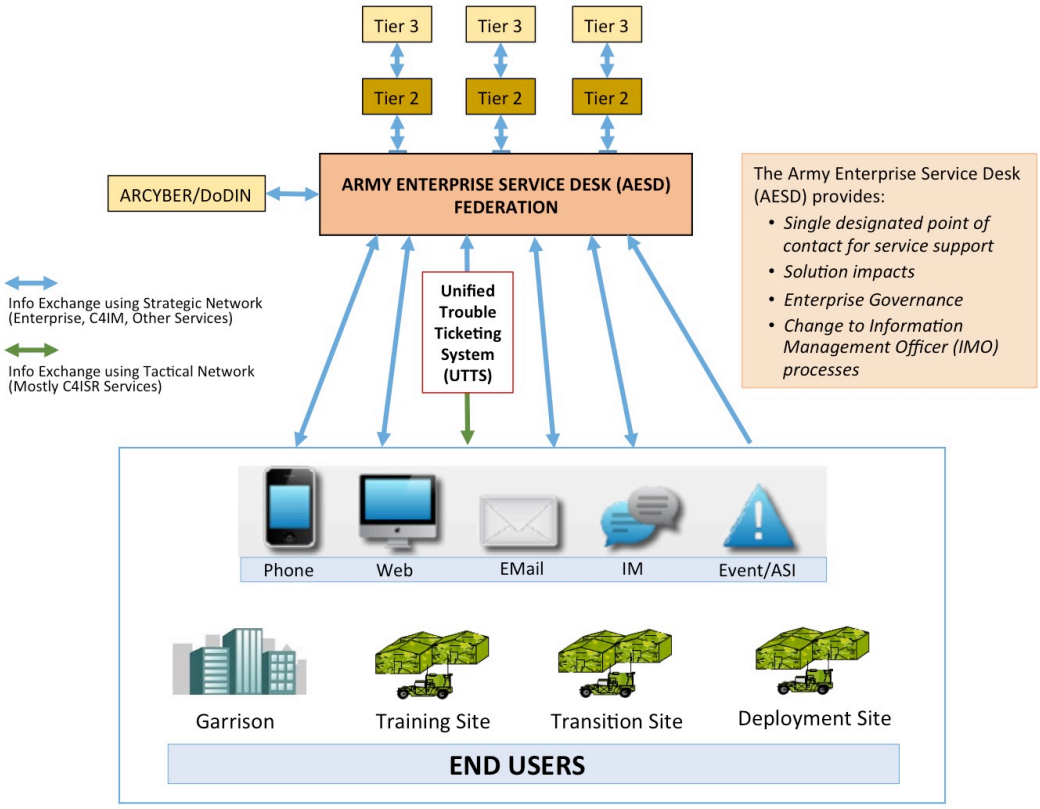


Figure 2-4: AESD Capability

Adding service desk support functions to the AESD-F is determined by the CIO/G-6 on a case-by-case basis. CIO/G-6 has requested that support from command application service providers be aligned within the AESD-F and/or that they migrate to AESD-W for user support where possible in FY16-19.

In FY16, AESD-F continued to support DEE, mobility and AKO. Individual Federation desks also supported their specific communities of interest. The AESD-F Information System

Capability Development Document (IS CDD) and business case analysis were submitted to Training and Doctrine Command (TRADOC) for final review prior to Army-wide staffing in the first quarter of FY17. An Army Research Lab (ARL) study was initiated to identify AESD-F reporting, force structure and technical requirements, and was used to update the AESD-F CONOPS at the end of FY16. The AESD-PO visited, and prepared designs for supporting, the Pacific and Korea theaters. It also initiated planning to support U.S. Southern Command (SOUTHCOM), Windows 10, UC and future services based on Joint Regional Security Stack (JRSS) deployment. AESD-W completed an operational validation of NETCOM's BMC Remedy 8.1 implementation and continued to support 7th SC(T) in the migration to Remedy 8.1 for local NEC services support. AESD-W also finished security control assessment verification and prepared to deploy improved enterprise services ticketing, user portal and business-to-business (B2B) ticket exchange capabilities in the first quarter of FY17.

In FY17, AESD-F will continue operations for DEE, mobility and AKO. It will begin to implement AESD-F reporting and force structure improvements per recommendations from the ARL study. It also will start to use the B2B capability for exchange of information between DISA and itself. The AESD-PO will develop a service desk services vehicle to enable AESD-F business process and technology improvements per the AESD-F IS CDD. The AESD-PO will go live with Pacific and Korea service support as part of AESD-F. It also will begin Windows 10 support, further develop SOUTHCOM, UC and JRSS support, and initiate planning for SWA service support. AESD-W will continue support to 7th SC(T) for local NEC services; AESD-P and AESD-K will provide similar local NEC services support to 311th SC(T) in the Pacific and Korea theaters and AESD-E to 5th SC(T) in Europe and Africa.

In FY18, AESD-F will continue operations for DEE, mobility, Windows 10 and AKO. The AESD-PO will go live with UC, SOUTHCOM and SWA service support as part of AESD-F. It also will begin to deploy business process and technology improvements for analytics, knowledge management and ticketing to AESD-F per the AESD-F IS CDD. Additionally, the AESD-PO will start development of self-reporting tools for the desktop, begin to federate and certify information management officers (IMOs), and merge IMOs into the AESD-F workforce and business processes. AESD-W, AESD-E, AESD-P, and AESD-K will continue support for 7th SC(T), 5th SC (T), 311th SC(T), and SOUTHCOM for local NEC services while being joined by AESD-S supporting 335th SC(T) for SWA.

Army Enterprise Service Management (AESM)

AESM is the means by which the Army will manage IT service delivery. AESM uses an integrated, holistic management approach based on best business practices as delineated in the DoD Enterprise Service Management Framework. Figure 2-5 below, AESM Life Cycle, describes the five life-cycle stages comprising the AESM Framework (AESMF), including 32 supporting processes and functions. The objective of the AESMF is to continually increase effectiveness, improve security and gain efficiencies in Army IT services by standardizing the service delivery process.

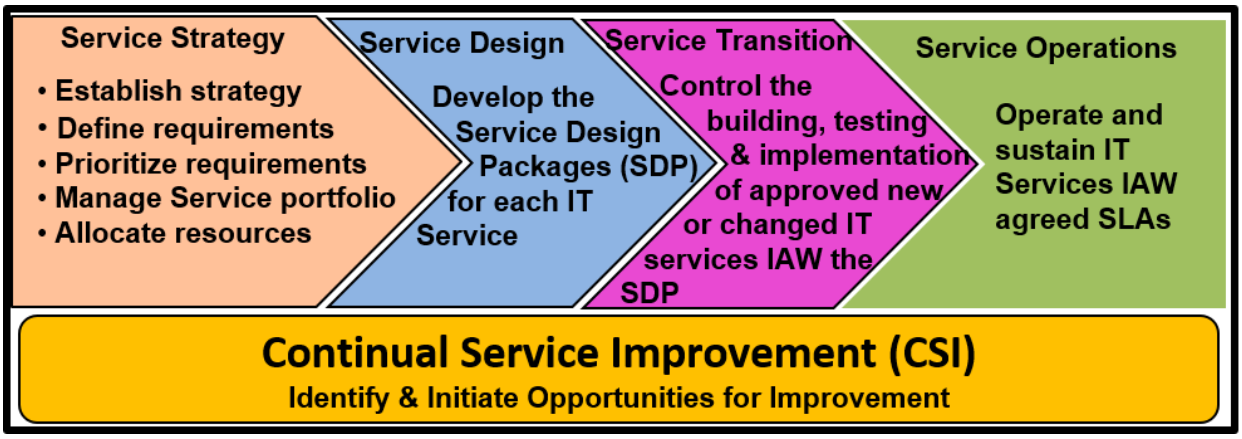


Figure 2-5: AESM Life Cycle

In FY16, Army Cyber Command (ARCYBER) and Second Army published AESM Implementation Operations Order (OPORD) 2015-367, which establishes the pace at which the Army will implement the IT service management (ITSM) policy. The OPORD lays out a phased approach based on current IT service and process priorities. The major tasks for implementing AESM are: 1) appoint process owners; 2) appoint service owners; 3) appoint service managers; 4) publish process management plans; 5) publish Service Design Packages; 6) publish service management plans; and 7) publish and execute the AESM Assessment Plan. In FY16, the Army completed the following.

1. Appointed process owners for:
   a) Configuration Management
   b) Service Knowledge Management
   c) Access Management
   d) Release and Deployment Management
   e) Service Level Management
   f) Incident Management
   g) Event Management
   h) Request Fulfillment
   i) Problem Management
2. Appointed service managers for:
   a) Email
   b) Desktop Services
   c) Telephone VoIP
   d) NIPRNet VTC Studio Services
   e) Public Key Infrastructure (PKI)

3. Published draft process management plans for:
    a) Change Management
    b) Service Desk
    c) Capacity Management
    d) Continual Service Improvement

AESM priorities for FY17-18 will be issued via fragmentary orders (FRAGOs) to ARCYBER and Second Army OPORD 2015-367 and shall include timelines for:

1. Publishing process management plans for:
    a) Release and Deployment
    b) Service Level Management
    c) Incident Management
    d) Event Management
    e) Request Fulfillment
    f) Problem Management
    g) Availability Management
    h) Service Catalog Management
    i) Asset Management
    j) IT Service Continuity
    k) Service Validation Testing
    l) Application Management
    m) IT Operations Function
    n) Tech Management Function
    o) Information Security Management
    p) Strategy Generation Management
    q) Demand Management
    r) Business Relationship Management
    s) Financial Management
    t) Service Portfolio Management
    u) Design Coordination
    v) Supplier Management
    w) Change Evaluation
    x) Engineer Function
    y) Transition Planning Support

2. Publishing Table G-1 final Service Design Packages for:
   a) VTC
   b) PKI
   c) Visual Information (VI)
   d) UC
   e) Messaging
3. Publishing draft service management plans for:
   a) VTC
   b) PKI
   c) VI
   d) UC
   e) Messaging
4. Publishing and executing the AESM Assessment Plan, using the following business rules.
   a) In the second quarter of FY17, publish the AESM Assessment Plan specifying how all assessments will be accomplished, and notify process and service owners of their schedules.
   b) Target eight process assessments a year (two per quarter) to support a three-year assessment cycle for all processes.
   c) Target one to two service assessments a year to support a three-year assessment cycle for all services.

FY17-18 Position, Navigation and Timing (PNT) Priority Activities

Providing accurate PNT is critical to the mission success of the Army's many assured PNT systems, to include precision munitions and Blue Force Tracker. Currently, the primary source for PNT is the Global Positioning System (GPS). GPS is entering a modernization phase that will offer greater jamming resistance for military users and performance enhancements for both military and civilian users. A major element of this modernization is the development of GPS Military Code (M-Code), designed to protect military users while preventing hostile use of GPS. M-Code complies with public law, which prohibits purchasing GPS equipment after FY17 without M-Code capabilities, unless the Secretary of Defense grants a waiver.

In FY16, the Army sustained its PNT investments and developed language to support new policy requiring M-Code capability on military GPS purchases.

In FY17, the Army intends to finalize the M-Code transition strategy, and to assess vulnerabilities and challenges in current and future material solutions. In FY18 and beyond, shortfalls will be addressed through Soldier training and preparedness plans.

Appendix 3 – Network Operations and Security Domain (NSD)

The Network Operations and Security Domain is responsible for ensuring that network operations and information technology (IT) security investments support the Army's vision, mission and goals. The NSD will select the best mix of IT investments in the domain to produce efficient and effective delivery of capabilities to the warfighter.

NSD capabilities will be measured, assessed for effectiveness, and managed relative to contribution to mission outcomes, strategic goals and objectives (in accordance with §§11103 and 11313 of Title 40, United States Code), per Department of Defense (DoD) Instruction 8500.01, para 3.e.(3).

The overarching guidance for the NSD in the FY17-18 timeframe is to meet the core mandated cybersecurity requirements from DoD, the Chairman of the Joint Chiefs of Staff and the Army. The NSD's primary goal is to provide a secure, seamless and continuous network environment with protected critical data and information in support of the Army and unified action partners (UAPs). The following objectives, taken from DoD guidance, support that goal.

- Achieve interoperability by ensuring adherence to DoD architecture principles and standards while managing all interconnections of Army IT to minimize shared risk and ensure that the security posture of one system is not undermined by vulnerabilities of interconnected systems.
- Standardize IT tools, methods and processes to the greatest extent possible to eliminate duplicate costs and to focus resources on creating technologically mature and verified solutions.
- Ensure strong identification and authentication, and eliminate anonymity in DoD IT.
- Identify and integrate qualified cybersecurity personnel into all phases of the system development life cycle.
- Protect information in electronic format with the appropriate levels of confidentiality, integrity and availability in a manner that balances the need for information sharing and security.

There are 18 initiatives (see Table 3-1 below) in FY17-18 that will enhance the network security posture and network management, and improve information sharing, with the objective of achieving the following outcomes.

- Networks and information are accessible, interoperable and protected against threats (data, hardware and software).
- Authorized users can effectively execute their missions by leveraging network capabilities.

FY17-18 Priority Activities

FY17-18 NSD Activities	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 Network	
Network Modernization – Joint Regional Security Stacks (JRSS), Joint Management System (JMS), Multi-Protocol Label Switching (MPLS), Installation Campus Area Network (ICAN)	•				•	
Provisioning Convergence	•					
Organize and Advance Mobility				•		
Transition to Key Management Infrastructure (KMI)				•		
Enhance Identity and Access Management				•		
Refine the Cyberspace Workforce					•	
DoD Cybersecurity Scorecard				•	•	
Army Insider Threat Program				•	•	
Align ISCM with the DoD Framework					•	
Cryptographic Modernization Initiative (CMI)				•		
AR 25-2 Information Management / Cybersecurity				•	•	•
Execute Army Proponent Activities for Common Access Card (CAC)/Public Key Infrastructure (PKI)				•		
Enhance Cyber Situational Awareness by Leveraging Big Data/Cyber Analytics	•	•	•	•	•	•
Defensive Cyberspace Operations – Maneuver Baseline (DCO-MB)						•
Global Enterprise Fabric (GEF)	•					

FY17-18 NSD Activities	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 Network	
Increase Agility of Spectrum Management Operations (SMO)			•			
Standardize Network Operations (Tools Convergence, IES, Metadata)	•					
Army IT Network Asset Visibility	•				•	•

Table 3-1: NSD Activities Aligned to JCAs

Network Modernization (NETMOD)

Implement Joint Regional Security Stacks (JRSS) and the Joint Management System (JMS)

JRSS are part of the Single Security Architecture for continental United States (CONUS) and outside CONUS (OCONUS) installations that will create a streamlined network with security and firewalls based on logical communities of interest rather than location. JRSS improve attack detection and malware management, and help prevent data loss. They provide a standard perimeter that empowers the cyberspace community to execute a high level of defense through greater situational awareness of focused and regional cyberspace events, and standardized defensive responses. JRSS benefit from architecture upgrades to the network transport infrastructure, which is a precursor to Joint Information Environment (JIE) alignment.

As the management system for JRSS, JMS will be used to manage, operate and defend the network through a hub-and-spoke configuration. JMS consists of systems, tools and information management capabilities required for DoD Information Network (DoDIN) operations and DCO - Internal Defensive Measures (DCO-IDM). These capabilities permit security and policy management of JRSS elements by the Services and DISA to fulfill their Title 10 responsibilities. Each Service is responsible for managing security contexts and policies under its operational command, while DISA is responsible for operation and maintenance of JRSS themselves. Implementation of JMS follows the timelines outlined in the NCD section of this document.

As JRSS come on line and reach functional maturity, the NSD will assume control and transition to network operations and security functions. In FY16, the DoD CIO published the JRSS Concept of Employment document (formerly known as JRSS Concept of Operations (CONOPS) and a Service Operations Annex). This document defines roles and responsibilities within the JRSS environment, as well as processes for developing TTPs to enable JRSS operations.

For FY16 JRSS and JMS accomplishments and FY17 planned activities, refer to Appendix 1 (Network Infrastructure Modernization). The NCD has the lead for the JRSS and NETMOD efforts.

Provisioning Convergence

The provisioning convergence effort pertains to the provisioning and support of Non-Secure IP Router (NIPR) and Secure IP Router (SIPR) workstations, local networks, peripherals and standard capabilities in Army Sensitive Compartmented Information Facilities (SCIFs). Currently, the Intelligence and Security Command (INSCOM) Ground Intelligence Support Activity (GISA) provides all network provisioning and support for Army SCIFs, while Network Enterprise Centers (NECs) provide similar capabilities for non-SCIF locations. Provisioning convergence intends to transition SCIF NIPR and SIPR support from INSCOM GISA to local NECs. INSCOM GISA will retain responsibility for supporting all other network capabilities in SCIFs.

Provisioning convergence will standardize NIPRNet and SIPRNet support for SCIF and non-SCIF end users under local NECs. This will align resources and actions for mission and technical support, and cybersecurity and command and control, resulting in an integrated, simplified, protected and interoperable network for the warfighter.

The Chief Information Officer/G-6 (CIO/G-6) Cybersecurity Directorate instituted the Provisioning Convergence Working Group (PCWG) to coordinate Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities - Policy (DOTMLPF-P), technical, process and related cost analyses and plans to implement SCIF provisioning convergence. The PCWG is chaired jointly by CIO/G-6 and Army G-2, and includes G-3/5/7, Army Cyber Command (ARCYBER), INSCOM and other stakeholder commands, as needed.

In FY16, the PCWG developed a charter and conducted a DOTMLPF-P analysis, highlighting issues related to transitioning SCIF provisioning from GISA to NECs. ARCYBER and Second Army developed a CONOPS to implement this provisioning convergence effort.

In FY17, the PCWG will continue developing the convergence CONOPS, collecting as-is information that describes how GISA and ARCYBER provide NIPRNet and SIPRNet to their respective end-user communities, and plans, processes, cybersecurity needs and technical designs to implement the convergence. This will include a detailed cost analysis of current and projected provisioning, and identification of year-by-year budget needs to conduct the transition and sustain future support by NECs. The PCWG will coordinate with Military Intelligence end users to identify a suitable SCIF as a pilot site, and implement provisioning convergence at that site. Lessons learned from the pilot will be incorporated in the provisioning convergence CONOPS and related plans, schedules and budgets.

In FY18, the PCWG will coordinate and oversee the Army-wide transition of SCIF NIPR and SIPR provisioning from INSCOM GISA to NECs. CIO/G-6 currently expects provisioning convergence to be completed by FY20.

Organize and Advance Mobility

As part of the overall Army mobility capability, the NSD will focus on enabling mobile users to perform work functions over a secure network anytime, from anywhere. A robust network infrastructure, reliable enterprise services and dependable mobile end-user devices (EUDs) are

all components necessary to make Army mobility successful. Mobile EUDs will augment the traditional desktop infrastructure, and replicate or utilize many of the same technologies in the current workplace environment. The ends, ways and means for the Army mobility capability will be captured in the Army Mobile Vision document, which will serve as the foundation for capability development and implementation moving forward.

At the end of FY16, mobility advancements included:

- The DoD Mobile Unclassified Capability Service achieved full operating capability, with an online unclassified Mobile Application Store.
- Delivered initial mobile access to unclassified data and information.
- Used government-furnished mobile communication devices to access classified knowledge centers and collaboration websites through multiple classification levels.
- Provided an online classified Mobile Device Manager.

A key focus in FY17 will be the finalization and publication of the Army Mobile Vision document. It will completely integrate tactical and strategic elements, include all forms of IT and scope all technical requirements, enabling the Army to be flexible and fully capable at all times. Other mobility activities in the near term include the following.

In FY17:

- Integrating UC into the Mobile Enterprise Unclassified Capability.
- Delivering initial mobile access to classified data and information.
- Establishing a mobile application development and vetting process.
- Delivering an Army Mobile Vision document for 2020 and beyond.

In FY18:

- Modifying Army workforce policies and procedures to enable mobile execution of mission functions and duties.

Transition to Key Management Infrastructure (KMI)

Key management enterprise services provide the foundational capabilities to securely generate, distribute and account for cryptographic key and communications security (COMSEC) materials.

Key management is the set of activities involved in the handling of cryptographic keys and other related security products, from production to destruction. It is critical to ensuring the confidentiality, integrity and availability of secure communications (voice, video, data). KMI will provide a unified, interoperable and trusted infrastructure for establishing, using, operating and managing cryptographic products and services in a net-centric environment.

The Army is currently migrating approximately 400 COMSEC accounts from the legacy Electronic Key Management System (EKMS) to KMI. With the implementation of KMI, the Army will have an enterprise solution that delivers cryptographic keys and products over the network, enhancing the ability to electronically field, receive and account for cryptographic products.

At the end of FY16, KMI-related accomplishments included:

- Transitioned 75 EKMS COMSEC accounts to KMI, bringing the total number of accounts transitioned to 103.
- Successfully stood up three KMI new equipment training classrooms to support KMI Management Client (MGC) hardware fielding across the Army.
- Provided new equipment training to approximately 334 KMI operating account managers.

In FY17, the Army will continue to transition Spiral 2, Spin 1 capabilities that support COMSEC accounts that require SIPRNet connectivity. The Army intends to start transitioning Spiral 2, Spin 2 capabilities in the third quarter of FY17, which will allow migration of accounts that require NIPRNet connectivity. By the end of FY17, the Army plans to have transitioned approximately 161 EKMS Tier 2 accounts to KMI MGCs, in accordance with delivered capabilities and the FY17 Sustainment Readiness Model. The Army will assist the DoD CIO, National Security Agency (NSA) and other Services in establishing the KMI Capability Increment 3 (CI-3) Capability Development Document (CDD). This document will provide the foundation for the next phase of the transition to KMI. It will incorporate EKMS Tier 1 functionality and expand KMI enterprise capabilities to support Mission Planning Management Support Systems, setting the framework to incorporate KMI advanced capabilities not implemented in CI-2 and to expand KMI enterprise capabilities.

By the end of FY18, the Army plans to have transitioned all EKMS Tier 2 accounts to KMI MGCs. Also, the NSA, in coordination with the DoD CIO and the Services, will finalize and publish the KMI CI-3 CDD.

Enhance Identity and Access Management (IdAM)

In FY16, the Army initiated the Risk Management Framework (RMF) process for the Directory and Identity Synchronization Service (DISS). This capability will be used to populate Army forests with a single trusted set of identity credentials. The Army expects to complete the DISS RMF process in FY17. Also, in FY16, the Army finished transitioning all eligible applications from Army Knowledge Online (AKO) Single Sign-On (SSO) to Direct Public Key Infrastructure (PKI) or a common enterprise authentication service.

In FY17-18, the Army will work to leverage an enterprise service-based authentication and access management capability that utilizes identity attributes from authoritative sources. The Army enterprise IdAM framework will ensure strategic, functional and tactical capabilities that use a single trusted set of DoD enterprise and Army-specific identity data (Single Identity) to enable SSO, cloud services and attribute-based access controls (ABAC) for IT resources. The use of accurate and reliable identity data will ensure that only authorized entities access information resources. It also will enhance interoperability by using standardized attributes and schemas, and will reduce the number of sources that proliferate untrusted identity data across the Army. In addition, by leveraging common services to provide seamless network access to information resources, the Army will be able to decommission standalone access control mechanisms, which are often insecure, inefficient and redundant, for applications, systems and networks. This enterprise service-based framework will allow the Army to set conditions for applications and systems to manage entitlements and audit the network transactions of privileged and non-privileged users.

The enterprise IdAM framework will support the following actions for all Army information resources.

- Sustain an enterprise service to manage Common Access Card (CAC)-ineligible mission partners and authoritative data sources for Army-specific attributes.
- Leverage an enterprise service-based authentication and access management capability for SSO, ABAC and cloud services.
- Provide a logical access control model that enforces the use of DoD and Army identity data, and a data-centric approach to access control that reduces domain-based security enclaves.
- Enable user activity monitoring (UAM) capabilities to monitor and analyze privileged user activities.
- Standardize the dissemination of enterprise identity data across tactical systems and environments.

Refine the Cyberspace Workforce

Cyberspace is acknowledged as a warfighting domain of mission-critical importance to DoD. As adversaries exploit this domain for their military, economic and political advantage, operations in cyberspace are evolving from an afterthought to a fundamental element. The cyberspace workforce is similarly evolving from supporting work roles to positions recognized as critical to the defense of the nation. The workforce is composed of personnel who build, secure, operate, defend and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable operations; and project power in or through cyberspace.

Operational planning teams have identified a set of workforce-related topics they will address to validate certain work roles (core, direct support and specialized support) within the context of the DoD Cyberspace Workforce Framework. In FY17-18, cyberspace workforce refinement activities will continue to define, identify, shape and track the civilian cyberspace workforce, and define and align its roles with the military Career Field 17 structure.

Define Work Roles

In FY16, the Army completed a workforce inventory and began assessing training availability. In FY17, the Army will establish a comprehensive cyberspace workforce talent management plan, which will identify strategies to acquire, develop, employ and retain the cyberspace workforce.

Identify, Shape and Track the Civilian Cyberspace Workforce

In FY17-18, the Army will continue to develop career management solutions to capitalize on investments in resident military and civilian cyber talent. Consistent with these efforts, the Army will concurrently develop a comprehensive workforce strategy and implementation plan to maximize Soldier and civilian personnel management.

Align Civilian Workforce Roles with the Military Career Field 17 Structure

Army cyberspace workforce development efforts will align with DoD Directive 8140, Cyberspace Workforce Management, which updates personnel policies and assigns responsibilities for the comprehensive management of the entire DoD cyberspace workforce.

The cyberspace workforce is divided into four defined categories: cybersecurity, cyberspace effects, cyberspace IT and intelligence (cyberspace). Coding the cyberspace workforce is critical to managing and standardizing cyberspace work roles, baseline qualifications and training requirements across DoD, and nesting with corresponding Service efforts.

By the end of FY18, the Army will establish an integrated civilian cyberspace workforce framework that will provide individual career management based on resident skills and qualifications. This framework will allow human resource managers to balance individual skill sets with work role requirements to ensure that the most qualified personnel are assigned to the right positions.

DoD Cybersecurity Scorecard

The DoD cybersecurity campaign, which includes the Cybersecurity Discipline Implementation Plan (CSDIP) and Cybersecurity Scorecard, addresses the overall cybersecurity posture and works to minimize the attack vectors exploited by adversaries to gain access to information networks.

The Cybersecurity Scorecard is a means for the Secretary of Defense to understand cybersecurity compliance at the strategic level through Service-tier metrics provided each month. It captures the cybersecurity posture of Army information systems and infrastructure, as well as system administrator and user compliance. Monthly scorecard reporting, which began in July 2015, forces awareness of and accountability for these key tasks into the command chain and up to DoD leadership, where resourcing decisions can be made to address compliance shortfalls. The 10 consolidated tasks in the Cybersecurity Scorecard focus on four major LOEs: 1) strong authentication; 2) device hardening; 3) reduce attack surfaces; and 4) alignment to cybersecurity/computer network defense service providers. DoD and the Services are working on automating the manual data entry/reporting processes. Implementing a healthy cybersecurity culture across all ranks, one that ingrains a self-correcting discipline, is of primary importance.

FY16 accomplishments include:

- ARCYBER issued a fragmentary order (FRAGO) directing units to disable access for system administrators and privileged users not using PKI for authentication.
- The Army moved to reduce the attack surface created by public-facing web servers. All non-compliant web servers have been or are in the process of being quarantined from public access. Non-compliant Army web servers are being moved behind approved demilitarized zones, going from 36% to 98% compliance.
- CIO/G-6 submitted five change requests that will incorporate a list of enumerated options to streamline the Cybersecurity Scorecard reporting process while improving consistency and accuracy. All requests have either been implemented or are at various stages of the confirmation and implementation process.
- CIO/G-6 established an integrated team, including key stakeholders, to: identify automated tools for data collection/reporting; clarify scorecard intent, definitions and reportable systems; and refine the reporting structure in order to improve accuracy and accountability.

In order to raise commanders' awareness of and accountability for the cybersecurity readiness of their information systems, associated reporting requirements will be included in the Defense Readiness Reporting System per DoD Directive 7730.65 and DoD Instruction 7730.66. Details

of the reporting criteria are included in each section of the CSDIP. Security principles in cyberspace are very similar to those in securing physical battlespace: Leaders throughout DoD are responsible for ensuring that the information capabilities they own, manage or lease have implemented the requisite level of cybersecurity.

Planned objectives for FY17 and FY18 include:

- Fortify DoD information networks' security posture by decreasing the number of vulnerable points through which an adversary could gain access and move laterally. This critical area drives three requirements: use strong authentication, harden devices and reduce the attack surface.
- Ensure continued protection, monitoring, analysis, detection and response against intrusion attempts. Computer network defense service providers (CNDSPs) perform this function for DoD information networks, which means commanders must align their systems and networks to CNDSPs.

The Army Insider Threat Program

The Army Insider Threat Program is an enhancing capability that provides timely threat information and risk-based analytic support across the full range of military operations to mitigate current and emerging insider threats. In accordance with the President's memorandum regarding national insider threat policy and minimum standards for the Executive Branch, the Army must deliver effective response and mitigation (by investigative authorities) to protect classified National Security Systems and information from unauthorized disclosure and acts of physical violence.

The Army must accomplish this task by utilizing UAM capabilities to observe and record a user's computer or network activity. These capabilities will enable the Army to monitor users interacting with sensitive IT resources and will generate alerts based on defined triggers when policy violations or anomalous activities occur. All indicators and activities monitored by UAM capabilities will be analyzed and utilized in compliance with all applicable legal authority and individuals' privacy rights and civil liberties.

In FY16, the Army awarded a contract for management of UAM activities, with hardware deployment in INSCOM's data center.

In FY17-18, due to the large scope of detecting and assessing the risks of potential insider threats within an Army population of more than 1.3 million personnel (military, civilian and contractor), the Army will prioritize and focus efforts on strategic and operational classified networks (SIPR and the Joint Worldwide Intelligence Communications System initially). UAM capabilities will enable the Army to collect highly detailed computer user activity to support the following mission tasks.

- Receive, access, integrate and analyze insider threat indicators, as authorized and applicable, from Army UAM, personnel security, counterintelligence, law enforcement and other pertinent data sources.
- Conduct holistic insider threat risk management to assess risk and determine risk priority in order to effectively impact response and/or risk mitigation measures.
- Provide timely reporting and referral of insider threat information to enable effective response and mitigation by investigative or command authorities.

- Inform investigative and/or command authorities, senior leaders and the DoD Insider Threat Management and Analytic Center in order to support risk decisions, responses and mitigation efforts.
- Monitor response and risk mitigation efforts in order to protect against current and emerging threats.

Also in FY17-18, the Army will assess several additional insider threat options for future implementation, such as: enacting two-person control/management of data and cross-domain transfers, to include removable media on classified networks; enabling portal security and auditing capabilities on all classified networks; and enhancing user activity monitoring in Big Data/cyber analytic environments via tools such as DISA's Cyber Situational Awareness Analytic Capability – Anomaly Detection Suite.

Align Army Information Security Continuous Monitoring (ISCM) with the DoD Framework

DoD defines continuous monitoring as the "ongoing observation, assessment, analysis and diagnosis of an organization's cybersecurity posture, hygiene and operational readiness."[a] The Army is aligning initiatives with the DoD ISCM Framework, which will be achieved in a multi-year, iterative effort, leveraging current investments in enterprise and non-enterprise cybersecurity tools and capabilities.

The DoD ISCM Framework encompasses the 11 security automation domains defined by National Institute of Standards and Technology Special Publication 800-137. Data are captured, correlated, analyzed and reported to present the risk and attack surface of the enterprise.

In FY16, several Army organizations began to implement ISCM solutions. In FY17-18, Training and Doctrine Command (TRADOC) will conduct a DOTMLPF-P assessment to determine whether capability gaps exist within ISCM. The Army will also continue its multi-year, iterative effort to implement a continuous monitoring solution that is aligned to both DoD and federal strategies, remains consistent with confidentiality, integrity and availability, uses best practices and is reliable and effective.

Cryptographic Modernization Initiative (CMI)

The Army will continue to modernize cryptographic capabilities (embedded and standalone) and key management services in accordance with DoD and NSA mandates and the Sustainable Readiness Model (formerly Army Force Generation).

At the end of FY16, CMI:

- Published the Army's cryptographic modernization technology roadmap (standalone) to assist with timelines for modernizing, divesting and inserting into the Program Objective Memorandum (POM) cryptographic and key management capabilities.
- Developed the Cryptographic Modernization Strategy and Implementation Plan, which provides overarching guidance and procedures to divest legacy systems, and a

[a] *DoDI 8510.01, Risk Management Framework for DoD Information Technology, 12 March 2014.*

modernization timeline to enhance security, interoperability and throughput to support UC, Common Operating Environment (COE) and JIE.

- Completed modernization of National Leadership Command Capability cryptographic capabilities by replacing legacy cryptographic components in accordance with DoD CIO-directed targets.
- During Phase 1 of Army-level COMSEC Modernization/Radio Working Group meetings, identified for elimination authorizations for 110,000 radios.

In FY17-18, CMI will continue to balance funding constraints against available technology and risk management by focusing on:

- Publishing new encryption guidance and policies for new technology trends and advanced cryptographic capability (ACC) devices in order to identify applications necessary to improve the Army's network security posture.
- Evaluating current operational nuclear command, control and communications technology against NSA ACC mandates.
- Developing and publishing a cryptographic modernization strategy (looking forward 36 months).
- Developing a near-term/long-term cryptographic technology (standalone and embedded) modernization roadmap, which will reduce the Army's cryptographic footprint by divesting legacy devices. These efforts support the Army requirement to improve network performance by reducing the overall burden on the network.

It is imperative that the warfighter be equipped with the latest cryptographic capabilities that effectively support modernized networks and the execution of operational missions. Therefore, the Army must continue to modernize and leverage new, innovative technologies that provide security, scalability, interoperability and reliability for the exchange of voice, video and data between authorized individuals, groups and entities across the Army and mission operations. CMI will develop targets for achieving modernization of the Army cryptographic inventory. As the Army transitions legacy waveforms, CMI will support the integration of a near-term capability across the Army and DoD components, and long-term Joint Force and coalition partner interoperability. The Army will account for all legacy crypto devices and track the transition to modernized capabilities.

Army Regulation (AR) 25-2, "Information Management / Cybersecurity"

In FY16, the Army selected a new approach for AR 25-2 that establishes five concurrent and continuous functions for managing cybersecurity risk: identify, protect, detect, respond and recover. It also sets responsibilities and prescribes high-level policies in a more understandable format. This approach allows responsible Army personnel to quickly grasp key policy tenets while providing task-focused implementation guidance in Department of the Army (DA) cybersecurity pamphlets. Seventeen DA Pamphlets were drafted to implement the policies in the regulation.

In FY17, CIO/G-6 will submit the draft AR 25-2 and the 17 DA cybersecurity pamphlets to the Army Publishing Directorate for publication. In FY18, CIO/G-6 will continue to collaborate with stakeholder organizations to develop policies and procedures to increase cybersecurity and address emerging threats and changing technologies.

Execute Army Proponent Activities for CAC/PKI

In FY16, the Army passed DISA's Registration Authority audit. The Army also ensured PKI Registration Authority and Local Registration Authority compliance by conducting several audits of its own. The Army provided 24/7 PKI daily operations, and NIPR Alternate Smart Card Login and SIPR token support and services to more than 150,000 Army and Army-supported personnel. In November 2016, CIO/G-6 transitioned PKI daily operations to Network Enterprise Technology Command (NETCOM), without the Army's experiencing a break in PKI support and services.

In FY17-18, CIO/G-6 will continue to serve as the Army's PKI proponent lead to the DoD CIO and oversee the Army PKI program. CIO/G-6 will conduct site assistance and compliance visits at Army Registration Authority sites for both person and non-person entity activities, in accordance with DoD guidance. Also, in coordination with NETCOM, CIO/G-6 will ensure that Army equities and capability requirements remain aligned with DoD PKI Program Management Office (PMO) acquisition activities; will participate in DoD PKI PMO, DoD CIO and NSA token management forums and test activities; and will respond to DoD CIO requests regarding acquisition objectives. Finally, CIO/G-6 will oversee integration of PKI from the strategic to the tactical level, ensuring end-to-end security for the Army’s networks and its users.

Enhance Cyber Situational Awareness by Leveraging Big Data/Cyber Analytics

The Army is constantly assessing threats against its network and defending against adversary attacks. One of the Army’s challenges is to fully exploit the unprecedented growth in data collected to enhance cyber situational awareness, to protect the network and to conduct effective DCO. The Army is addressing the cyber situational awareness capability gap by leveraging Big Data technology, including the government off-the-shelf Big Data Platform (BDP) and development of mission-specific cyber analytics.

BDP provides the capability to collect and analyze the massive volumes of configuration, operations and security data generated across the Army’s strategic environments. Analytics within BDP will enable correlation across multiple data sources in order to identify anomalies within the environment more rapidly and effectively than has been possible with segmented tools and data sets.

The Army’s major Big Data/cyber analytics initiatives include the following.

Program Executive Office Enterprise Information Systems (PEO EIS) Big Data Pilot II

Based on the ARCYBER Operational Needs Statement, Big Data Pilot II, led by PEO EIS, has four primary goals: 1) add operational capabilities to the CNDSP and Cyber Protection Teams (CPTs) supporting Army Materiel Command and the Defense Research and Engineering Network; 2) transition externally developed analytic capabilities into the platform; 3) enable ingest from at least five JRSS data feeds to the BDP developed by Pilot I; and 4) conduct technical testing to optimize performance of the platform (increase volume and velocity).

In FY16, the Army focused on data acquisition, performance measures and improvements, and integration of analytic creation and visualization capabilities. ARCYBER continued development of analytics in the Amazon Web Services GovCloud for the Army Cyberspace Operations and Integration Center, using BDP. PEO EIS matured for production “virtual” Army Cyber-Research Analytics Laboratory prototypes, including Automated Mission

Mapping Operations (AMMO), Cyber Cloud Operations Services (CYCLOPS), Doc Holliday and Dagger.

In FY17, the Army's main focus will move to integration with DCO-I; incorporating identity and access management, and a distributed query and cross-domain capability; and evaluation of a continuous monitoring and risk scoring prototype from Cyber Innovation Challenge 2. The Army will continue adding Big Data efforts into its DCO program and will deploy additional Big Data/cyber analytics platforms to JRSS sites. In addition, AMMO, CYCLOPS, Doc Holliday and Dagger prototypes will enter production.

ARCYBER Big Data Initiatives

As part of the Army's efforts to embrace and leverage Big Data analytic capabilities, ARCYBER (including NETCOM) has configured and installed instances of BDP on the NIPRNet to support DoDIN operations and DCO. This joint effort, begun in FY16, is known as Gabriel Nimbus and supports ARCYBER and DoDIN Fusion Center operations. The intent is to produce a more effective capability for analyzing and correlating data across multiple sensors (network operations, cyber and non-cyber), performing analytics on the collected data, and developing a holistic operational picture that provides mission context to support decision making at multiple echelons. Some of the specific analytics and use cases implemented in FY16 included:

- Holistic Global View of the Network
- Network Operations Anomaly Detection
- Malware and Botnet Detection
- Asset Inventory and Configuration View

In FY17, NETCOM will extend the scope of data sources ingested into the platform and expand analytics use cases. It also will assess key attributes for an enterprise-wide capability, such as the appropriate time period to store ingested data, identification of critical data versus data not required to be captured, appropriate data standards, access controls and organizational roles, and identification of critical data sensors and their placement. In addition, the Army will refine the requirements that will inform future program of record capabilities.

DCO – Maneuver Baseline (DCO-MB)

Cyberspace defense requires the development of a maneuver baseline built on an infrastructure, platform and tool/payload paradigm. "Infrastructure" is defined as "the collection of hardware and software/firmware that enables the instantiation and/or execution of software platforms". The infrastructure contains a physical layer and an abstraction layer, when applicable. The physical layer consists of hardware resources necessary to support the services provided via platform deployment, and typically includes physical servers, storage and network components. The abstraction layer consists of software deployed across the physical layer that enables a common interface to underlying hardware resources that provide on-demand services, broad access, resource pooling and elasticity. The term "platform" is defined as a capability provided to the operator that enables the deployment of necessary tools and payloads onto the infrastructure. Platforms (publically available, licensed and orchestrated virtual machines) are installed on the infrastructure and consist of software such as operating systems, middleware, runtimes, databases, web servers and development environments. A cyberspace tool is software,

data or an application that supports or directly causes effects related to cyberspace mission force and cyberspace workforce tasks. These tools are executed or managed within a platform. DCO-MB's key components are Garrison DCO Platform (GDP), Tactical DCO Infrastructure (TDI) and Deployable DCO System (DDS).

Garrison DCO Platform (GDP)

The GDP provides virtual terrain for Cyber Protection Teams (CPTs) to maneuver remotely and augment cyberspace defenders within the NECs in support of military and business operations. GDP is composed of prepositioned hardware and software at select installations. Fielding will nest with both the Army's network modernization strategy and installation protection priority list. The "enhanced" version of GDP will support data collection and storage requirements for Big Data/cyber analytics.

In FY16, PEO EIS designed and integrated hardware and software into a GDP, and fielded it to three pilot locations (Fort Gordon, GA; Redstone Arsenal, AL; Fort Belvoir, VA). These pilots will be used to further inform DCO requirements documents, specifically the Requirement Definition Packages for garrison, tactical and deployable DCO capabilities.

FY17 GDP efforts include:

- Completing initial fielding on the NIPRNet at the Cyber Battle Lab (Ft. Gordon, GA), Ft. Belvoir, Redstone Arsenal and Wiesbaden, Germany.
- Completing fielding of SIPRNet version of GDP at Wiesbaden.
- Incorporating the use of GDP in Army Warfighting Assessment (AWA) 17.1, Network Integration Evaluation (NIE) 17.2 and Cyber Quest 17.

FY18 GDP efforts include:

- Supporting the establishment of a GDP program of record.
- Installing both NIPRNet and SIPRNet GDPs at eight select Type I installations in accordance with the Army's Installation Protection Priority List.
- Incorporating the use of GDP in AWA 18.1, NIE 18.2 and Cyber Quest 18.

Tactical DCO-Infrastructure (TDI)

Similar to GDP, TDI provides virtual terrain for CPTs to maneuver remotely to a designated network. Unlike GDP, TDI is meant to solely support military operations and augment cyberspace defenders organic to the corps, division and Brigade Combat Teams (BCTs) levels. Currently, the Army plans to deploy TDI within an organization's main and tactical command posts for both SIPRNet and coalition networks. The Army also is analyzing whether there is a requirement for TDI on NIPRNet and the colorless core.

The Army now has 10 instantiations of the TDI, managed by the PEO Command, Control and Communications - Tactical (C3T) Tactical Cyber and Network Operations Division. In FY16, PEO C3T successfully demonstrated use of the 10 kits during NIE 16.2.

FY17 TDI efforts include:

- Incorporating the use of, and evaluating, TDI in AWA 17.1, NIE 17.2 and Cyber Quest 17.
- Initiating integration of Big Data/cyber analytics.

FY18 TDI efforts include:

- Supporting establishment of a TDI program of record.
- Fielding four sets each to three corps, 11 divisions and 30 BCTs (all active Army components).
- Continuing to work integration of Big Data/cyber analytics.
- Incorporating the use of TDI in AWA 18.1, NIE 18.2 and Cyber Quest 18.

Deployable DCO System (DDS)

DDS provides a fly-away (deployable) capability that enables CPTs to locally augment cyberspace defenders at any base, post, camp or station (including tactical sites). DDS is used in situations where a supported unit is not assigned a prepositioned capability or cannot be reached remotely through GDP or TDI.

In April 2016, phase I of the DDS prototype effort delivered a total of three systems to the Army. Each DDS consists of three configurations: "Initial" – a small configuration for hasty missions lasting no more than five days; "Enhanced" – a medium configuration for deliberate missions of up to four months; and "Sustain" – a large, prepositioned configuration for missions lasting more than four months. At the end of FY16, phase II of the prototype effort delivered one DDS to the Cyber Protection Brigade (CPB).

FY17 DDS efforts include:

- Completing prototype phase II fielding, which consists primarily of replacing the current initial category systems with a more robust infrastructure.
- Completing phase III fielding of DDS prototypes in the second quarter of FY17. Phase III includes converging Enhanced and Sustain configurations into a single configuration to produce a complete DDS consisting of one Initial and one Sustain configuration.

FY18 DDS efforts include:

- Supporting establishment of a DDS program of record.
- Fielding 10 DDSs to the CPB.

DCO Tool Suite

The DCO Tool Suite provides the tools/payload layer of the DCO - MB. The tool suite will consist of a flexible, dynamic, software-based set of warfighting capabilities that comply with the JIE and COE and enable CPTs to perform survey, secure and protect missions. The full baseline set of tools is referred to as version 1.5. To ensure synchronization, efficiencies and deconfliction, CIO/G-6, ARCYBER and the Cyber Center of Excellence are working with NETCOM on the tools convergence effort.

In FY16, PEO EIS completed an initial buy of nine tools, which were delivered to the CPB in June 2016, based on ARCYBER priorities. PEO EIS also continued to work the transition of web vulnerability scanners, which are part of the DCO Tool Suite, in support of phases II and III of the Web Scanning Operational Need Statement.

FY17 DCO Tool Suite efforts include:

- Continuing to purchase tools within available CPT support funding.

- Incorporating select tools into AWA 17.1, NIE 17.2 and Cyber Quest 17, based on approved operational threads.

FY18 DCO Tool Suite efforts include:

- Purchasing and fielding a full set of version 1.X tools, to be synchronized with GDP and TDI fielding.
- Incorporating select tools into AWA 18.1, NIE 18.2 and Cyber Quest 18, based on approved operational threads.

Overall, the DCO-MB and its elements will ensure the Army's ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities and designated systems.

Global Enterprise Fabric (GEF)

NETCOM's GEF will provide the Army a complete suite of enterprise computing services under three broad areas: infrastructure as a service (IaaS), network services and computer network defense (CND). The GEF utilizes a converged hardware architecture with a software-defined infrastructure consisting of compute, network and storage management elements that support enterprise operation and management (O&M) capabilities. By leveraging advanced virtualization technology, the Army will reduce overall infrastructure costs, increase agility in the deployment of enterprise O&M capabilities and gain centralized management, monitoring and reporting of LandWarNet.

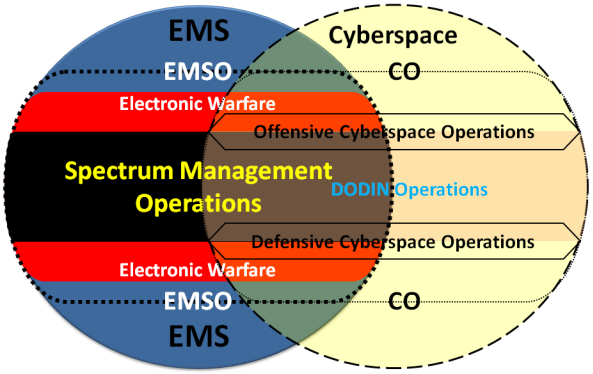
In FY16, NETCOM submitted a request for proposal to industry for the initial Army cloud architecture to provide virtual capacity in support of enterprise initiatives and LandWarNet sensor grid life-cycle requirements. The Army expects fielding to begin in FY17.

When initial GEF fielding is completed (likely in FY17), infrastructure services such as Active Directory, PKI, Online Certificate Status Protocol and identity management will be virtualized onto the GEF, a process known as on-boarding. The LandWarNet sensor grid toolset also will begin to on-board. An enterprise capacity manager will be appointed to prioritize on-boarding of enterprise, regional and local tools and services, and to manage available capacity for emerging missions.

Increase the Agility of Spectrum Management Operations (SMO)

SMO must become more agile and effective in order to provide the Army the freedom of movement it requires for expeditionary maneuver. Likewise, spectrum managers must be equipped with the tools necessary to accurately assess the spectral environment as it changes. Further, electromagnetic spectrum operations (EMSO) doctrine must be refined to better coordinate SMO with electronic warfare (EW) in order to safeguard the necessary robust networks that support the command and control systems of the modern battlefield. By working in concert with EW planners, spectrum managers are able to plan timely, relevant and effective SMO to enable the agile, expeditionary force depicted in the Army Operating Concept. In this manner, EMS is utilized as a domain for conducting EW. Effective EMSO allows "Army forces

to maneuver and project power across all domains,"[b] and enables the extension of the network from garrison to the forward-deployed Soldier.



EMSO	Cyberspace Operations (CO)
SMO: Host-Nation Coordination Frequency Allocation Frequency Assignment Policy Enforcement	**Offensive Cyberspace Operations:** Cyberspace Attack Cyberspace Intelligence, Surveillance, Reconnaissance Cyberspace Operational Preparation of the Environment
EW: Electronic Attack Electronic Support Electronic Protect	**Defensive Cyberspace Operations** (Responsive Actions): Cybersecurity Cyberspace Defense
	DoDIN Network Operations

Figure 3-1: Impact of Spectrum Management Operations on EMSO and Cyberspace Operations

The figure above illustrates the relationship between EMS and cyberspace in order to deliver effects upon enemy networks, to defend our own networks, and to detect and deter enemy cyber activity within friendly cyberspace.[c] It underscores the importance of effective SMO and the role the spectrum manager plays in mitigating harmful electromagnetic environmental effects in order to safeguard the Army's access to EMS. Spectrum managers require modern tools, such as the Electronic Warfare Planning and Management Tool (EWPMT), to keep pace with the ever-changing electromagnetic environment.

EWPMT integrates cyber electromagnetic activities (cyberspace operations, SMO and EW), and supports overall mission command, by adding the electromagnetic order of battle to the fight. It enables the spectrum manager to plan, coordinate, manage, control and deconflict the electromagnetic operational environment with the EW officer in order to synchronize EMSO across the intelligence, operations and signal arenas. EWPMT will be fielded in increments called Capability Drops (CD). CD 1, integrated with the Command Post Computing Environment, will provide a partial spectrum management capability to create, import, export and modify force structure information, radio frequency emitter data and characteristics, and

[b] *TRADOC Pam 525-3-1.*

[c] *For information regarding cyberspace operations, refer to Field Manual 3-38, Cyber Electromagnetic Activities; or Joint Publication (JP) 3-12(R), Cyber Space Operations. For information regarding EW and EMSO, refer to JP 3-51, Joint Doctrine for Electronic Warfare; and JP 6-01, Joint Electromagnetic Spectrum Management Operations.*

frequency assignments. CD 2 will improve upon the initial capabilities provided in CD 1, with all data exchanges being made in DoD's Standard Spectrum Resource Format (SSRF).

Near-term deliverables for CDs 1 and 2 include:

- Initial unit fielding of EWPMT CD 1 occurred in September 2016. Fielding will continue through FY17, with Ft. Bliss scheduled for May and June 2017.
- Development of EWPMT CD 2 was initiated, with fielding scheduled (notionally) for the fourth quarter of FY18 through the third quarter of FY20.

By transitioning to SSRF, the Army's EMS data will become interoperable, discoverable, accurate and relevant to Army spectrum managers, other Services' spectrum managers, DoD entities involved in spectrum operations and other government agencies, such as the National Telecommunications and Information Administration and the Federal Communications Commission. SSRF enables the Army to receive data in the standard, joint format in order to conduct operations in support of the Joint Force, in accordance with the Army's doctrinal mission. The Army expects to complete the SSRF transition in FY18.

Throughout FY16, the Army Spectrum Management Office (ASMO) remained engaged at the joint, DoD and global levels, as well as with industry, to make spectrum operations more agile and flexible. ASMO also published the FY16 biennial update to AR 5-12; and participated in interagency and DoD meetings to coordinate and discuss spectrum requirements for EW, reallocation of the 1300-1350 MHz band, and spectrum auctions that impacted the Lightweight Counter Mortar Radar, the Air Traffic Navigation, Integration and Coordination System, and the Digital Airport Surveillance Radar. In FY17-18, the Army will maintain its efforts to increase EMS situational awareness in order to mitigate potential electromagnetic interference and to improve the overall health of the network by exploring emerging EMS monitoring capabilities.

Standardize Network Operations

Network Operations Tools Convergence, Information Exchange Specifications (IES) and Metadata

Network operations are a core competency of Signal Regiment support to the Army, and entail engineering, installing, operating, maintaining and securing the Army's portion of the DoDIN. The Army's network operations construct is now aligned with DoDIN Operations (to include cybersecurity).

To enhance standardization of network operations processes and IT across the Army network, CIO/G-6 and the network operations community developed an authoritative CONOPS, metadata requirements and technical IESs. These documents will help the Army to synchronize network operations and align services and applications to a common baseline. Additionally, CIO/G-6 has undertaken a multi-year effort to shape and influence the convergence of network operations tools across the Army. CIO/G-6 is coordinating the process of identifying and evaluating the needs and requirements for end-to-end network operations tools (enterprise and tactical) and applications in order to streamline and standardize. To achieve this, the Tools Convergence Working Group (TCWG) will monitor and influence the development, assessment, training and integration of network operations tools to ensure standardization and interoperability from an end-to-end perspective.

In FY16, the Army established and validated the network operations tools convergence methodology. In addition, a TCWG charter was drafted.

In FY17, CIO/G-6 and key stakeholders will focus on developing the network operations tools convergence implementation strategy, which will lead to Army-wide network operations tools standardization in support of LandWarNet mission users. The Army also intends to establish the selected network operations tools repository. The Army will publish information exchange specifications for standardization of network systems (e.g., routers, servers), which will help to support asset visibility and situational awareness of key network infrastructure. IESs also will be integrated into the RMF. The Army will draft metadata requirements documents that support integrated, end-to-end DoDIN operations. Additionally, CIO/G-6 will complete the transition of the TCWG charter to a memorandum of agreement.

In FY18, the Army will focus on populating the online network operations tools repository with all applicable technical, contract, license, cost, user/owner and mission data. This will be accomplished through integration with existing authoritative data sources, tool/capability users and information owners. These data will be used to support recommendations presented to the AENC for tool-related decisions.

Army Network IT Asset Visibility

The ultimate goal of the Army IT asset visibility strategy is to have a complete, up-to-date and accurate view of all network components, including PCs, laptops, tablets, mobile phones, servers, printers, hubs, routers, switches, databases, applications and other software – everything that comprises the enterprise IT infrastructure. All of these assets are connected, all are related and all are responsible for supporting the people, processes and transactions that power the warfighter's mission and business operations. Additionally, the Army cannot secure or defend what it cannot see on the network; therefore, asset visibility is critical to the network operations, DCO and cybersecurity missions. Network IT assets should be closely managed throughout their entire life cycle – from the day they are requested and procured, through fielding, until retirement and removal from the network.

In FY16, CIO/G-6 investigated the current asset visibility problem and began documenting ends, ways and means for a long-term strategy that will contribute to greater IT efficiency and network security. Additionally, CIO/G-6 partnered with the Joint Staff and Air Force to leverage existing real-time visibility and response technology capabilities that comply with the JIE single security architecture. The goal is to implement several pilots in FY17 based on the current fiscal environment.

In FY17-18, the enterprise license division will coordinate with PEO EIS to determine the most economical means of procuring licenses to execute pilots using existing DoDIN technologies. Based on the results of Second Army and NETCOM pilots, the Army will develop an implementation plan to enable PEO EIS to deliver a network asset visibility capability. The capability will provide the means to see assets at near-real time throughout all echelons of LandWarNet, from the enterprise to the tactical.

Appendix 4 – Key Performance Indicators

Army Directive 2016-16 (Changing Management Behavior: Every Dollar Counts), dated 15 April 2016, states that the Army must be innovative and serve as a good steward of taxpayer dollars. To that end, the Army must adapt good financial management practices and improve outcomes. The Chief Information Officer/G-6 (CIO/G-6) will use key performance indicators (KPIs) to track and manage major initiatives, and to measure performance of near-term activities. These metrics will serve as living indicators of how well network modernization efforts are progressing, and will provide key leaders the information necessary to make informed decisions. These results-oriented indicators include measures that are supported by metrics nested in the Strategic Management System.

Network Capacity Domain Key KPIs

Initiative	KPI	Measure
Joint Regional Security Stacks (JRSS) Non-Secure IP Router (NIPR) / Secure IP Router (SIPR)	Enhance protection and improve throughput.	# of NIPR sites completed # of SIPR sites completed
Multi-Protocol Label Switching (MPLS)	Improve throughput to fully leverage enterprise services and support unified capabilities (UC).	# of Defense Information Systems Network Subscription Services (DSS) sites completed
Installation Campus Area Network (ICAN)	Improve throughput to fully leverage enterprise services and support UC.	# of DSS sites completed
Optical Path Links	Improve throughput to fully leverage enterprise services and support UC.	# of links completed
Korea Asynchronous Transmission Mode (ATM) / Synchronous Optical Network (SONET)	Improve throughput to fully leverage enterprise services and support UC on the Korean Peninsula.	# of sites completed in Phase 1 # of sites completed in Phase 2 # of sites completed in Phase 3 # of sites completed in Phase 4
Capability Set	Deliver a common equipment baseline through a deliberate and disciplined modernization method that provides a complete, integrated package of networking equipment and functional software to combat formations, from the Home-Station Mission Command Centers (HSMCCs) to the dismounted Soldier.	# of combat formations fielded an integrated networking package
HSMCCs	Improved reach-back and reach-forward expeditionary mission command supporting Regionally Aligned Forces, military support to civil authorities, homeland defense and other non-traditional missions.	# of HSMCCs that undergo tech refresh
Common Operating Environment (COE)	Approved set of computing technologies and standards that normalize the network environment, making computer systems, operating systems, databases, security configurations and end-user devices common and interoperable across the entire force.	# of validated top-level COE requirement sets developed that align to the Joint Information Environment (JIE) and Mission Partner Environment # of requirements sets implemented

Initiative	KPI	Measure
Integrate Separate Networks	Enhance security architecture and improve throughput.	# of separate networks consolidated
Data Center Consolidation	Reduce unnecessary overlap in IT capabilities and the number of data centers in order to shrink the IT footprint and improve security.	% reduction of the Army's data center inventory # of Army Base/Post/Camp/Station (B/P/C/S) with more than one IPN
Application Rationalization	Reduce the number and cost of IT systems and applications while optimizing the remaining IT systems and applications in enterprise computing environments.	Complete a 100% assessment of Army applications
End-User Services	Enhanced wireless infrastructure that provides unclassified and classified information sharing via voice, video and data regardless of mission environment.	# of installations with improved wireless infrastructure
Divestiture	Identification and divestiture of unneeded legacy circuits, switches and routers to free up life-cycle sustainment resources.	Complete a 50% assessment of legacy equipment

Table 4-1: NCD KPIs

Enterprise Services Domain KPIs

Initiative	KPI	Measure
UC	Implementation of enterprise solutions that enhance collaboration. Recouped investments based on divestiture of licenses, applications or hardware.	# of Time Division Multiplexing (TDM) circuits transitioned to IP # of Integrated Services Digital Network (ISDN) circuits transitioned to IP video teleconference (VTC) Amount of money saved due to migration to IP
Army Knowledge Online Transition	Transition to the next generation of services to lower costs, increase efficiencies and assist in security improvement.	% of applications that have migrated to Enterprise Access Management Service - Army # of portal transformation requirements identified
Enterprise License Agreements (ELAs)	Lower costs and simplify contracts.	% reduction over General Services Administration and DoD Enterprise Software Initiative costs % reduction of separate procurement / maintenance contract actions
Army Enterprise Service Desk (AESD)	Improve the quality, lower the cost and raise the productivity of service desk activities.	# of calls resolved during first contact % increase in customer satisfaction
Army Enterprise Service Management (AESM)	Mature the delivery of IT services.	% of satisfied customers % reduction of service incidents
Position, Navigation And Timing (PNT)	Improve the ability to obtain valid PNT data in a non-permissive environment.	% of time PNT is able to operate in restrictive terrain with enemy interference, jamming or spoofing % of time PNT data are within reliable parameters

Table 4-2: ESD KPIs

Network Operations and Security Domain KPIs

Initiative	KPI	Measure
Provisioning Convergence	A single, secure, uninterrupted, global environment that provides NIPR and SIPR networks and services throughout all phases of operations in support of the Army Operating Concept.	% of milestones reached towards developing a memorandum of agreement to provide guidance to stakeholders % of milestones reached towards developing initial CONOPS % of initial site surveys completed for development of requirements
Army Mobility	The long-range vision for Army mobility clearly articulates the capabilities required to enable Army users to perform missions anywhere, at any time, and lays the foundation to achieve these capabilities through various mobility-related initiatives.	Army Mobile Vision is signed and published by planned suspense Progress in developing the implementation plan
Key Management Infrastructure (KMI)	The confidentiality, integrity and availability of Army-wide communications are fully enabled by KMI, providing a unified, interoperable and trusted infrastructure for establishing, using, operating and managing cryptographic products and services in a net-centric environment.	# of accounts fully transitioned out of the number planned
Identity and Access Management (IdAM) / Common Access Card (CAC) / Public Key Infrastructure (PKI)	Leverage a single trusted set of authoritative identity credentials to authenticate, authorize and audit users' (military, civilian, contractor, etc.) network transactions over DoD and Army resources (19 Army NIPRNet and five SIPRNet forests).	The Army Directory & Identity Synchronization Service (DISS) will populate 19 Army NIPRNet directories and five SIPRNet directories with DoD identity data by the end of FY17.
Civilian Cyberspace Workforce	Cyberspace personnel are fully integrated into the Army workforce across all components and the warfighting domain, supported by a robust workforce strategy, an implementation plan and a comprehensive career management plan.	# of civilian workforce roles aligned with military Career Field 17 Develop civilian cyberspace workforce strategy, to include implementation plan and career management plan, by the end of FY17
Insider Threat	Threat information and risk-based analytic support is enhanced Army-wide by insider threat initiatives, enabling the Army to mitigate current and emerging insider threats.	# of user accounts monitored out of total number planned for the fiscal year
Information Security Continuous Monitoring (ISCM)	Establish an ISCM framework that enables near-real time risk assessment of mission and business information systems.	50% of Army enterprise is continuously monitored by the first quarter of FY18
Cryptographic Modernization Initiative (CMI)	Legacy equipment is effectively divested, new cryptographic technology is integrated, and guidance, policies and standards are in place to ensure that the Army network and operations are fully supported by the latest cryptographic capabilities.	% of legacy equipment fully divested Progression of guidance, policies and strategies being developed in FY17 (i.e., 1QFY17 milestones met, 25% complete)

Initiative	KPI	Measure
Big Data/Cyber Analytics	Army-wide cyber situational awareness is enhanced by cyber analytics, allowing network managers to more effectively protect the network and execute defensive cyberspace functions.	# of cyber analytics use cases developed by Network Enterprise Technology Command (NETCOM)
Spectrum Management Operations (SMO)	Army spectrum managers have the tools necessary to accurately assess the spectral environment as it changes and effectively execute their missions – in this case, the Electronic Warfare Planning & Management Tool (EWPMT).	The progression of EWPMT Capability Drops 1 & 2 against what is planned as a fully realized solution
Standardize Network Operations (Tools Convergence, IES, Metadata)	Network operations and Army-wide IT processes, governance, architecture, etc. are streamlined to a degree sufficient to eliminate redundancies, realize cost savings, and identify and fill gaps in order to reach the goal of a standardized, interoperable end-to-end network.	Establishment of Network Operations (NETOPs) Tools Repository per established timeline # of NETOPS tools eliminated by functional capability category % of cost savings realized from reduction in tools and the associated licenses, hardware and operational support

Table 4-3: NSD KPIs

Appendix 5 – Glossary

TERM	DEFINITION
Automated Mission Mapping Operations	A standalone, semi-automated mission mapper that provides a mission-centered prioritization of vulnerabilities. The vulnerabilities most threatening to mission success get priority for mitigation.
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 between 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 the 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)
Cyber Cloud Operation Services (CYCLOPS)	CYCLOPS consists of two analytics, Boombox and Leaderboard. Boombox allows cyber analysts to observe event trends between organizations, regions and IPs, and the volume of events that occur between two end points. Leaderboard uses DISA-provided whois data, GeoLite City data and combatant command-provided LAN data to map IP addresses to a three-level organizational hierarchy. Used in conjunction with a temporal anomaly detector, it provides a fine-grained view of network anomalies by command element.
Cybersecurity	The ability to provide the measures that protect, defend and restore information and information systems. (JCA 6.1.3)
Dagger	A tailorable mission dependency tool that visually links a mission to the key computer, network, power and cooling components and systems that support the mission. It provides the commander automated decision support, mission planning and real-time course-of- action analysis to help answer questions (e.g., Can the mission succeed? How does the loss or degradation of component X affect the mission? What are my priorities for restoring components?). It uses live data feeds from the Cloud Analytic Platform to display the status of components with an easy-to-read green (good) to red (bad) scale.

TERM	DEFINITION
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) Enterprise resource planning (ERP enclave environment, which contains ERP technologies using 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, which 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 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 components' 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	The ability to provide a virtual computing capability to an end user or application through federation of distributed, location-independent computing resources. (JCA 6.2.2.2)
Doc Holliday	An analytic tool that enables an analyst to quickly discover potential web and structured query language injection (SQLi) attacks. This analysis combines a number of behavioral and signature-based indicators to extract potential web and SQLi attacks.
End-User Services	The ability to provide client computing devices and 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 to access information, applications and services. (JCA 6.2.2.4)
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 and/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)

TERM	DEFINITION
Long-Haul Telecommunications	The ability to disseminate, transmit and/or receive voice, data, video and integrated telecommunications via wire or optical means to, from and between platforms and/or fixed locations (e.g., command posts, installations or federal buildings). (JCA 6.1.1.1.2)
Line of Sight	The ability to exchange data or information via electromagnetic spectrum within the line of sight. (JCA 6.1.1.2.1)
Net Management	The ability to configure and reconfigure networks, services, the underlying physical assets that provide end-user services, and connectivity to enterprise application services. (JCA 6.1.2)
Network Operations Tools Convergence	Network Operations Tools Convergence is the effort to develop, assess, align, standardize and integrate network operations capabilities used to manage, monitor and defend Army IT networks, while eliminating redundancies.
Network Resource Visibility	The ability to determine 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 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	The ability to determine accurate and precise location, orientation, time and course corrections anywhere in the battlespace, and to provide timely and assured position, navigation and timing 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 ability to prevent unauthorized access. (JCA 6.1.3.2.1)
Protect Against Denial or Degradation of Services	The ability to prevent or contain activities that may degrade or deny authorized use of network resources. (JCA 6.1.3.2.2)
Protect Against Disclosure or Modification of Data	The ability to prevent or contain activities that may expose or modify data. (JCA 6.1.3.2.3)
Protect Data and Networks	The ability to anticipate and prevent successful attacks on data and networks. (JCA 6.1.3.2)
Provisioning Convergence	The consolidation of support for NIPRNet and SIPRNet workstations, local networks and peripherals, and standard capabilities in Army Sensitive Compartmented Information Facilities (SCIF).
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.

TERM	DEFINITION
Solution Architecture	Framework or structure that portrays the relationships among all of the elements of a solution to a problem. This architecture type is not part of the DoD Enterprise Architecture but is used to define a particular project to create, update, revise or delete established DoD activities. A solution architecture may be developed to update or extend one or more of the other architecture types. A solution architecture is the most common type of architecture developed in DoD. Solution architectures include, but are not limited to, service-oriented architectures developed in support of specific data and other services solutions.
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)
Transport Convergence	The merging of command and control, intelligence, logistics and medical systems (and networks) onto a common network architecture.
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 6 – Acronyms

ACRONYM	DEFINITION
ABAC	Attribute-Based Access Controls
ACAS	Assured Compliance Assessment Solution
ACC	Advanced Cryptographic Capabilities
AEDC	Army Enterprise Data Center
AEN	Army Enterprise Network
AENC	Army Enterprise Network Council
AESD	Army Enterprise Service Desk
AESD-E	Army Enterprise Service Desk – Europe
AESD-F	Army Enterprise Service Desk Federation
AESD-G	Army Enterprise Service Desk – Guard
AESD-K	Army Enterprise Service Desk – Korea
AESD-M	Army Enterprise Service Desk – MEDCOM
AESD-MP	Army Enterprise Service Desk – MEPCOM
AESD-P	Army Enterprise Service Desk – Pacific
AESD-PO	Army Enterprise Service Desk – Program Office
AESD-R	Army Enterprise Service Desk – Reserve
AESD-S	Army Enterprise Service Desk – SWA
AESD-T	Army Enterprise Service Desk – Tactical
AESD-USAREC	Army Enterprise Service Desk – U.S. Army Recruiting Command
AESD-W	Army Enterprise Service Desk –Worldwide
AESM	Army Enterprise Service Management
AESMF	Army Enterprise Service Management Framework
AKO	Army Knowledge Online
AMC	Army Materiel Command
AMMO	Automated Mission Mapping Operations
ANCP	Army Network Campaign Plan
APCE	Army Private Cloud Enterprise
AR	Army Regulation
ARCYBER	Army Cyber Command
ARL	Army Research Lab
ARNG	Army National Guard
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ASMO	Army Spectrum Management Office
ATEC	Army Test and Evaluation Command
ATM	Asynchronous Transmission Mode
AWA	Army Warfighting Assessment
B2B	Business to Business
BCT	Brigade Combat Team
BDP	Big Data Platform

ACRONYM	DEFINITION
B/P/C/S	Base/Post/Camp/Station
CAC	Common Access Card
CARR	Cyberspace Acquisition, Requirements and Resourcing
CD	Capability Drop
CDC	Core Data Center
CDD	Capability Development Document
CE	Computing Environment
CIO	Chief Information Officer
CMI	Cryptographic Modernization Initiative
CMRS	Continuous Monitoring and Risk Scoring
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COCO	Commercially Owned/Commercially Operated
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial Off the Shelf
CP	Command Post
CPB	Cyber Protection Brigade
CPT	Cyber Protection Team
CS	Capability Set
CSA	Chief of Staff of the Army
CSDIP	Cybersecurity Discipline Implementation Plan
CSO	Cloud Service Offering
CYCLOPS	Cyber Cloud Operation Services
DA	Department of the Army
DC/C/GF	Data Center/Cloud/Generating Force
DCO	Defensive Cyberspace Operations
DCOI	Data Center Optimization Initiative
DCO-IDM	Defensive Cyberspace Operations - Internal Defensive Measures
DCO-MB	Defensive Cyberspace Operations - Maneuver Baseline
DDS	Deployable DCO System
DEE	DoD Enterprise Email
DEOS	DoD Enterprise Office Solutions
DEPS	Defense Enterprise Portal Service
DHA	Defense Health Agency
DISA	Defense Information Systems Agency
DISS	Directory and Identity Synchronization Service
DoD	Department of Defense
DoDIN	DoD Information Network

ACRONYM	DEFINITION
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy
DSS	Defense Information Systems Network Subscription Services
EIE	Enterprise Information Environment
EIEMA	Enterprise Information Environment Mission Area
EKMS	Electronic Key Management System
ELA	Enterprise License Agreement
EMS	Electromagnetic Spectrum
EMSO	Electromagnetic Spectrum Operations
ESB	Expeditionary Signal Battalion
ESD	Enterprise Services Domain
EUD	End-User Device
EUS	End-User Services
EXORD	Execute Order
EW	Electronic Warfare
EWPMT	Electronic Warfare Planning and Management Tool
FRAGO	Fragmentary Order
FY	Fiscal Year
gbps	Gigabits per Second
GDP	Garrison Defensive Cyberspace Operations Platform
GEF	Global Enterprise Fabric
GISA	Ground Intelligence Support Agency
GPS	Global Positioning System
HBSS	Host-Based Security System
HQDA	Headquarters, Department of the Army
HSMCC	Home-Station Mission Command Center
IaaS	Infrastructure as a Service
IC	Intelligence Community
ICAN	Installation Campus Area Network
IdAM	Identity and Access Management
IES	Information Exchange Specification
IMCOM	Installation Management Command
IMO	Information Management Officer
INSCOM	Intelligence and Security Command
IOC	Initial Operating Capability
IP	Internet Protocol
IPN	Installation Processing Node
IPT	Integrated Project Team
IP VTC	Internet Protocol Video Teleconference
IS	Information System
ISCM	Information Security Continuous Monitoring
ISDN	Integrated Services Digital Network

ACRONYM	DEFINITION
IT	Information Technology
ITSM	Information Technology Service Management
JCA	Joint Capability Area
JIE	Joint Information Environment
JMS	Joint Management System
JRSS	Joint Regional Security Stack
KMI	Key Management Infrastructure
KPI	Key Performance Indicator
LOE	Line of Effort
L/V/C/G	Live/Virtual/Constructive/Gaming
MC	Mission Command
M-Code	Military Code
MEDCOM	Medical Command
MGC	Management Client
MIRC	Migration Implementation and Review Council
MPE	Mission Partner Environment
MPLS	Multi-Protocol Label Switching
MUOS	Mobile User Objective System
NCD	Network Capacity Domain
NEC	Network Enterprise Center
NETCOM	Network Enterprise Technology Command
NETMOD	Network Modernization
NETMOD-C	Network Modernization CONUS
NETOPS	Network Operations
NIE	Network Integration Evaluation
NIPR	Non-Secure Internet Protocol Router
NIPRNet	Non-Secure Internet Protocol Router Network
NOSC-L	Network Operations and Security Center - Light
NSA	National Security Agency
NSD	Network Operations and Security Domain
NSI	National Security Information
O&M	Operation and Maintenance
OCONUS	Outside the Continental United States
OMB	Office of Management and Budget
OPORD	Operations Order
PCWG	Provisioning Convergence Working Group
PEO C3T	Program Executive Office Command, Control, Communications - Tactical
PEO EIS	Program Executive Office Enterprise Information Systems
PfM	Portfolio Management
PKI	Public Key Infrastructure
PMO	Program Management Office

ACRONYM	DEFINITION
PNT	Position, Navigation and Timing
POM	Program Objective Memorandum
PoR	Program of Record
RAF	Regionally Aligned Forces
RCC	Regional Cyber Center
RHN	Regional Hub Node
RMF	Risk Management Framework
SAM	Software Asset Management
SCIF	Sensitive Compartmented Information Facility
SC(T)	Signal Command (Theater)
SINCGARS	Single Channel Ground and Airborne Radio System
SIPR	Secure Internet Protocol Router
SIPRNet	Secure Internet Protocol Router Network
SMO	Spectrum Management Operations
SONET	Synchronous Optical Network
SOUTHCOM	Southern Command
SSRF	Standard Spectrum Resource Format
SSO	Single Sign-On
STAN	Shaping the Army Network
SWA	Southwest Asia
SWB	Software Block
T2C2	Transportable Tactical Command Communications
TCWG	Tools Convergence Working Group
TCN-Lite	Tactical Communication Node – Lite
TDI	Tactical Defensive Cyberspace Operations Infrastructure
TDM	Time Division Multiplexing
TRADOC	Training and Doctrine Command
TTP	Tactics, Techniques and Procedures
UAM	User Activity Monitoring
UAP	Unified Action Partner
UC	Unified Capabilities
USAR	U.S. Army Reserve
VI	Visual Information
VoIP	Voice over Internet Protocol
VTC	Video Teleconference
WGS	Wideband Global SATCOM
WIN-T	Warfighter Information Network - Tactical

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu