

Office of the Army Chief Information Officer/G-6

# ARMY NETWORK CAMPAIGN PLAN

IMPLEMENTATION GUIDANCE

# NEAR TERM

# 2016-17



**CIO/G-6**  
**ENABLING SUCCESS** For Today and Tomorrow



**U.S. ARMY**



CIOG6.ARMY.MIL

**DISCLAIMER**

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

**CHANGES**

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

## Executive Summary

Over the last decade, the Army invested heavily in augmenting and integrating the network's operational component capabilities. Investments in enterprise and installation components, however, remained relatively stagnant, fostering significant disparities. To enable the Army of 2025 to meet the challenges of the 21<sup>st</sup> century, the Army is working to rebalance and unify the network to provide an end-to-end capability. The *Army Network Campaign Plan (ANCP) - Implementation Guidance, Near Term*, first produced in 2015 and now being updated, sets the framework to support the design, development and fielding of network capability enhancements in alignment with the *ANCP* and the *Army Operating Concept*.

The Army will synchronize the hardware, applications and services that support both warfighting and business operations. Using assessments conducted as part of the Army Enterprise Network portfolio management and the Army Warfighting Challenge (AWFC) processes, the Army will continue to maintain and modernize the network in fiscal years (FY) 2016-2017. Efficiencies from FY15 network modernization efforts will be realized over the Future Years Defense Program. In FY16-17, the main goal of network modernization is to change the break-fix methodology that is currently being used and transition to a managed services model, Army Enterprise Service Management, in alignment with DoD and Joint guidance.

This document describes how planned initiatives in FY16-17 will enable the capabilities outlined in the ANCP. The near-term implementation guidance provides direction and insight to align development of enterprise, system-of-systems and solution architectures with Army network strategy and information technology portfolio planning. This document also sets the conditions for the mid-term implementation guidance, which covers capability modernization and associated activities in FY18-22.

The initiatives to be executed in FY16-17 are informed by what was planned and actually executed in FY15, given fiscal realities, with the intent of mitigating the impact of budget realities on network advancements required to support future mission operations and bring the enterprise to the Soldier. Programs of record and other initiatives will focus on end-to-end network integration. Near-term efforts center primarily on increasing bandwidth, improving security and deploying enterprise services within a common operating environment to drive effectiveness, efficiency and security. The Army Chief Information Officer/G-6, along with stakeholders from across the Army, is working to improve the Army network, the services provided, and the ways in which the network enables all Army capabilities.



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

This page intentionally left blank.

## Table of Contents

Introduction.....	7
Army Network Campaign Plan Construct .....	7
ANCP Near-Term Construct.....	7
FY16-17 Planning Guidance .....	9
FY16-17 Primary Efforts .....	11
FY16-17 Supporting Efforts .....	20
Summary .....	25
Appendix 1 – Network Capacity Domain (NCD).....	1-1
FY16-17 Priority Activities .....	1-2
Summary.....	1-12
Appendix 2 – Enterprise Services Domain (ESD).....	2-1
FY16-17 Priority Activities .....	2-2
Summary.....	2-12
Appendix 3 – Network Operations and Security Domain (NSD).....	3-1
FY16-17 Priority Activities .....	3-2
Summary.....	3-21
Appendix 4 – Glossary.....	4-1
Appendix 5 – Acronyms .....	5-1

**UNCLASSIFIED**

This page intentionally left blank.

**UNCLASSIFIED**

## Introduction

Building on the momentum and network-related efforts of FY15, the Chief Information Officer/G-6 (CIO/G-6) is leading near-term activities in FY16-17 to continue the modernization necessary to support Army strategy and missions. The *ANCP – Implementation Guidance, Near Term* captures the major activities within the FY16-17 timeframe and sets conditions for the *ANCP – Implementation Guidance, Mid Term* to resource capabilities in FY18-22.

## Army Network Campaign Plan Construct

The ANCP is composed of three documents that align with the DoD Joint Information Environment (JIE) and the Army Campaign Plan (ACP): 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 yearly. The ANCP is designed to impact network planning activities across the Army and to reflect the budget realities that affected execution in FY15. The table below describes the purpose of each document and the associated timeframes.

ANCP Document	Purpose	Timeframe
<i>Army Network Campaign Plan (ANCP)</i>	<ul style="list-style-type: none"> <li>Links with relevant Army and DoD strategies.</li> <li>Describes network-related end states at a high level and outlines lines of effort (LOEs).</li> </ul>	2020 and Beyond
<i>ANCP – Implementation Guidance, Near Term</i>	<ul style="list-style-type: none"> <li>Describes execution activities within a two-year timeframe.</li> <li>Reflects acquisition, resource and Army mission reality.</li> <li>Guides the design and development of the next network capability set.</li> </ul>	2016-2017
<i>ANCP – Implementation Guidance, Mid Term</i>	<ul style="list-style-type: none"> <li>Focuses on network capabilities.</li> <li>Designed to impact resource planning within Program Objective Memorandum venues.</li> </ul>	2018-2022

**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 second iteration; it reflects FY15 accomplishments and describes FY16-17 planned activities. Aligned with the *ANCP*, it provides the direction for execution-level network activities, and informs the annual HQDA Institutional Network Modernization Execute Order.

The near-term implementation guidance is developed in alignment with the Army Enterprise Network (AEN) domains – Network Capacity (NCD), Enterprise Services (ESD) and Network Operations and Security (NSD) – and in coordination with multiple communities of practice, including functional experts, mission area representatives, information technology (IT) strategic planners, resource planners and managers, and acquisition experts. The AEN domains conduct cross-cutting analysis, utilizing multiple data sources that include: Army strategic guidance, senior leader goals and objectives, current Army mission obligations, the status of Enterprise

Information Environment Mission Area (EIEMA) IT investments, acquisition plans and resourcing plans. Near- to mid-term activities, supported through IT investments, will be aligned, managed and tracked through the CIO/G-6's five lines of effort (LOE).

Described below in Figure 1, LOEs link tasks, effects and conditions to the strategic vision and end state, and help define how individual actions contribute and combine to achieve the outcomes desired in 2020 and beyond. These end states align with the six focused end states codified in the 20 February 2015 Chief of Staff of the Army memorandum regarding the Mission Command 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.

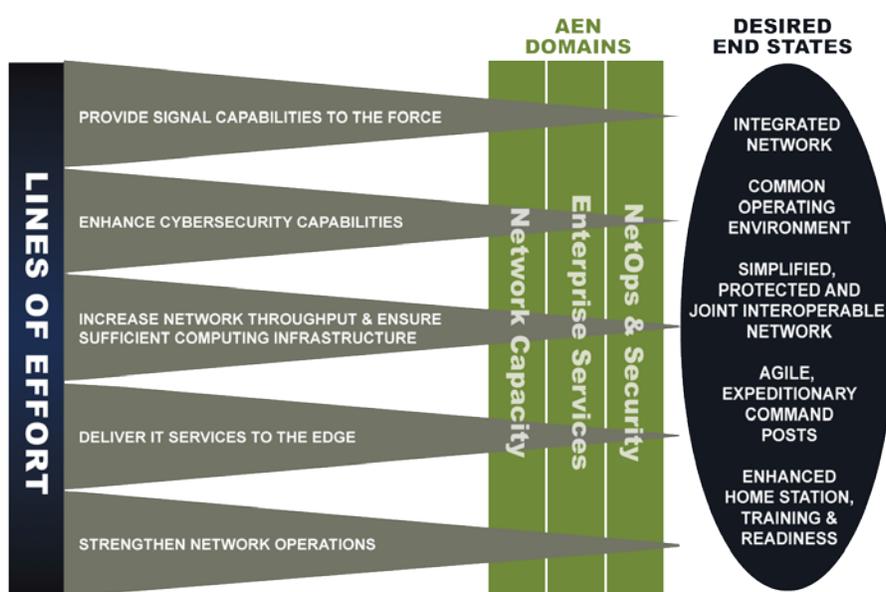


Figure 1: ANCP Operating Construct

LOE goals are outlined below.

**LOE 1, Provide Signal Capabilities to the Force** – Optimize the Signal force to synchronize delivery of future force capabilities; and 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 and Department of Defense 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 to establish common processes and standards. Simplify and standardize network operations capabilities in support of and integrated with DoDIN operations.

The activities planned for FY16-17 execution enable network advancements to support future mission operations and bring the enterprise to the Soldier. They will occur through programs of record and other initiatives to ensure that the institutional network infrastructure is proactively modernized to seamlessly integrate with capability set efforts. Near-term initiatives focus on transitioning Army users from disjointed systems to enhanced and centralized services and Unified Capabilities (UC) that conform to the Common Operating Environment (COE). These changes will return tangible benefits to the user as the Army increases bandwidth, improves security and deploys enterprise services.

### **FY16-17 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 Department of Defense 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 Network Capacity Domain portfolio encompasses DoDIN capabilities related to information transport and computing services; the Enterprise Services Domain encompasses information sharing and core enterprise services; and the Network Operations and Security Domain encompasses network management, cybersecurity and defensive cyber/internal defensive measures.

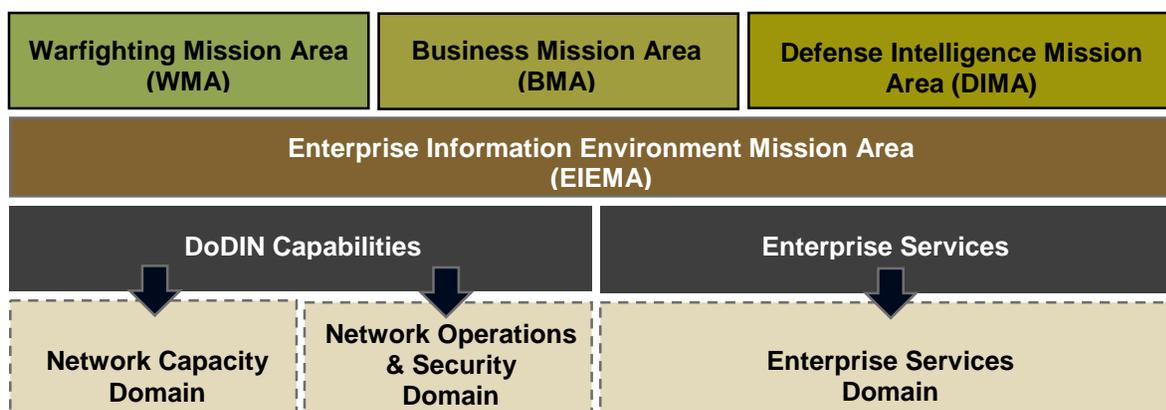


Figure 2: Army IT Portfolio Management Construct

The AEN domain efforts have complex relationships and dependencies, which are critical to reaching desired end states in the near term and which facilitate achieving 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 either to achieve end states in the near term or to set conditions for modernization in follow-on years, e.g., FY18-22. Supporting efforts bolster planned initiatives or deliver forecasted efficiencies. Primary and supporting efforts can occur only within a specific AEN domain or, due to interdependencies, may span multiple AEN domains (i.e., Joint Regional Security Stack installation vs. operation) to achieve a common goal and benefit the network. Details associated with individual activities are covered in depth in Appendices 1 through 3 and are summarized below.

Several strategic resource and environmental factors affect the planning and execution of FY16-17 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 to support achievement of strategic goals.
- **ORGANIZATIONAL STRUCTURE.** Key decision-making entities prioritize resources to achieve strategic goals.
- **INFORMATION.** Critical to resources in order 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 the Army IT processing and services.
- **CULTURE, ETHICS AND BEHAVIOR.** Critical for the organization to realize strategic goals.
- **FINANCIAL.** Discard the break-fix methodology and transition to a managed services model.

## FY16-17 Primary Efforts

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

- Establishing a Common Operating Environment (COE)
- Delivering Unified Capabilities (UC)
- Achieving Operational Component Modernization
- Establishing Home-Station Mission Command Centers (HSMCCs)
- Achieving Network Infrastructure Modernization and Network Consolidation
- Reducing the Cyberspace Attack Surface
- Standardizing Authorized Hosting Environments
- Organizing and Advancing Mobility
- Aligning Army Information Security Continuous Monitoring with the DoD Framework
- Enhancing Cyberspace Situational Awareness (SA) by Leveraging Big Data/Cyber Analytics
- Refining the Role of the Cyberspace Workforce

### *Establishing a Common Operating Environment (COE)*

The COE is an approved set of computing technologies and standards that enable secure and interoperable applications to be rapidly developed and executed across a variety of computing environments. It provides overarching governance, technical guidance and a set of validated technical and non-functional requirements for the centralization, standardization and optimization of IT infrastructure, data center operations and business and mission capabilities. Requirements will be implemented incrementally across successive versions of the COE.

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

- Data Center/Cloud/Generating Force CE
- Command Post CE
- Mounted CE
- Mobile-Handheld CE
- Sensor CE
- Real-Time/Safety Critical/Embedded CE

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. Greater emphasis on incorporating Army

Special Forces into the COE will improve Mission Command and situational awareness between Army conventional and special operating forces during planning and operations.

In FY14, the Army published the *LandWarNet 2020 and Beyond Enterprise Architecture* with Annex A (Technical Standards Guidance for the COE) and Annex B (Definitions and Guidance for the Common Operating Environment). Detailed COE implementation activities were captured in the COE Execute Order for implementation in the operating force (dated 10 September 2014). The G-3/5/7 is the lead for determining when COE compliance across technologies and systems will become mandatory.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Develop a set of validated top-level COE requirements, aligned to the Joint Information Environment (JIE) and Mission Partner Environment (MPE), to guide the design and architecture of the individual CEs.</li> <li>• Implement open standards within the CE architecture.</li> <li>• Field COE iteratively. Successful Army interoperability testing (Army Interoperability Certification) is required prior to introducing new capabilities into the COE.</li> <li>• In coordination with TRADOC, develop communications protocols and data standards mapped to TRADOC-approved information exchange requirements (IERS).</li> </ul>	1	NCD	<ul style="list-style-type: none"> <li>• Facilitates interoperability across environments and foster reuse of common components.</li> <li>• Enables device-agnostic capabilities.</li> <li>• Greater capability agility.</li> <li>• Lower life-cycle costs through standardized applications and unity of effort.</li> <li>• Flexible infrastructure that evolves to match rapidly emerging standards.</li> <li>• Enhanced cyberspace protection.</li> <li>• Alignment with JIE/MPE will position the Army to achieve mission command interoperability between Army conventional and Special forces, and with unified action partners.</li> <li>• Improved mission command interoperability with unified action partners.</li> </ul>
	3	ESD	
	4	NSD	
	2		
	5		

**Table 2: COE Activities and Benefits**

*Delivering Unified Capabilities (UC)*

UC consists 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 for the warfighter and business communities.<sup>1</sup> 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 Mission Command Network should not change radically across echelons, formations or phases of the operation. It should facilitate the transmission of information that warfighters require, regardless of echelon, at the point of need.

---

<sup>1</sup> Department of Defense (DoD) Unified Capabilities Master Plan (UC MP), October 2011.

In FY15, the conditions were set to transition to Internet Protocol (IP) video teleconference (VTC) and the Army produced requirements for a UC soft client enterprise capability. To support the consumption of a UC soft client from a commercial cloud, the Army and the Defense Information Systems Agency (DISA), in partnership with the National Security Agency, crafted a UC Reference Architecture. (Use of a commercial service provider will depend on the computer network defense service provider’s architecture and services, and conformance to Risk Management Framework policy.) Following a request for information to industry, the Army opted for limited institutional deployment of the UC soft client.

In FY16-17, the Army will deploy a pilot of the Microsoft Office 365 Premium product to inform, assess and learn how this solution can support the Army's UC effort and how it can improve daily business processes. The Army also intends to analyze and plan for the consolidation of communications solutions in order to reduce reliance on disparate and legacy communication methods and simplify the user experience.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Limited deployment of soft client capabilities to include chat/instant messaging, soft phone, screen sharing, presence and the continuation of Voice over Internet Protocol (VOIP) and IPVTC either via the Network Enterprise Technology Command theater plan or the DISA Global Video Service (GVS).</li> <li>• Implementation of Microsoft Office 365 pilot.</li> <li>• IPVTC and Time Division Multiplexing (TDM) transition plans in support of DoD-wide efforts.</li> <li>• Develop VoIP user framework for assured and non-assured users.</li> </ul>	4	ESD NSD NCD	<ul style="list-style-type: none"> <li>• Improve user experience with timely access to data at the point of need.</li> <li>• Standardize and improve ease of use.</li> <li>• Reduce operating and sustainment costs.</li> </ul>
	3		
	2		
	5		
	1		

**Table 3: UC Activities and Benefits**

*Achieving Operational Component Modernization*

The capability set process establishes a common equipment baseline through a deliberate and disciplined fielding method that provides a complete, integrated package of network equipment and software to combat formations, from the Tactical Operations Center to the dismounted Squad Leader, rather than introducing new systems and technologies piecemeal. In FY15, three Brigade Combat Teams (BCTs) received capability sets and two others were programmed for fielding.

Concerted efforts will continue in FY16-17 to align the operational and institutional components of network modernization through various bodies, such as the Army Network Synchronization Working Group. The end-to-end alignment of the network’s operational and institutional components will produce a synchronized, interoperable network that improves readiness, training, collaboration with Army Special Operations Forces and HSMCC operations. For example, Soldiers and units will have more direct and transparent access to enterprise-level

services through end-to-end initiatives such as Installation as a Docking Station (IaaS) and the Integrated Training Environment (ITE). The table below describes activities that support this alignment.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Fielding of Warfighter Information Network – Tactical (WIN-T) Increments 1B and 2</li> <li>• Command Post CE 1.0 and 2.0</li> <li>• Institutionalize IaaS concept</li> <li>• Interim en route MC capability</li> <li>• Synchronize HSMCC capabilities with network modernization efforts</li> <li>• Continue Joint Battle Command - Platform (JBC-P) fielding</li> <li>• Rifleman Radio full-rate production decision and fielding (FY16)</li> <li>• Handheld Man Pack full-rate production decision and fielding (FY17)</li> <li>• Field and sustain Army Requirements Oversight Council-validated Tactical Transportable Command and Control (T2C2) bridge</li> </ul>	<p>1</p> <p>3</p> <p>2</p> <p>4</p> <p>5</p>	<p>NCD</p> <p>NSD</p>	<ul style="list-style-type: none"> <li>• Provide more reliable and versatile on-the-move tactical communications, improving collaboration among forces at all levels.</li> <li>• Simplify the network – ease of use, fewer physical components and more agile command posts.</li> <li>• Improve force readiness for no-notice deployments.</li> <li>• Enable deploying forces to develop situational understanding and continue to plan while embarked on strategic airlift.</li> <li>• Ensure that all Army forces are trained and ready prior to deployment.</li> </ul>

**Table 4: Operational Component Modernization Activities and Benefits**

*Establishing Home-Station Mission Command Centers (HSMCCs)*

Divisions and Corps require enduring and fixed operation centers that enable reach-back and reach-forward expeditionary Mission Command even when tactical operation centers are deployed. Enduring command centers are required 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 to establish an interim technical baseline while enduring Army requirements are finalized. The Army will then focus on development of a cloud-enabled Mission Command capability, instantiation of the COE Data Center/Cloud/Generating Force 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 tactical hardware to enable HSMCCs.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Institutionalize IaaS concept</li> <li>• Command Post CE 1.0 and 2.0</li> <li>• Continue deployment of Multi-Protocol Label Switching to installations inside and outside the Continental United States</li> <li>• Continue implementation of Installation Campus Area Networks</li> </ul>	1	NCD	<ul style="list-style-type: none"> <li>• Simplify the network – ease of use, fewer physical components, more agile command posts.</li> <li>• Improve force readiness for no-notice deployments.</li> <li>• Enable deploying forces to develop situational understanding and continue to plan while conducting distributed Mission Command through “reach back.”</li> </ul>
	3		
	2		
	4		
	5		

Table 5: HSMCC Activities and Benefits

*Achieving Network Infrastructure Modernization and Network Consolidation*

In FY15, two operational Non-Secure Internet Protocol Router (NIPR) Joint Regional Security Stack (JRSS) sites became operational. In addition, DISA purchased sufficient equipment for 25 Secure Internet Protocol Router (SIPR) JRSS sites. Multi-Protocol Label Switching (MPLS) routers were installed at 15 installations and were passing traffic as of the end of FY15. Also, DISA fielded Area Core Switches (ACS) and Edge Access Switches (EAS) as part of the Installation Campus Area Network (ICAN) upgrades at 12 CONUS installations.

In FY16-17, the Army will continue to improve institutional network infrastructure while converging and integrating separate networks. The table below summarizes network activities and the benefits to the Army.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Continue deployment of MPLS to installations inside and outside the Continental United States.</li> <li>• Continue the technical integration of separate networks, e.g., Army Reserve, Army National Guard, Corps of Engineers, ITE, Army Materiel Command and Medical Command.</li> <li>• Continue implementation of ICANs.</li> </ul>	3	NCD	<ul style="list-style-type: none"> <li>• Provide sufficient throughput to fully leverage enterprise services and support UC.</li> <li>• Increase reliability, availability and flexibility to enable garrison-based MC operations and live, virtual, constructive and gaming training.</li> <li>• Improve user experience with timely access to data at the point of need.</li> <li>• Divest legacy systems; reduce operating and sustainment costs.</li> <li>• Enhanced security architecture and improved throughput that supports Unified Capabilities.</li> </ul>
	2		
	5		

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

*Reducing the Cyberspace Attack Surface*

In FY16, convergence and consolidation of Top-Level Architecture Stacks into JRSS continue to be a major priority for the Army. The Army’s installation of JRSS NIPR sites and JRSS SIPR sites sets conditions for a more rapid transition to full 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 FY16, the Army will begin to implement plans to re-provision NIPR and SIPR networks that traverse the Intelligence Community’s Ground Intelligence Support Activities (GISA) to the operational control and oversight of the Signal community. The intent is to transition from enterprise NIPR/SIPR/Top Secret provisioning to a single entity, which will lead to greater efficiency in the operation and maintenance of networks, as well as significant cost savings. Additionally, in FY16 community-of-interest (USACE, USAR and ARNG) networks will complete migration behind the JRSS single security architecture.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Converge and consolidate Top-Level Architecture Stacks into Joint Regional Security Stacks</li> <li>• Provisioning convergence</li> <li>• Network tools convergence</li> </ul>	2	NSD	<ul style="list-style-type: none"> <li>• Simplify the network, reduce the network attack surface and standardize network security.</li> <li>• Integrated, simplified, protected and interoperable network.</li> </ul>
	5		
	3		

**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 FY15, a total of 352 data centers had been closed.

The Army simultaneously is pursuing a major rationalization effort for current applications, systems and data. In FY15, three applications were migrated to Core Data Centers (CDCs) and 41 were terminated. The Army Application Migration Business Office (AAMBO) received 262 review requests in preparation for migration to DISA CDCs or the commercial cloud.

Rationalization and consolidation are laying the computing foundation for future-year data support and data analytics across the network. Enterprise service hosting, for capabilities such as email, UC, file sharing, mission software and the Army Software Marketplace, will be executed through the Data Center/Cloud/Generating Force Computing Environment. In FY16, the Army will refine requirements, policies, and resource and transition planning, and in FY17 pursue acquisition of all these services.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Continue to transition standalone data centers to DoD-authorized hosting environments.</li> <li>• Designate standard Installation Processing Nodes (IPN) and Installation Service Nodes (ISN). Establish service-oriented standard operating procedures.</li> <li>• Rationalize, virtualize and migrate applications to DoD-authorized hosting environments (application migration to NIPRNet enclave in commercial and DoD hosting environments).</li> <li>• Standardize Core Data Centers.</li> <li>• Develop and publish an Army application hosting methodology.</li> </ul>	3	NCD ESD NSD	<ul style="list-style-type: none"> <li>• Provide robust data storage, on-demand computing, elastic capacity, improved security and more efficient operation and maintenance.</li> <li>• Reduce the operating force footprint in theater.</li> <li>• Enable rapid and more efficient evolution of applications, minimizing costs and speeding dissemination of application enhancements.</li> <li>• Support the processing of large amounts of data to improve decision-support cycles.</li> </ul>
	4		
	2		
	5		
	1		

**Table 8: Standardized Authorized Hosting Environments Activities and Benefits**

*Organizing and Advancing Mobility*

Mobility is the core of Army operational capability. To execute their missions, 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 housed. This ability to be “always connected” is directly contingent on modernization initiatives to 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 that can easily be integrated into the network and withstand the operational environment.

In FY14, the Army published the End-User Device (EUD) Reference Architecture. Creating an EUD Strategy and associated execution plans, which will complement the forthcoming Army Mobility Strategy, is a major initiative in FY16-17. While an optimal enterprise mobility capability will not be fully achieved in FY16-17, 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 and robust applications from multiple devices.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Develop and publish an End-User Devices Strategy that supports the Army, to include traditional reserve component Soldiers.</li> <li>• Select, standardize and certify EUD platforms across the Army, with a focus on commercial devices.</li> <li>• Rationalize commercial contracts that provide devices and transport infrastructure to the Army.</li> <li>• Leverage the DISA effort to establish a mobile device store to centralize the hosting and availability of vetted applications that support Army users.</li> <li>• Leverage the DISA effort to establish a mobile device manager (MDM) to manage devices and the transport infrastructure.</li> <li>• Identify multifactor authentication technologies, other than Public Key Infrastructure (PKI), that meet DoD requirements.</li> <li>• Develop and publish a Mobility Strategy.</li> </ul>	<p>3 4 2 1 5</p>	<p>NCD ESD NSD</p>	<ul style="list-style-type: none"> <li>• Ensure that the Army is on a modernization path that keeps pace with the evolving technology environment.</li> <li>• Provide an efficient, consistent, secure and reliable mobile device management process, resulting in cost savings and collaboration.</li> <li>• Standardize and simplify the end-user experience across devices.</li> </ul>

**Table 9: Mobility Activities and Benefits**

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

Continuous monitoring of security controls assists in maintaining ongoing awareness of information security, vulnerabilities and threats, which helps inform organizational risk-management decisions. In FY15, the Army began to align ISCM initiatives with the DoD ISCM Framework and optimized the Host-Based Security System (HBSS) SIPR baseline through deployment of the Device Control Module (DCM), which enhanced asset information reporting. The Army also deployed Assured Compliance Assessment Solution (ACAS) Security Center and Nessus modules, thereby operationalizing this asset management capability.

In FY16, the Army will continue its multi-year, iterative effort to align with the ISCM Framework, which will leverage current investments in enterprise and non-enterprise cybersecurity tools and capabilities.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Optimize Host-Based Security System implementation.</li> <li>• Enhance asset information reporting.</li> <li>• Operationalize continuous monitoring risk scoring (CMRS).</li> <li>• Operationalize the Assured Compliance Assessment Solution.</li> <li>• Reduce self-reporting.</li> <li>• Correlate operational attributes.</li> <li>• Enable correlation of vulnerability configuration data.</li> <li>• Enable program-of-record reporting.</li> <li>• Converge compliance scoring.</li> <li>• Provide support to insider threat initiative.</li> </ul>	<p>2</p> <p>5</p>	NSD	<ul style="list-style-type: none"> <li>• Provide the Army the ability to make continuous risk-management and authorization decisions.</li> <li>• Maintain ongoing awareness of information security vulnerabilities and threats to support organizational risk-management decisions by producing risk scores.</li> <li>• Drive down vulnerabilities in Army information systems.</li> <li>• Create a top-down culture of cybersecurity compliance.</li> </ul>

Table 10: ICSM Activities and Benefits

*Enhancing Cyberspace Situational Awareness by Leveraging Big Data/Cyber Analytics*

Big Data/cyber analytics is the use of substantially more computational power to run advanced analytical tools against data sets whose size is beyond the ability of typical database software tools to capture, manage and analyze. The true value of Big Data/cyber analytics is achieved when an organization applies advanced analytics to very large, rapidly changing and different types of data sets for decision making and operations. As the Army generates more and more information about the range of threats and its personnel, training, materiel, finances and operations, it has an opportunity to enable better and quicker decisions and to be more operationally focused.

In FY15, NSD integrated its efforts with U.S. Army Cyber Command/Second Army (ARCYBER/Second Army) to conduct a pilot project at the Army Research Laboratory (ARL). The pilot involved collaboration with multiple government, academic and private research laboratories, and produced several advanced analytic capabilities that can be applied to generating cybersecurity situational awareness.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Integrate Big Data management into the Army Data Strategy.</li> <li>• Continue implementation of Big Data/cyber analytics pilot projects.</li> </ul>	<p>2</p> <p>5</p>	NSD	<ul style="list-style-type: none"> <li>• Improve cyber workforce experience by providing timely access to data to make informed and actionable risk-management decisions.</li> <li>• Reduce time required to perform cyber analytics and forensics.</li> <li>• Provide leadership near-real-time risk information to make informed decisions.</li> </ul>

Table 11: Big Data/Cyber Analytics Activities and Benefits

*Refining the Role of the Cyberspace Workforce*

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

In FY15, the Army began aligning civilian workforce roles with the military Career Field 17 structure and focusing on getting policies, strategies and plans approved and codified. In FY16, the Army will continue to refine its cyberspace workforce activities in the same focus areas.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>Identifying, shaping and tracking the civilian cyberspace workforce.</li> <li>Defining work roles.</li> <li>Aligning the cyberspace civilian workforce with the military.</li> <li>Aligning the COE with training and education opportunities.</li> </ul>	2 5 3	NSD	<ul style="list-style-type: none"> <li>The development and retention of an exceptional cyber workforce is central to DoD's strategic success in cyberspace.</li> </ul>

Table 12: Cyberspace Workforce Activities and Benefits



Figure 3: Organization of IT, Cyber and Intelligence Workforce

**FY16-17 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
- Cryptographic Modernization Initiative (CMI)
- Providing Army Enterprise Service Management (AESM)
- Enhancing Identity and Access Management (IdAM)
- Establishing and Leveraging Enterprise License Agreements

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

*Standardizing Network Operations*

Standardizing DoDIN operations across the Army will increase effectiveness, availability and performance of the DoDIN-Army. 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 from the generating force to the far reaches of the Army’s theater, expeditionary and contingency environments.

In FY15, the Army established a collaborative integrated product team (IPT) and published strategies, frameworks, standards, processes, policies and guidelines to set the conditions for implementation in subsequent years. In FY16-17, the Army will continue to standardize Army DoDIN operations through the Army DoDIN operations tools convergence strategy, developing and improving Army DoDIN operations policies, and publishing Army DoDIN operations metadata requirements, interoperability specifications and configuration control processes.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Implement the DoDIN concept of operations.</li> <li>• Oversee compliance with DoDIN operations technical information exchange specifications.</li> <li>• Develop and publish DoDIN operations metadata requirements.</li> <li>• Implement the DoDIN operations tools framework for tools identification and categorization.</li> </ul>	5	NSD	<ul style="list-style-type: none"> <li>• Simplified and standardized network operations.</li> <li>• Interoperable end-to-end network operations.</li> <li>• Visibility and accountability of all Army network operations tools.</li> </ul>

**Table 13: Network Operations Activities and Benefits**

*Increasing the Agility of Spectrum Management Operations*

Spectrum operations facilitate implementation of the wireless portion of net-centric warfare. Understanding the operational process in planning, managing and employing this resource is critical to the conduct of all warfighting functions.

In FY15, the Army established and adopted plans, strategies, standards and practices to set the conditions for implementing enhanced spectrum management operations in subsequent years. FY16-17 will see a concerted effort to simplify and consolidate spectrum management tools. The convergence of multiple tools to enterprise-level solutions will provide spectrum managers greater visibility of the electromagnetic operating environment to assign access to and de-conflict use of the electromagnetic spectrum (EMS) in congested and contested environments. Additionally, the Army will be able to divest standalone, redundant solutions, and to implement DoD spectrum data and architecture standards to support the COE and Big Data/cyber analytics.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Transition multiple spectrum management tools to enterprise-level network operations tool solutions.</li> <li>• Implement spectrum data and architecture standards.</li> </ul>	<p>5</p> <p>3</p> <p>1</p>	NSD	<ul style="list-style-type: none"> <li>• Simplify network management.</li> <li>• Provide automated EMS reporting capabilities in near-real time to make informed decisions.</li> <li>• Enable more efficient use of spectrum resources and prioritize in congested bands.</li> </ul>

Table 14: Spectrum Management Activities and Benefits

*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 Sustainment Readiness Model (SRM) (formerly Army Force Generation (ARFORGEN)). In FY16, the Army will implement and establish new standards by publishing the Army Communications Security (COMSEC) Strategy and implementation guidance. These efforts will set the foundational framework and provide a roadmap 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 national security information.

In FY17, the Army will see a transformational effort to simplify and enhance the network to extend enterprise services to the tactical edge; therefore, cryptographic and key management capabilities must enable the exchange of secure, authentic voice, video and data between authorized individuals, groups and entities across the entire Army and among unified action partners. Persistent modernization of these capabilities will enhance the confidentiality, integrity and availability of information, and support the Army requirement to increase network capacity and improve network performance. These objectives are accomplished by replacing the legacy technology, waveforms, algorithms and cryptographic equipment used to defend information systems and networks against evolving cyberspace threats.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>• Provide an “over-the-network-keying” (OTNK) management capability.</li> <li>• Transition from Electronic Key Management System to Key Management Infrastructure.</li> <li>• Modernize cryptographic capabilities (devices, waveforms, algorithms, etc.).</li> <li>• Replace legacy technology, waveforms, algorithms and cryptographic equipment.</li> <li>• Publish Army Communications Security Strategy, which addresses Advanced Cryptographic Capabilities (ACC) and standards.</li> </ul>	<p>2</p> <p>5</p> <p>1</p>	NSD	<ul style="list-style-type: none"> <li>• Decrease manual key delivery, minimizing the number of Soldiers placed in harm’s way.</li> <li>• Enhance programmable and interoperable encryption capability to ensure exchange of authentic data, information and knowledge between authorized individuals, groups and entities.</li> <li>• Enhance network encryption capability for improved network performance.</li> <li>• Modernized cryptographic equipment and upgraded key management infrastructure capabilities in line with COMSEC Strategy.</li> </ul>

**Table 15: Cryptographic and Key Management Capabilities Activities and Benefits**

*Providing Army Enterprise Service Management (AESM)*

In FY15, 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 effectiveness, improving security 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 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 FY16-17, the Army will determine the processes to begin preparation for implementation, conduct maturity assessments and identify opportunities for improvement. ITSM improvements will align the Army with DoD and joint efforts while 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
<ul style="list-style-type: none"> <li>Implement the AESM Framework.</li> <li>Enhance the Army Enterprise Service Desk (AESD) to improve Tier 0 and Tier 1 services to end users.</li> <li>Deliver Enterprise Service Management System as a Service (ESMSaaS) to improve IT services.</li> </ul>	4	ESD NCD NSD	<ul style="list-style-type: none"> <li>Provide value to Army users by delivering IT services effectively, securely and efficiently.</li> <li>Eliminate the time, cost, effort and distraction associated with running local and internal service management platforms.</li> </ul>
	5		
	3		
	2		
	1		

Table 16: AESM Activities and Benefits

*Enhance Identity and Access Management (IdAM)*

In FY15, the Army developed strategies, policies and architectures to support the establishment of a single, managed identity for users throughout their career, which will decrease the amount of time users are without network connectivity while transitioning between duty stations. In the FY16-17 timeframe, the Army will provision and synchronize 19 NIPRNet Active Directory forests utilizing Army Directory & Synchronization Services (DISS). The Army will also continue to leverage identity management solutions to enhance users’ ability to search for personnel on the network. This effort will be synchronized with global force information management within the JIE construct. Additionally, the Army plans to identify, standardize and implement multifactor authentication processes to complement the National Security Systems (NSS) and DoD PKI infrastructures to enhance operational security in austere environments.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>Continue identity and access management (IdAM) efforts to establish life-cycle management for user identities.</li> <li>Leverage user identity solutions to support directory services.</li> <li>Identify non-PKI multifactor authentication technologies that meet DoD requirements.</li> </ul>	2	NSD ESD	<ul style="list-style-type: none"> <li>Improved security for authentication, authorization and accountability of user network transactions.</li> <li>Decrease the time users are without network connectivity while transitioning between duty stations.</li> <li>Provide a reliable directory to locate users.</li> </ul>
	4		
	5		

Table 17: IdAM Services Activities and Benefits

*Establish and Leverage Enterprise License Agreements (ELAs)*

By the end of FY15, the Army had 15 ELAs or joint ELAs in place, eliminating redundant and unnecessary contracts and getting more from Army dollars by leveraging scale to deliver significant savings. In FY16, the Army’s focus is creating new Joint ELAs for Microsoft, Adobe and VMware products, as well as new Army ELAs for BMC and Symantec/Veritas enterprise requirements. The Army will fully support and implement DoD-wide plans for the transition to Microsoft Windows 10 by the end of FY16.

Network Activities	LOEs	AEN Domains	Army Benefits
<ul style="list-style-type: none"> <li>Negotiate and maintain ELAs with vendors that support the network.</li> <li>Enterprise software management.</li> <li>Address top initiatives, such as operating system migration, through JELA negotiations.</li> </ul>	<p>4</p> <p>3</p> <p>5</p>	<p>ESD</p> <p>NSD</p> <p>NCD</p>	<ul style="list-style-type: none"> <li>Centralize the Army’s purchasing power to potentially provide the Army larger amounts of software/equipment at a lower cost per item.</li> </ul>

Table 18: ELAs Activities and Benefits

Summary

To enable the Army of 2020 and beyond to meet the challenges of the 21<sup>st</sup> 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 to enable a resilient, easy-to-use and available network. It is critical for senior leaders across the Army to understand the relationships and interdependencies among activities occurring within each of the AEN domains and LOEs. The near-term implementation guidance provides the context to guide network modernization activities in FY16-17, synchronizing planning with the realities of Army mission obligations, the resourcing picture and changes in acquisition practices. This will ensure that modernization efforts are coordinated and, when solutions are delivered, they can be fully utilized to their optimal potential by Army users.

FY16-17 primary efforts will set the infrastructure foundation to achieve the vision for Network 2020 and Beyond in support of the Army Operating Concept. Network infrastructure modernization will dramatically improve network capacity and strengthen network security. Greater capacity and security will enable COE implementation and delivery of Unified Capabilities. They also will allow the operating force to leverage institutional capabilities, such as home-station operations centers and global Core Data Centers 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. In addition to infrastructure efforts, the CIO/G-6 will aggressively lead the evolution of the cyberspace 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 FY16-17 include the standardization of network operations capabilities to more effectively manage the Army’s single network environment. The Army will modernize cryptographic and key management capabilities, enhance identity and access management, directory services and public key infrastructure, enable key information terrain and increase the agility of spectrum management operations. The Army will continue to expand enterprise services management and the use of enterprise license agreements to optimize economies of scale and ensure Army-wide distribution of the most up-to-date capabilities and tools.

Each of the AEN domains has an appendix that discusses in detail the activities planned for FY16-17.

## Appendix 1 – Network Capacity Domain (NCD)

The NCD portfolio includes the physical IT infrastructure over which all data, voice and video services and information-based activities must pass. The NCD portfolio provides the essential “information highway” for conducting wartime and traditional business communication operations. Both the ESD and the NSD require this infrastructure to effectively operate the systems within their portfolios.

The efforts below are driven by this implementation guidance and 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*. This memo identifies the need for a robust transport infrastructure that provides sufficient, modern, resilient and reliable computing and storage capacity, in addition to enabling end-user device and mobile capabilities. It mandates migration of applications, systems and data to DoD-approved enterprise hosting facilities (EHF) by the end of FY18, thus driving FY16-17 data migration activities. The 9 July 2014 Under Secretary of the Army memorandum titled *Migration of Army Enterprise Systems/Applications to Core Data Centers* provides further guidance on the procedure for data center consolidation and application rationalization.

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 and unified action partners the full range of military and business operational advantages across all joint operational phases.

The NCD will produce three outcomes in FY16-17.

1. A resilient transport network designed to manage throughput to meet demand.
2. An optimized, responsive computing and storage capability, and the capability to identify opportunities to mitigate demand.
3. A standardized range of user device options.

### FY16-17 Priority Activities

In FY16-17, 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 FY16-17 NCD activities and shows their alignment to Joint Capability Areas.

FY16-17 NCD Activities	Joint Capability Area 6 Communications and Computers									
	6.1 DoDIN Capabilities						6.2 Enterprise Services			
	6.1.1 Information Transport						6.2.2 Computing Services			
	6.1.1.1 Wired Transport		6.1.1.2 Wireless Transmission		6.1.1.3 Switching and Routing		6.2.2.1 Shared Computing	6.2.2.2 Distributed Computing	6.2.2.3 Server Services	6.2.2.4 End-User Services
	6.1.1.1.1 Localized Communications	6.1.1.1.2 Long-Haul Telecommunications	6.1.1.2.1 Line of Sight	6.1.1.2.2 Beyond Line of Sight	6.1.1.3.1 Communication Bridge	6.1.1.3.2 Communication Gateway				
Network Infrastructure Modernization and Path Diversity	•	•	•	•	•	•				
Integrate Separate Networks	•	•	•	•	•	•				
Improve Transport Capacity for Deployable Forces			•	•	•	•				
Data Center and Application Consolidation; IPN/ISN/SPPN Standardization							•	•	•	
EUD Strategy										•
Divestiture Planning	•	•	•	•	•	•	•	•	•	•

Table 19: 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) at major installations. Infrastructure modernization will ensure that installations have dual-path diversity to minimize or mitigate the impact of network transport interruptions on critical user communities. The Army National Guard (ARNG), United States Army Reserve (USAR) and Army Corps of Engineers (USACE) are working to converge upon the DoD enterprise network architecture, improving throughput and connectivity for the National Guard, Joint Force

## UNCLASSIFIED

Headquarters, armories, Reserve centers and active component installations. These efforts also will strengthen network security. FY16-17 targeted priorities are critically dependent upon available resources. 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 FY14-15, network infrastructure modernization projected and actual accomplishments included:

- Projected: Installation of NIPR JRSS at 23 sites.  
Actual: DISA completed installation at two sites (JBSA and Montgomery), both of which are operational.
- Projected: Installation of SIPR JRSS at 25 sites.  
Actual: DISA purchased sufficient equipment for 18 SIPR sites. It also refined Joint Migration Team (JMT) and Service Migration Team (SMT) roles and responsibilities to meet CIO/G-6 FY16 migration priorities.
- Projected: Installation of MPLS at 20 sites.  
Actual: DISA installed MPLS at 15 installations in FY15, all of which are operational.
- Projected: Installation of 17 ICANs via ACS and EAS on CONUS installations.  
Actual: 13 installations received switches in FY14-15 and are operational.
- Projected: Upgrade optical pathway links at 10 CONUS installations.  
Actual: 7 optical links delivered in the Southeast and Southwest CONUS regions in FY15.
- Projected: Replacement of Asynchronous Transmission Mode (ATM) and Synchronous Optical Network (SONET) equipment at 54 sites on the Korean peninsula.  
Actual: Completed site surveys at 15 sites (Phase 1 sites) in FY15.

In FY16-17, network infrastructure modernization activities (as resources allow and in accordance with G-3/5/7 priorities) include:

- Continuing deployment of MPLS upgrades at 47 sites in CONUS, Southwest Asia (SWA) and Europe while initiating build-out efforts in the Pacific theater.
- Migrating a minimum of five installations per quarter (and a maximum of nine) to JRSS.
- Continuing to increase throughput for ICANs via ACS and EAS at 11 CONUS and SWA installations. The goal is to complete the remaining six installations in FY16.
- Continuing optical transport link upgrades at 10 installations.
- Continuing to field Operational Capability Sets to BCTs, with three BCTs projected for FY16-17.
- Beginning initial HSMCC implementation, in accordance with emerging requirements definition, in FY16, and synchronization and implementation in FY17.
- Developing and implementing a divestiture plan.
- Updating the Network Security Reference Architecture as required.

## UNCLASSIFIED

By the end of FY17, as resources allow, the installation network infrastructure will be modernized (i.e., wide area switching throughput increased to 100 gigabits per second (gbps) and switching capacity for the installation wide area network increased to 10 gbps at the majority of prioritized installations). This improvement is required to accommodate the greater network capacity and speed needed to use the additional applications and services offered by DoD-approved enterprise hosting facilities. Priority installations will have physically diverse access to the 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 HSMCC operations, as well as distributed live, virtual, constructive and gaming (L/V/C/G) training. It also will set the foundation for full integration with the JIE construct, to include the flexibility to scale bandwidth 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 COE Data Center/Cloud/Generating Force Computing Environment, cloud-based enterprise business systems and Unified Capabilities.

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 and sets the conditions for cloud-based hosting of systems and UC. The MPLS design can easily and incrementally be upgraded to 100 gbps of switching capacity as demand evolves, extending the utility of this solution and easing the modernization burden.

### **Integrate Separate Networks**

The integration 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 Army enterprise services, such as UC, to access critical information.

In FY14-15, integration of separate networks projected and actual accomplishments included:

- Projected: Continue to integrate community of interest networks (e.g., Army Reserve, Corps of Engineers, Army Materiel Command and Medical Command 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: ARNG and USACE completed network discovery and two private IP circuits were connected to JRSS at JBSA and Montgomery. Completed a characterization test with WIN-T networks and the WGS architecture in December 2014. Published detailed technical procedures for the use of the WIN-T Network-Centric Waveform over the WGS architecture. (Funding constraints delayed network modernization initiatives, thereby directly impacting integration of separate networks.)

## UNCLASSIFIED

In FY16, integration of separate networks activities include:

- Continue integration of community of interest networks (e.g., Army Reserve, Corps of Engineers and National Guard networks).
  - Develop and coordinate memorandum of understanding with stakeholders for JRSS operations.
  - Complete JRSS migration and acceptance.
- Set the conditions for integration of deployable network transport solutions into a unified information transport delivery capability.
- Transition network modernization efforts from the NCD to the NSD for Joint Management System (JMS) implementation.
- Confirm and publish TTPs for the use of WGS with WIN-T systems.

In FY17, the CIO/G-6 and the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)) will continue to integrate separate institutional networks into the enterprise network and to collaborate on COE implementation. By the end of FY17, targeted installations will have one unified transport network, improving network efficiency and effectiveness. This unified network will facilitate faster data transfer, 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 deployment of Operational Capability Sets (OCS). OCS fielding will be executed in accordance with HQDA Execute Order (EXORD) 244-12, and will incrementally enhance the throughput and agility of the tactical network and extend it further down into tactical formations. In FY16-17, planned capabilities include mission command on the move (OTM) and enhanced command and control/situational awareness (C2/SA) for the dismounted Soldier.

In FY14-15, the projected and actual accomplishments to improve transport capacity for deployable forces included:

- Projected: Field 14 BCTs with modernized OCS.  
Actual: In FY14, four BCTs received OCS. In FY15, two BCTs received OCS.
- Projected: Develop guidance for wireless technologies.  
Actual: In FY15, CIO/G-6 published a guidance memo for use of wireless technologies on the tactical network.

In FY16, activities to improve transport capacity for deployable forces include:

- Continuing to field operational force units' greater capability in accordance with EXORD 244-12.

## UNCLASSIFIED

- Continuing development of the Soldier Radio Waveform, Wideband Networking Waveform, Network-Centric Waveform and High-band Networking Waveform.
- Conducting operational assessments of the WIN-T Inc. 2 Network-Centric Waveform and High-band Networking Waveform.
- Continuing development and developmental testing of the WIN-T Inc. 2 Tactical Communication Node – Lite (TCN-Lite) and the Network Operations and Security Center – Lite (NOSC-L).
- Completing WIN-T Inc. 1B upgrades (by the fourth quarter of FY16).
- Continuing the operational evaluation of intelligence convergence at the BCT level.
- Determining the impact of the Installation Mobility Strategy on the deployed environment and the way ahead for cellular/wireless communications support in the deployed environment.
- Finalizing HSMCC network support requirements.
- Refining IaaS operational and supporting infrastructure requirements in order to improve network connection processes and support L/V/C/G training.
- Refining installation network support requirements for L/V/C/G training.
- Providing secure, robust, jammer-resistant, short-range (<5 km) capability between mobile platforms.

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

- Continuing to modernize tactical formations with WIN-T Increment 2 and Handheld, Manpack and Small Form Fit (HMS) Rifleman Radios through Capability Set fielding.
- Conducting initial operational test and evaluation of Mid-Tier Networking Vehicular Radio (MNVR).
- Conducting initial operational test and evaluation of the WIN-T Inc. 2 TCN-L / NOSC-L.
- Enabling garrison-based HSMCC operations by conducting a technical refresh of existing hardware.
- Setting the conditions for L/V/C/G training from the desktop.
- 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.

Upgrades 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 the commander's capabilities at all levels to collaborate with units distributed across diverse locations. 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. Usage of WGS/MUOS will help reduce the cost of training, while the integration of separate transport networks will increase the reach and agility of the deployable transport infrastructure. Continuing to modernize Regional Hub Nodes (RHNs) as part of the evolution of WIN-T will ensure connectivity between the deployed tactical network

## UNCLASSIFIED

and the enterprise cloud, greatly enhancing accessibility 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.

The T2C2 Very Small Aperture Terminal (VSAT) system will meet the operational need to facilitate the fusion of maneuver, fires, intelligence, operations support and sustainment information by select teams and small units at the front edge of the battlefield with higher headquarters, and will be critical to the Army's ability to conduct unified land operations over extended distances in all tactical terrains. Aerial Networking Nodes will connect UH-60 command-and-control aircraft, the Shadow Unmanned Aerial System and tactical aerostats with existing networks, and will perform bridging or act as a gateway between upper, mid and lower network tiers.

Continued refinement of IaaS will improve force readiness for no-notice deployments, enhance the security of the network, and enable system and operator readiness and proficiency. It will ensure that equipment has the latest cybersecurity and operational patches, and that units can maximize L/V/C/G training opportunities.

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 Sets are fielded to units 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 continue to conform to the Federal Data Center Consolidation Initiative in alignment with the July 2013 DoD CIO memorandum<sup>2</sup> that directed the Services and agencies to consolidate or close a minimum of 60 percent of their data centers by the end of FY18. Army efforts to achieve the 60 percent reduction will continue through 2021 due to technical complexity and resource constraints. In addition, the Army will continue to follow DoD CIO direction to migrate enterprise applications and systems that support users across installation boundaries to DoD CDCs by the end of FY18. Using the data center consolidation effort, the Army will align with the JIE construct for Installation Processing Nodes, Installation Service Nodes (ISNs) and Special Purpose Processing Nodes (SPPNs). Preparation for migration of applications and systems began in FY15 and will continue in FY16. In a controlled manner, CIO/G-6 will assist Commands with migration during FY16-17. CIO/G-6 will then assess Army progress and adjust cloud migration efforts in FY18-21, and become cloud-enabled via the COE Data Center/Cloud/Generating Force Computing Environment.

In FY14-15, the projected and actual accomplishments for data center consolidation and standardization included:

---

<sup>2</sup> Memorandum, Department of Defense Chief Information Officer, 11 July 2013, subject: Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration.

## UNCLASSIFIED

- Projected: In FY14, the mandate was to close 90 data centers.  
Actual: 142 were closed.
- Projected: In FY15, the mandate was to close 135 data centers.  
Actual: 71 were closed.
- Projected: Application owners initiate migration to DISA CDCs or commercial cloud facilities.  
Actual: Three applications migrated to CDCs and 109 were terminated by the end of FY15. The Army Application Migration Business Office received 262 requests for review in preparation for migration to DISA CDCs or commercial cloud facilities.

In FY16, data center consolidation and standardization activities include:

- Continuing application rationalization and migration across Commands, mission areas and domains.
- Migrating applications currently in local data centers to DoD CDCs (designated DISA Defense Enterprise Computing Centers) through application rationalization (decision to sustain or kill, then modernize and virtualize).
- Closing 151 data centers.
- Producing the long-term Enterprise Operations and Management CONOPS.
- Establishing the standard Data Center Computing Environment (DCCE) baseline and plan, in accordance with the COE, which enable JIE concepts, support ISN implementation, facilitate cloud capability, enforce Army and DoD guidelines, and reinforce joint force interoperability.
- Updating the Army Cloud Computing Reference Architecture as required.
- Establishing the Army Private Cloud Enterprise (APCE) as a pilot, and systematically testing, evaluating and refining the acquisition, management and operation approaches for a commercially owned-commercially operated (COCO) private cloud before Army-wide adoption. In the short term, the Army Private Cloud will support Army customers at one location.

In FY17, data center consolidation and standardization activities include:

- Closing 135 data centers.
- Continuing to migrate applications now in local data centers to DoD CDCs (designated DISA DECCs) through application rationalization (decision to sustain or kill, then modernize and virtualize).
- Continuing the standardization and consolidation of data centers to the appropriate JIE-designated ISN or SPPN, or Army-designated EHF.

By the end of FY17, plans and processes will be validated, against previous data center and consolidation activities, for the migration of applications, services and data. Data crossing installation boundaries will only be migrated to approved DoD CDCs (DISA DECCs) or Army-approved enterprise hosting facilities. Applications, services and data not crossing installation

## UNCLASSIFIED

lines will be hosted in IPNs or ISNs. Applications with unique information and support requirements will be identified and the conditions will be set to migrate them to SPPNs.

Commands must holistically analyze, prioritize and plan enterprise-hosting resourcing requirements, then determine the existing/programmed resourcing (within the Command) that can be applied. Resources to refresh existing hardware or to execute major software upgrades will serve as the base for covering costs. Resources recouped from rationalization actions and terminated systems must be internally prioritized and applied to application virtualization efforts. Resource planning and programming actions (based on Army Budget Office artifacts) must be proactively assessed to ensure that correct appropriation sources are in place to support migration/programming requirements and timelines. If resource gaps are identified, the Command must prioritize internally before engaging the Army Budget Office/G-8 for additional resource support. Program Budget Assessment Team review/briefing guidelines will apply.

Data center consolidation and standardization, in concert with the Army Cloud Strategy, will enable the Army to better focus resources for hosting of data, applications and systems to effectively meet evolving mission needs. This effort will produce on-demand computing for the generating force, elastic capacity, better security and more efficient operation and maintenance. By shrinking the data center and network footprint, it also will improve the Army's cybersecurity posture.

Through the rationalization, modernization and virtualization of applications (and dependent on the standards being developed under the DC/C/GF CE initiative), the Army will identify unnecessary overlap in IT capabilities and reduce the number of applications it owns. In turn, this will increase efficiency, reduce life-cycle sustainment requirements and simplify IT capabilities, thereby supporting a more rapid and efficient evolution to the COE.

Combined with transport infrastructure enhancements, these various efforts will enable the staging of information for global access as users move between mission environments. They also will allow regionally aligned partners to: collaboratively plan, train and execute missions, capitalizing on their home-station information capabilities; transition seamlessly to their deployed mission environments; maintain continuous visibility of the changing mission status; and proactively engage and respond to the changing situation, utilizing their globally available information capabilities.

The Army currently is participating in a number of commercial cloud pilots that leverage infrastructure as a service (IaaS). Through these pilots, the Army has concluded that:

- Existing policies, procedures and infrastructure are not 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 DC/C/GF CE.

## UNCLASSIFIED

These lessons learned will impact the use of the cloud environment. For specific guidance, see the ADCCP, the Army Cloud Strategy, the Army Policy for Migration to Commercial Cloud Service Providers and the Army Cloud Computing Reference Architecture.

### End-User Device (EUD) Strategy

As the Army's interest in and demand for mobile EUDs grow, the Army must develop a standardized strategy for EUD implementation and use. Cybersecurity and enterprise service capabilities will be incorporated into the EUD Strategy. Additionally, the NCD will coordinate with the NSD and ESD to ensure that it complements and supports the overarching Mobility Strategy.

In FY14-15, projected and actual EUD accomplishments included:

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

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

In FY16, EUD activities include:

- Developing an EUD Strategy to define requirements for a common EUD environment.
- Beginning implementation of the decisions drawn from COTS-IT WG recommendations.
- Updating the EUD Reference Architecture as required.

In FY17, EUD Strategy activities include:

- Establishing the technical parameters to enable enterprise-level agreements with service providers for mobile data service.
- Identifying and beginning implementation of adjustments to the installation and deployable network infrastructure components necessary to support the mobile aspect of the EUD Strategy.

By the end of FY17, the Army will provide a DoD-synchronized EUD Strategy that outlines how to meet mission requirements while achieving efficiencies and reducing security vulnerabilities. The Army will standardize procurement of infrastructure and EUD solutions (e.g., hand-held devices and thin/zero clients).

The development of an EUD Strategy will ensure that the Army is on a modernization path that keeps pace with the rapidly changing technology environment. It will enable end users to acquire and utilize services through mobile devices in an efficient, consistent, secure and reliable manner.

Implementation of a standard suite of EUD systems will produce significant cost savings and the ability to collaborate across the force. The suite will provide Soldiers, civilians and contractors performing official Army business seamless access to the right information; the

## UNCLASSIFIED

ability to identify authoritative documents; automated business processes; workflow management and task tracking; management of personnel and organizations; and the ability to share information across functional communities and centers of excellence.

### Divestiture Planning

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

In FY14-15, projected and actual divestiture accomplishments included:

- Projected: Implement divestiture plans for unneeded legacy circuits, switches and servers resulting from fielding of MPLS, JRSS and ACS/EAS in CONUS, Southwest Asia and Europe. Develop and implement divestiture plans for unneeded Command local area networks (LANs), wide area networks (WANs) and transport infrastructure that support dedicated video teleconference (VTC) networks as new equipment migrates to the enterprise infrastructure. 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-D.

Actual: None. (Funding constraints delayed network modernization initiatives, which directly impacted divestiture of legacy equipment.)

In FY16, divestiture activities include:

- Implementing divestiture plans for obsolete legacy circuits, switches and servers replaced by MPLS, JRSS and ACS/EAS in CONUS, Southwest Asia and Europe.
- Developing and implementing divestiture plans for unneeded command LANs, WANs and transport infrastructure supporting dedicated VTC networks as they 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 the appropriate hosting facilities.
- Implementing divestiture of SINCGARS Models A-D (to be completed no later than FY18).

In FY17, divestiture activities include:

- Implementing divestiture plans for unneeded circuits, legacy switches and servers replaced by MPLS, JRSS and ACS/EAS in Pacific Command, European Command and Africa Command.
- Continuing implementation of divestiture plans for unneeded Command LANs, WANs and transport infrastructure that support dedicated VTC networks.

## UNCLASSIFIED

- Continuing implementation of divestiture plans for unneeded servers and storage pods as Commands virtualize and migrate applications and data to the appropriate hosting facilities.
- Implementing divestiture plans for the Enhanced Position Location Reporting System, which will be supplanted by fielding Joint Battle Command - Platform to Brigade Combat Teams (to be completed no later than FY18).

Three new factors will enable the start of legacy equipment divestiture at posts, camps and stations 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 FY16, and divestiture activities are fully initiated for Army organizations in Europe, the Pacific and Africa. By the end of FY17, the Army will initiate the divestiture process to remove unnecessary equipment from the network in CONUS and Southwest Asia.

The Army and Commands will be able to reallocate legacy network equipment life-cycle sustainment resources to higher-priority requirements; and facilitate and expedite the migration to the more efficient network, helping to meet operational and modernization objectives in a resource-constrained environment. Divestiture of unneeded legacy equipment will also improve network infrastructure effectiveness by simplifying the architecture.

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

### Summary

By the end of 2017, the network infrastructure will be adequately modernized to provide the throughput and computing necessary to extend enterprise services and Unified Capabilities to tactical-edge users. The robust approach to IaaS will empower garrison-based mission command operations, distribute training while leveraging a fully networked ITE, and augment unit readiness, particularly that of deployable network components. The infrastructure will support rapid evolution and deployment of applications to meet changing user needs. It will also support the staging of information to ensure availability at the point of need as users transition between mission environments.

The Army network backbone connecting installations to the DoDIN will be increased to 10 gbps, with the capacity to grow to 100 gbps when required in the future. Network capacity from the core installation network architecture to the tactical edge will be expanded, as well. Plans and procedures for enterprise operations and management will be established. The Army will continue to stand up IPNs and ISNs and move to approved enterprise hosting facilities to accommodate consolidation of applications and data storage, and to meet the DoD CIO's strategic mandates and the Army's vision. The transport and computing infrastructure will be modernized to support cloud capabilities, which will enable better-informed decision-making.

## Appendix 2 – Enterprise Services Domain (ESD)

Army enterprise services must be an easy-to-use, integrated suite of globally available, adaptable solutions that seamlessly supports the Army while working with unified action partners. These services, both user-facing and enabling, provide the Army awareness of and access to information, and take into consideration both institutional and operational components.

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

<b>Support the Army</b>	DOTMLPF-P (doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy) solutions should account for all Army components.
<b>Go Joint First</b>	The Army will use Joint solutions before pursuing Army-only solutions. The default approach for investment will be to share services across Joint forces whenever reasonably possible.
<b>Simplify, Standardize and Integrate</b>	Following DoD’s lead, the Army must shift from mission-specific sets of systems, processes, governance and controls to a more seamless, coordinated, unified and integrated data-centric enterprise environment that conforms to COE standards and specifications.
<b>Build for Change</b>	Solutions will be developed incrementally in order to ensure that services evolve with the dynamic, constantly changing environment.

**Table 20: Guiding Principles to Enterprise Services**

The ESD’s primary goal is to ensure an integrated collaborative environment that supports all mission areas. The ESD is comprised of three major capability areas:

1. Information Sharing
2. Core Enterprise Services
3. Position, Navigation and Timing

Enterprise Services will also play a supporting role in achieving any outcome led by the other AEN domains (NCD and NSD).

ESD will team with key stakeholders to achieve the following outcomes in FY16-17:

1. Enterprise applications and services are used by the Army, enabling global collaboration with unified action partners on any trusted device.
2. Enterprise applications and services provide a consistent user experience to any authorized user through simplified and standardized global service delivery, which accounts for a variety of transport characteristics.
3. Enterprise Services are integrated with Home-Station Mission Command and tactical forces. The primary capabilities include chat, instant messaging and email, based on priority.

**FY16-17 Priority Activities**

The ESD will focus on several high-priority activities that align to ESD capabilities/net-centric Joint Capability Areas. This alignment is described below.

FY16-17 ESD Activities	Joint Capability Area 6 Communications and Computers								
	6.2 Enterprise Services								
	6.2.1 Information Sharing	6.2.3 Core Enterprise Services							6.2.4 Position, Navigation and Timing
		6.2.3.1 Portal Services	6.2.3.2 Collaboration	6.2.3.3 Content Discovery	6.2.3.4 Content Delivery	6.2.3.6 Enterprise Messaging	6.2.3.7 Directory Services	6.2.3.8 Enterprise Application Software	
Application Portfolio Rationalization, Standardization and Disposition								•	
Army Data Management Program	•	•	•	•	•	•	•	•	•
Army Enterprise Directory Services							•		
Army Enterprise Service Desk						•			
Army Mobility Services			•			•			
Defense Enterprise Email						•			
Enterprise Content Management and Collaboration Services		•	•						
Enterprise License Agreements								•	
C4IM Services List and LandWarNet Services Catalog		•	•	•	•	•	•	•	•
milSuite			•						
Storage as a Service		•	•	•	•	•	•	•	•
Unified Capabilities - Software UC - Hardware Voice - Hardware Video			•						
Army Enterprise Service Management Framework		•	•	•	•	•	•	•	

**Table 21: ESD Activities Aligned to JCAs**

**Application Portfolio Rationalization, Standardization and Disposition**

Enterprise applications and systems are defined as those with users that cross installation boundaries. DoD has mandated that all enterprise applications and systems be migrated to DoD-approved enterprise hosting facilities by the end of FY18. Consolidation of data centers,

## UNCLASSIFIED

operations centers and help desks will enable users' and systems' timely and secure access to the data and services needed to accomplish their assigned missions, regardless of their location. The migration to consolidated data storage is discussed in the NCD appendix, and secure access is addressed in the NSD appendix.

Application rationalization, as part of portfolio management, allows the Army to simplify and streamline IT infrastructure while delivering mission-essential capabilities. Application disposition enables an effective balance of cost, benefit, risk and dependencies. Application migration follows a path toward standardization and supports the Common Operating Environment. As applications are standardized, the Army's requirement to develop capabilities in a more consistent, agile, effective and secure manner is achieved. In cooperation with the other AEN domains, efforts to standardize applications will help to modernize the network, support the ITE and mobility, and enable realization of the IaaS CONOPS. The Army will identify services to be redeployed as enterprise services, based on a systematic approach that looks at application capabilities rather than just the mission they support.

In FY15, application portfolio rationalization, standardization and disposition established a foundation for migrating applications and services to approved data centers. This foundation helped reduce unnecessary redundancy across the network and established responsibilities to support the application life cycle. At the end of FY15, guidance for migrating enterprise applications and methods for determination of application disposition were in place.

In FY16 and FY17, enterprise applications will migrate to approved data centers, eliminating unnecessary redundancy across the network. At the end of FY16, application consolidation will yield standard policies, procedures and guidelines for application owners to determine where their application should be hosted; and will provide the support necessary to handle the increased demand for data and application hosting.

### **Army Data Management Program (ADMP)**

The Army CIO is responsible for and prescribes the Army's information management (IM) policy and guidance, and oversees data management through the Army Data Management Program (ADMP). Army Data Strategy guidance and compliance requirements allow Army data stakeholders to envision, design, develop, deploy and use information systems that are consistent, comprehensive, compatible and integrated in their ability to share information across the Army, align to the DoD information-sharing vision and meet Army information-sharing objectives.

The Army Data Strategy, which was developed in FY14-15, focuses on three major areas.

- The ADMP: Identifies the functional areas of Army data management and serves as a tool for organizing and planning the development and application of the guidance that comprises the ADMP.
- The Army Information Architecture (AIA): Provides design and development guidance, in accordance with Army and DoD objectives, for improving data access, data exchange and information-sharing capabilities between information systems.

## UNCLASSIFIED

- **Authoritative Data Sources:** Recognized as an official data production source with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers.

One FY16 Army Data Strategy initiative is development of the COE Data Foundation (CDF). The CDF will provide guidance and resources to program managers and programs of record, including a data dictionary and a methodology that facilitate interoperability among Army systems across all COE CEs. The CDF will initially address the operational force, then be extended to generating force systems, to include enterprise data elements. The intent of the CDF is to reduce development costs and improve interoperability among Army systems by aligning data semantics across information exchange specifications (IES) without mandating the use of a specific IES.

In FY16, CIO/G-6 will continue to support Army organizations in identifying and registering Army Authoritative Data Sources and other data artifacts in accordance with Army Data Council/Army Data Board direction. Additionally, CIO/G-6 will establish Army implementation guidance for the National Information Exchange Model (NIEM).

In FY16-17, CIO/G-6 will also create, sustain and/or update the following Army Data Strategy artifacts based on Joint and DoD guidance, as well as feedback from the Army data stakeholder community.

- Army Information Architecture (AIA)
- AIA Compliance Tool and AIA Assessment Process
- ADMP Volumes I and II
- Army Data Strategy Playbooks
- Army Data Management Guides (formerly Army Data Framework)
- Rules for Cross-Cutting Capability (CCC) IES in Interface Specifications

The goals of the Army Data Strategy are to enable the Army data stakeholder community to develop systems that are visible, accessible, understandable, trusted and interoperable, and to increase registration of data sources, IES, service interfaces and industry standard and/or NIEM-compliant data models. Accurate data lead to improved analysis and will empower Army leadership to make better, faster decisions. Through these efforts, the Army will ensure a consistent user experience across enterprise services.

### **Army Enterprise Directory Services**

Army Enterprise Directory Services (EDS) provide, operate and maintain a centralized global directory of users and resources that can be accessed through a single interface. They include directory synchronization with other lower-level directories across the Army network.

In FY15, EDS continued to identify ways to improve the Global Address List (GAL), which is utilized via the global directory. EDS updated policy to ensure that individuals continuously maintained user attributes, as well as identified and prioritized attributes based on mission for both access and display to users.

## UNCLASSIFIED

In FY16, EDS will incorporate IT entitlements, which define in the directory the IT services and service levels available to individuals or groups of people. By the end of FY16, EDS will provide a single source for directory information across all enterprise services, and will continue to look for attributes for future incorporation. Organizations that provide directory services independently and need additional time to transition to the Enterprise Directory must submit a Plan of Action and Milestones and implementation guidance. However, all directories must be able to utilize enterprise identity attributes by the end of FY16, in accordance with U.S. Cyber Command TASKORD 14-0025.

In FY17, with EDS as the single source for directory information, users will have global access to directory and resource information via the Army network. The consistent user experience and interface offered by EDS will reduce time spent employing multiple systems to search for and maintain personnel data, reducing overall costs to the Army. EDS attributes will provide information for the GAL, through the identity and access management (IdAM) initiative led by the NSD (see Appendix 3).

Implementation of Army EDS will reduce the need for local directory service solutions at Army installations and thereby cut directory sustainment costs. Through synchronization with lower-level directories, EDS will also provide greater efficiency and effectiveness in Army personnel and resource location as directory information will be centralized rather than maintained in many disparate systems.

### **Army Enterprise Service Desk (AESD)**

AESD provides a single designated point of contact for IT support across the Army network. End users are able to report incidents and submit service requests via phone or email, and obtain self-service options at the AESD web portal. AESD operates 24 hours a day, seven days per week, 365 days per year, and is responsible for incident management, request fulfillment, knowledge management and activity reporting.

In FY15, the AESD-Worldwide NIPR-based service desk processed approximately 1 million unclassified service requests and incidents in support of enterprise services (Army Knowledge Online (AKO), Defense Enterprise Email (DEE) and Enterprise Collaboration and Content Management Services) and 7<sup>th</sup> Signal Command. The AESD project office successfully transitioned the Army's largest service desk to a new mission contractor without protest and with minimal impact to operations. It also fielded an on-premises, government-owned, contractor-operated SIPR service desk capability to support enterprise services (AKO-S, EE-S). The project office successfully demonstrated the use of end user-facing knowledge (Tier 0) to solve incidents. By creating knowledge articles that led users through the process of reducing DEE mailboxes to under 4 gigabytes, more than 50,000 potential calls became 50,000 knowledge article reads. The AESD project office also began Tier 1 support of the Standard Procurement System for the Office of the Deputy Assistant Secretary of the Army - Enterprise Business Systems Directorate. In parallel, it worked with 10 Army Command- and theater-level services to support their inclusion into an AESD Federation construct that was formally approved by the CIO/G-6. Additionally, the project office coordinated AESD Federation support of DoD Mobility Unclassified Capability services, and initiated projects in Korea and the Pacific and with Army Reserve Command to improve federation capability.

## UNCLASSIFIED

In CONUS, AESD-Worldwide currently provides Tier 1 support for command, control, communications, computers and information management (C4IM) services for end users at 44 Network Enterprise Centers (NECs). In FY16 and FY17, AESD-W will continue to on-board installations within 7<sup>th</sup> Signal Command's area of responsibility. AESD-Worldwide also will continue to provide global support for enterprise services, such as DEE, Enterprise Collaboration and Content Management Services, DISA Mobility Unclassified Capability and AKO. In FY16, AESD will reach initial operating capability for the UC soft client and continue to expand UC support in FY17 as UC deployment is completed.

In FY16 and FY17, the AESD Federation will improve service quality by standardizing internal service desk processes and tools, utilizing new incident ticket exchange capabilities and increasing user access to self-service features. These actions will also improve network availability to Army end users, synchronize institutional and operational components, and provide situational awareness through coordination among AESD, NECs/local operations, Regional Cyber Centers and the Army Cyber Operations Integration Center.

### Army Mobility Services

Individual mobility is increasing across the Army. Army mobility services have become a key initiative supported by all three AEN domains. The ESD's main focus for this initiative is to provide enterprise applications and services to the user via the Army Software Marketplace, as well as enterprise agreements for mobile data and cellular service that enable mobile devices while users are at home station, en route and deployed. In addition, Army mobility services will offer blanket purchase agreements (BPAs) with various commercial carriers so that each Command can select approved devices and the carrier plan that best meets mission needs.

In FY15, the Army initiated BPAs in CONUS and made them available via the Computer Hardware, Enterprise Software and Solutions (CHESS) website. Mobility services also opened a mobility application store (MAS), where users have access to a wide variety of applications for download and use.

In FY16, Army mobility services will provide multiple BPAs with commercial carriers. It will also provision and manage applications and services for trusted mobile devices through a MAS model and a managed mobile catalog. By the end of FY16, Army mobility services will be available via multiple BPAs through the CHESS website, where select Army users will be able to order a trusted mobile device and a carrier package that best meets mission needs. This will help the Army to conduct mission and business functions globally, and to effectively employ derived PKI credentials for authentication and access control, creating a common user experience.

In FY17, the Army will achieve significant efficiencies, to include cost savings in implementation and sustainment, by consolidating various individual Command mobile subscriber contracts into several enterprise BPAs for wireless devices and effectively employing derived PKI credentials for authentication and access control. These efforts will help integrate enterprise and deployed aspects of the network. Additionally, with one central location to assist with acquisition of services and equipment, Commands will have better, easier access to this capability.

## UNCLASSIFIED

### Defense Enterprise Email (DEE)

DEE provides secure email, hosted by DISA, for the Army and other DoD components. Recent efforts have focused on service implementation and shutting down disparate email servers. In FY15-16, a technical feasibility analysis will continue to determine whether it is possible to provide users a single identity regardless of location (CONUS or deployed), the perception of one mailbox and enterprise services at the tactical edge.

In FY15, DEE was in sustainment and focused on adding or enhancing features, such as additional GAL search fields, being able to use NIPRNet soft certificates on Blackberries, being able to use NIPRNet certificates to sign and encrypt for Non-Person Entity (NPE) mailboxes, and improving the functionality of the enterprise portal used to provision and change mailboxes. The Army Project Office Enterprise Email also worked with CIO/G-6 on the Army's guidance for journaling (i.e., the ability to retain independent copies of all correspondence sent and received, which is used to support Freedom of Information Act requests, congressional inquiries and statutory compliance investigations). The Army planned for the implementation of centralized, dynamic, tiered storage with global search, laying the foundation to meet an Office of Management and Budget directive to place electronic content under records management by FY17.

In FY16, DISA will implement several different size options for DEE mailboxes, allowing the Army to adjust its consumption to meet mission requirements. Additionally DISA will determine the feasibility of extending DEE to the tactical edge, allowing the possible retirement of standalone email services and providing the Army cost recovery opportunities. In FY16, DISA will work with CIO/G-6 on guidance to ensure that individuals continuously maintain user attributes in milConnect and organizations establish semi-annual reviews and update procedures. Additionally, DEE will implement the ability to use SIPRNet soft certificates to sign and encrypt from non-person entity mailboxes. DEE also will begin transition and integration activities with the storage environment to achieve records management compliance and create savings.

In FY17, DEE will continue transition and integration activities with the storage environment to gain records management compliance and create savings. Also in FY17, DEE will transition the cost of certain current mobile service from baseline (centrally funded) to mission funded (by Commands).

### Enterprise Content Management and Collaboration Services (ECMCS)

ECMCS provide a set of complementary services that include collaboration, content management, records management and business process management that can only be accessed via Common Access Card (CAC).

In FY15, ECMCS began the process of identifying a replacement for the AKO 1.0 FOUO portal. Before AKO is retired, organizations will have a transition period to transfer their users and content. ECMCS also continued the Defense Enterprise Portal Service (DEPS) pilot program, which will eventually include up to 100,000 participants.

## UNCLASSIFIED

In FY16, ECMCS will be available to onboard users to an enterprise-level service and will start divestiture planning for legacy systems. The Army will increase the use of DEPS with the primary intent of further refining requirements for an integrated solution, to be fielded in FY18-19. The CIO/G-6 will continue to analyze alternative solutions for NIPR collaboration and will implement Army SIPR collaboration through the Network Enterprise Technology Command (NETCOM) office at Rock Island Arsenal, using SharePoint 2013.

### **Enterprise License Agreements (ELAs)**

ELAs allow the Army to make bulk purchases, thereby providing a better negotiating position and decreasing the cost of productivity-enhancing software solutions. By having a centralized purchasing process and capitalizing on economies of scale, the Army will be able to negotiate additional value-added services, such as training, and reduce the total cost of software ownership. The Army will continue to work closely with DoD partners to ensure alignment with JIE strategies and the Better Buying Power initiative. To access ELA listings and details, visit <https://chess.army.mil/>.

At the end of FY15, the Army had 15 ELAs in place to eliminate redundant or unnecessary purchases. In FY16, the Army will maintain these 15 ELAs and will continue to identify opportunities for additional ELAs for the most commonly used products across the Army and Joint enterprise. As ELAs are brought online, standalone investments (services and software) will be targeted for sunset. This will generate significant cost savings and provide a consistent software user experience. The Army will fully support and implement DoD-wide plans for the intended transition to Windows 10 by the end of FY16.

In FY17, the Army will require a new Microsoft Joint ELA and will continue to identify opportunities for additional ELAs (e.g., RedHat, Oracle). Currently, seven ELAs are supported by central funding and budgeted through 2020.

### **C4IM Services List and LandWarNet Services Catalog**

The Army C4IM Services List defines Army baseline and mission-funded IT services provided and/or supported by the Network Enterprise Centers on Army installations. (Baseline services are centrally funded, while individual Commands provide the monies for mission-funded services.) These C4IM Services are aligned to Base Operations Support services 700 (Automation), 701 (Communications Systems), 702 (Multimedia/Visual Information) and 703 (Information Assurance), as defined by the Assistant Chief of Staff for Installation Management. The C4IM Services List is the foundation for the LandWarNet Services Catalog, the customer-facing document that identifies standards for delivery of services based on funding constraints.

In FY15, CIO/G-6 staffed and published C4IM Services List Version 6.0, which included both customer-facing and enabling IT services for use in FY16.

The C4IM Services List and LandWarNet Services Catalog are managed and updated through a forum known as the IT Service Management/IT Metrics Working Group and are the basis for network services. The working group, which is an integral part of the Army Enterprise Services Management Framework, discusses, develops and submits recommendations to the CIO/G-6 through the Army Enterprise Network Council (AENC) regarding Army IT services

## UNCLASSIFIED

management planning, policy, programming, systems, standards, architecture, procedures, performance and other issues as they relate to the provisioning, delivery, measuring and reporting of the network and C4IM services used to support the Army. It leverages the Army Enterprise Service Management Framework (AESMF) to develop future C4IM service lists in order to improve efficiency and standardize IT service management. In FY16, the working group will focus on including all network segments – NIPR, SIPR, Defense Research and Engineering Network, Joint Worldwide Intelligence Communications System – and all service providers in a dynamic C4IM Services List and Catalog while continuing to incorporate and refine enterprise services (AESD, UC, DEE).

In FY16 and FY17, the Army IT Metrics Program will support the use of metrics to assess the current status of IT infrastructure and the performance of C4IM services on Army installations. IT metrics provide the key components of the cost-per-seat (CpS) model, which generates the funding requirements for NETCOM to provision baseline C4IM services. In FY16, the Army National Guard and Army Reserve will also develop a CpS model, in alignment with their business models, to generate their C4IM service requirements. The CpS model provides decision makers the information necessary to improve C4IM services and operational effectiveness, efficiency, network defense and resource balancing across the enterprise by evaluating viable alternatives to increase consistency, quality, user satisfaction, information security, capabilities and responsiveness.

### milSuite

The Army information environment is overwhelmed by a complexity and uncertainty that "business as usual" simply cannot address. While the ability to describe, capture, store and retrieve information that we already know will always be critical, the most valuable work in the Army will be the creation, sharing and discovery of new knowledge. milSuite, which is a collection of Web 2.0 tools, will establish a culture of information sharing across Services, ranks and positions, and connect and encourage those who have expertise to create new knowledge. It currently links more than 420,000 users across the military, civilian and contractor workforce from the Army and DoD enterprise, and provides all DoD individuals, units and organizations a way to quickly and easily build tools and business processes to efficiently support mission execution. It consists of four applications: milBook, milWiki, milWire and milTube. Collectively, milSuite provides users professional networking and collaboration through the use of wikis, discussion forums, document sharing, blogs and video sharing. It offers a secure, centralized location for Army personnel to discuss military topics. The ad hoc collaboration feature allows users to share knowledge and exchange information among a larger global community, speeding solution development in a secure environment.

In FY15, the DISA Defense Collaboration Service Portfolio Council designated milSuite as a DoD enterprise service. In FY16, the Army will decide whether to use milSuite to satisfy the portal and front page replacement capability for AKO. Currently, the Army is transitioning all applications from AKO single sign-on (SSO) to direct PKI for authentication, where applicable (in accordance with the January 2015 CIO/G-6 memorandum regarding transition of current web applications to direct Public Key Infrastructure).

## UNCLASSIFIED

In FY17, if milSuite is not funded by either DoD or the Army, and it is not selected as the future state for asynchronous collaboration as a result of the Unified Capabilities and AKO analyses of alternatives, it will be recommended for sunset.

### Storage as a Service (STaaS)

The Army is experiencing unprecedented growth in data storage requirements and requires a cost-effective, capacity-on-demand solution that collapses storage from installations across the Army into a consolidated environment, delivered as a service, for unclassified and classified data. Army end users require secure-access organizational and personal storage, to include files, data sets and information from whatever device they are using. STaaS addresses the gathering, storage and dissemination of information within a community to accomplish a specific mission or objective. STaaS integrates all other enterprise services (email, collaboration and portal) to reduce overall costs and improve the user's ability to access information.

STaaS is explicitly provided by enterprise software and is not mission or domain specific. As such, it will be available to all Army end users. Access will be constrained based on infrastructure availability, cost, security and service level agreements. STaaS supports only those Army end users who access the service through the Common Operating Environment. Access to STaaS and data will be controlled via attribute-based and role-based methodologies through the DoD Enterprise Directory Service.

In FY15, Army STaaS created integrated project teams (IPTs) to gather requirements and obtain validation from Army Commands, Army Service Component Commands and direct reporting units. The Army STaaS IPTs also drafted email records management and retention policies and business rules to maintain governance of and a compliance check on storage capacities.

In FY16, the Army STaaS IPTs will start looking at storage solutions to satisfy Army-wide needs. The CIO/G-6 is encountering greater demand for data storage through the Information Technology Approval System (ITAS) process, which places a significant burden on the Army's IT budget. The Army will consolidate its current disparate low- and moderate-performance storage solutions to a more cost-effective, standardized, capacity-on-demand, commodity storage service to the greatest extent functionally and technically possible. This standardized storage service will be scalable, secure and available on both the NIPRNet and SIPRNet. The storage solution will consolidate data and replace locally hosted mapped network drives, file shares and other repositories for unstructured file data.

### Unified Capabilities (UC)

UC directly support collaboration by providing synchronous Army access to media, such as voice, video and data. In FY15-17, the Army will consolidate and standardize the way it communicates by focusing on three LOEs for this initiative: deploying a limited UC soft-client institutional solution; transitioning to Voice over Internet Protocol (VoIP); and transitioning to IP VTC.

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

## UNCLASSIFIED

Army will not decommission legacy systems until the deployment of soft-client hardware upgrades for voice (e.g., VoIP phones) and video (e.g., Global Video Services) is completed. Legacy systems waiting for decommissioning are: Private Branch Exchanges (PBXs), Public Switched Telephone Network (PSTN), Multiple Control Units (MCUs), Integrated Service Digital Network (ISDN), AKO instant messaging and Defense Collaboration Service (DCS).

In FY15, CIO/G-6 published extensive guidance and policy to support the VTC transition to IP and provided training sessions, shared TTPs and lessons learned to cultivate cultural change. The Army worked closely with the Air Force and DISA to produce requirements for a UC soft-client institutional capability. The individual Service requirements integrate with Enterprise Voice over Internet Protocol (EVoIP) on NIPRNet and Enterprise Classified Voice over Internet Protocol (ECVoIP) on SIPRNet to allow calls between UC soft client and voice-only end points, including other legacy end points. UC soft clients will also reach commercial numbers through the EVoIP system. In addition, the Army and DISA partnered with the National Security Agency to produce a security architecture that supports the consumption of UC soft client from a commercial cloud. Following a request for information and analysis of industry responses, the Army began re-scoping the UC soft client strategy, with a focus on limited institutional deployment. The Army also published a UC Reference Architecture.

In FY16, the Army will divest AKO instant messaging and begin limited deployment of an IP-based UC Soft Client to standardize and simplify the way the Army communicates. While the UC Soft Client institutional strategy is being developed, the Army will continue transitioning to IP VTC and reducing its reliance on traditional telecommunications and disparate implementations of UC by decommissioning expensive legacy technology infrastructure. This will help support the Army's overall efficiency goals. The Army will also continue to divest expensive, outdated infrastructure, such as desktop analog phones and Time Division Multiplexing (TDM) switches, and move to VoIP services. By the end of FY16, the UC institutional strategy will be complete and the UC Soft Client institutional funding baseline approved. If needed, the Army will update the UC Reference Architecture.

In FY16, the CIO/G-6 will lead a pilot of the Microsoft Office 365 Premium product to inform, assess and learn how this solution can support the Army's UC effort and improve the Army's daily business processes.

The transition to VoIP and EVoIP is expected to last through FY17 and will coincide with the modernization of installation infrastructure. As a gap filler, the Army will take advantage of DISA services, such as the Defense Collaboration Service and Global Video Services. The Army will provide basic UC capability, including voice, video, instant messaging/chat, presence and awareness, screen sharing, GAL integration and unified messaging (enterprise email integration), on NIPRNet and SIPRNet for a limited number of Army business users and CONUS regions. By the end of FY17, limited deployment of UC soft client will be established, plans will be in place to scale across the remainder of CONUS, SWA and USARPAC, and end-to-end integration of UC will be in progress. Full worldwide UC operating capability is expected by the end of FY18.

## UNCLASSIFIED

### Army Enterprise Service Management Framework (AESMF)

In FY15, the Army published three AESM capstone documents: the Army IT Service Management (ITSM) Policy, CONOPS and Reference Architecture (RA). The ITSM Policy introduces an AESMF that continually increase effectiveness, improves security and gains efficiencies in Army IT services by standardizing the service delivery process. The AESM CONOPS provides a detailed description of the associated AESMF processes, functions and governance structure. The RA defines the critical success factors and key performance indicators for all processes in the AESMF.

The intent of the AESMF is to provide value to Army users by delivering quality IT services effectively, securely and efficiently. The Army has adopted and adapted the DoD Enterprise Service Management Framework (DESMF) to achieve this objective. The AESMF will apply to all IT services listed in the C4IM Services List.

In the first quarter of FY16, ARCYBER and Second Army published OPOD 2015-367, Implementation of Army Enterprise Service Management Framework (AESMF). This OPOD defines the tasks and controls implementation priorities. FY16 priorities are to update and publish service and process management plans in accordance with the OPOD.

In FY17, Fragmentary Orders (FRAGOs) will be used to establish priorities for continual improvement of services and processes. Additionally, the Army will update capstone documents.

### Assured Position, Navigation and Timing (PNT)

Assured Army position, navigation and timing systems (i.e., precision munitions, Blue Force Tracker, etc.) presently are critically dependent on PNT information.

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 civil users. A major element of this modernization is the development of GPS Military Code (M-Code), which is 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. The Army requires a coordinated, synchronized and affordable approach to modernizing with an assured PNT and M-Code capability.

The near term PNT focus for the Army is to develop an Army PNT Roadmap and a prioritized list for integration of modernized GPS user equipment across the Army. The Army also intends to finalize an M-code transition strategy by the end of the fourth quarter of FY17. Vulnerabilities and challenges will be assessed in current and future material solutions, and shortfalls will be addressed in Soldier training and preparedness.

### Summary

The ESD provides the user interface layer of the Army network. Enterprise services include IT and information management services that are “visible” to the entire Army to enable and

**UNCLASSIFIED**

automate business processes, functions, solutions and applications. FY16 activities will lay the groundwork for the fielding by FY18 of a cloud-based collaboration solution, development of a “one entry for all” user portal and improved content discovery tools that utilize identified data sources. Together, these capabilities will support Army collaboration with unified action partners on any trusted device globally through a consistent user experience.

## Appendix 3 – Network Operations and Security Domain (NSD)

The NSD is responsible for ensuring that IT network operations and security investments support the Army's vision, mission and goals. The NSD will select the best mix of IT investments in the domain to ensure efficient and effective delivery of capabilities to the warfighter. It also will establish quantifiable outcome-based performance measures and evaluate against those measures to maximize return on investment for the enterprise.

The overarching guidance for the NSD in the FY16-17 timeframe is to meet the core mandated cybersecurity requirements from DoD, the Chairman of the Joint Chiefs of Staff and the Army. The primary goal of the NSD is to provide a secure, seamless and continuous network environment with protected critical data and information in support of the Army's Future Modular Force concept, Mission Partner Environment and unified action partners. The supporting goals are:

- Defending the information network, securing data and mitigating mission risk.
- Building and maintaining ready forces and capabilities to conduct cyberspace operations.
- Enabling information sharing for authorized users so that the Army can support partners and build capacity.

### Defending the Information Network, Securing Data and Mitigating Risk to Missions

The Army will plan and build a resilient, reliable and secure information enterprise and information network to deliver capabilities that provide the technological advantage to prevail against any adversary. The Army will integrate cybersecurity risk management into all mission and operational phases to protect its critical information and data in support of achieving successful mission outcomes.

### Building and Maintaining Ready Forces and Capabilities to Conduct Cyberspace Operations

The Army will provide forces and personnel that operate effectively in cyberspace by training them to the highest standard, and equipping them with best-in-class technical capabilities.

### Enabling Information Sharing for Authorized Users So That the Army Can Support Partners and Build Capacity

The Army will provide a secure, seamless and continuous network environment with protected critical data and information, which will support the Army's Operating Concept to provide the Joint Force multiple options to integrate the efforts of unified action partners, operate across multiple domains and present adversaries multiple dilemmas.

Cybersecurity efforts will be closely nested with the Cyber Mission Force, enabling the Army to more effectively counter traditional threats, as well as to address increasingly sophisticated threats, such as the insider threat and the advanced persistent threat. The Army Insider Threat Mitigation Program will provide an integrated capability to monitor and audit user activity across

**UNCLASSIFIED**

all domains (i.e., SIPRNet and JWICS) and to facilitate the sharing of counterintelligence, cybersecurity/information assurance, law enforcement, human resources, security and other related information with unified action partners.

The NSD will continue to maintain the following outcomes during the FY16-17 timeframe:

- Ensure that data, information and IT services are visible, accessible, understandable, trusted and interoperable, as well as protected, secure and resilient against warfare, terrorism, criminal activities, natural disasters and accidents.
- Expand the Army’s capability to build partners and capacity by enabling the sharing of data, information and IT services with authorized users.

There are 14 initiatives in FY16-17 that will enhance the network security posture and improve information sharing.

**FY16-17 Priority Activities**

<b>FY16-17 NSD Activities</b>	<b>Joint Capability Area 6 Communications and Computers</b>					
	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	
Implement Joint Regional Security Stacks					•	
Implement the Joint Management System	•					
Army Network IT Asset Visibility	•					
Enhance Identity and Access Management					•	
Cryptographic Modernization Initiative (CMI)				•		
Transition to Key Management Infrastructure				•		
Organize and Advance Mobility				•		
Align Information Security Continuous Monitoring with the DoD Framework					•	
Army Insider Threat Program				•	•	
Provide Army Enterprise Service Management	•					

**UNCLASSIFIED**

Standardize Network Operations	•					
Increase Agility of Spectrum Management Operations			•			
Enhance Cyber Situational Awareness by Leveraging Big Data/Cyber Analytics	•	•	•	•	•	•
Refine the Cyberspace Workforce					•	

**Table 22: NSD Activities Aligned to JCAs**

**Implement Joint Regional Security Stacks (JRSS)**

Numerous unclassified and classified external access points, secured by Top-Level Architecture (TLA) stacks, retain varying degrees of information and network management capabilities. Each TLA stack requires a wide range of network defense tools and personnel for management. The Army, DISA and the Air Force are collaboratively working to lead the effort to re-engineer and simplify the network architecture, reduce the network attack surface and standardize network security by implementing Joint Regional Security Stacks. Successful JRSS/Joint Management System implementation is strongly dependent upon having the MPLS transport, network modernization and Installation Campus Area Network (ICAN) in place.

To facilitate who has operational control, roles and responsibility, and operational maintenance responsibility, DISA will publish a JRSS Concept of Operations (CONOPS). The Army, in concert with DISA, will develop common security policies for the environment under a centrally managed, decentralized execution concept, yet will retain the right to implement security policies for Army-specific network missions.

In conjunction with the Army and other Services, DISA will also produce a JRSS Service Operational Annex (JRSS SOX) that defines the roles and responsibilities within JRSS, as well as processes for developing tactics, techniques and procedures (TTP) to enable JRSS operations.

The envisioned end state is defined by the Joint Migration Team (JMT) CONOPS, which sets the concept of operations for the transition of current service security architectures into JRSS. This migration strategy incorporates the necessary roles and responsibilities for DISA and the Services in order to successfully perform migrations.

Success is defined when each community of interest (COI) and bases, posts, camps and stations are migrated behind JRSS and move to steady state operations. Once JRSS capabilities have matured, provisional authorities such as the JMT will stand down and switch operations to DISA and the Combatant Commands, Services and agencies.

The NCD has the lead on installation of JRSS and MPLS. For FY15 installation accomplishments and FY16 planned activities, refer to Appendix 1 (Network Infrastructure Modernization). At a point to be determined, installation activities will reach a level of maturity

## UNCLASSIFIED

that will allow the NSD to assume control of this effort and transition to network operations and security functions.

The consolidation of the current TLA stacks to JRSS will improve network security by decreasing the cyberspace attack surface, standardizing firewall rule sets and clearly defining and centrally managing enclaves. JRSS are part of the single security architecture (SSA) for CONUS and OCONUS installations, and 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 to prevent data loss. They provide a standard perimeter that empowers the cyberspace community to execute a high level of defense through improved 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 and Intelligence Community Information Technology Enterprise alignment.

The transition of TLA stacks to JRSS also significantly reduces equipment and support personnel at installations, resulting in a network that is more defensible and efficient. By eliminating local base security systems, with a focus on cyberspace labor at the regional level, JRSS will reduce the cost of security functions.

In FY17, JRSS will continue to enable the management capability for the JIE Single Security Architecture on CONUS installations and OCONUS posts, camps and stations. As part of this process, the Army will remove its TLA stacks and the Air Force will take down its gateways. Marine Corps and Navy boundary traffic will only be peered with JRSS. During this timeframe, JRSS will deploy multiple new tools and capabilities, such as cyberspace situational awareness analytic cloud capabilities, and integrate them with Service and DISA DoDIN operations and TTPs for defensive cyberspace operations internal defensive measures (DCO-IDM).

### **Implement the Joint Management System (JMS)**

The Joint Management System encompasses the entire spectrum of network operations activities within the context of the DoD Enterprise Service Management Framework. JMS, through a hub-and-spoke configuration, will be used to manage, operate and defend the network as the management system for JRSS. It consists of systems, tools and information management capabilities required for DoD information network operations and 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.

In FY15, JRSS and JMS 1.0 were successfully fielded at two CONUS locations. To facilitate future activities, the Army participated in the DISA-led JRSS Initial Operational Assessment Phase 2. This assessment was designed to evaluate the people, process and technology of JRSS, JMS and MPLS in an operational environment with real users and in the approved configuration. Results will support Army decisions regarding additional migrations and retirement of the Top-Level Architecture.

## UNCLASSIFIED

In FY16, Army TLA and Air Force gateways will be removed, and Marine Corps and Navy boundaries peered, with traffic passing through JRSS. JMS 1.5 represents the minimum acceptable capability and capacity required to meet these objectives and the planning assumptions. As the demand for capacity grows, programming of additional funds may be required to reach the JRSS baseline in order to address the capacity risks inherent in this plan. The reduced-cost JMS/JRSS 1.5 capability suite consists of the JRSS capabilities currently being deployed plus full packet capture and web content filtering. In order to meet Army FY16-17 JRSS/JMS fielding and implementation objectives, in conjunction with the JMT's goals, the Army will increase the current number of Service Migration Teams, which are responsible for migrating COIs from the current TLA infrastructure to the JRSS/JMS infrastructure.

In FY16, JMS 1.0 NIPR and SIPR will be installed and activated at 10 CONUS, two SWA and two European locations, with DISA providing operation and maintenance at all sites.

In FY16, JMS 1.5 NIPR and JMS 1.0 SIPR will be installed and activated at eight CONUS and two SWA locations, with DISA providing operation and maintenance at all sites. Eight Pacific locations will only be installed and activated with JMS 1.0 SIPR in FY16, with DISA providing operation and maintenance.

In FY17, JMS 1.5 NIPR will be installed and activated at four CONUS, one European and eight Pacific locations, with DISA providing operation and maintenance at all sites.

In FY17, JMS 2.0 NIPR will continue to provide the management capability for the JIE Single Security Architecture. JMS will deploy multiple new tools and capabilities, such as cyberspace situational awareness and analytic cloud capabilities, and integrate them with Service and DISA DoDIN operations and DCO-IDM TTPs. JMS will provide a remote access capability to JRSS, enabling DoDIN operations and allowing DCO-IDM analysts to execute their missions without being co-located with JMS. All users will be able to monitor JMS information but will only have the capability to change configurations in concert with the requirements of their positions and organizations.

### **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. These network IT assets should be managed from the day they are requested and procured, to when they are deployed, throughout their entire life cycle, until retirement and removal from the network.

In FY16, CIO/G-6, in coordination with Second Army, Army Cyber Command and Network Enterprise Technology Command, will define an asset visibility strategy that will contribute to improved IT efficiencies, network security and defense, cost containment and mitigation of compliance risk. Additionally, CIO/G-6 will seek to partner with the Joint Staff and Air Force to assess any existing real-time visibility and response technology capabilities they are using that

## UNCLASSIFIED

comply with the Joint Information Environment Single Security Architecture and would enable the Army to meet emerging compliance requirements that require network asset visibility.

In FY17, an implementation plan will be developed to carry out the asset visibility strategy throughout all echelons of the Army network.

### **Enhance 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, the JIE and federal identity, credential and access management requirements and regulations.

The Army's enterprise IdAM framework centrally manages users' digital identity based on a single authoritative data source, resulting in improved access across organizational security boundaries to required network resources and information services. It will ensure that the right individuals obtain the right information at the right time for the right reasons.

Through privileged identity credential services, role-based access control solutions and auditing of privileged users' sessions, the framework will provide seamless identification, authentication, authorization and accountability of personnel (military, civilian, contractor) accessing logical and physical resources. It will allow the Army to decouple applications from existing directories and leverage authoritative attributes from the Defense Manpower Data Center to manage user access to IT resources across different security and organizational boundaries. The Army will then be able to decrease the number of standalone access control mechanisms for applications, systems and networks, which are often insecure, inefficient and redundant. Enterprise IdAM also will improve operational efficiency by decreasing the time Soldiers are disconnected from the network while transitioning between installations, deployments and training.

At the end of FY15, the Army finished preparing 19 NIPRNet and five SIPRNet forests to utilize DoD Enterprise Directory Services for the provisioning and synchronization of user accounts, in accordance with a DoD CIO mandate.<sup>3</sup> These activities consisted of revising policies and standard operating procedures for directories, and implementing a Public Key Enabling requirement to enhance cybersecurity.

In FY16, the Army will complete the transition of the 19 NIPRNet and five SIPRNet directories in order to fully leverage a single digital identity across the institutional force. This effort enables electronic policy enforcement for life-cycle management of digital identities, raises visibility of users and systems that access enterprise resources, and fulfills the DoD mandate to utilize DISA's Enterprise Directory Services. The Army will refine the IdAM strategy to align the

---

<sup>3</sup> Memorandum, Department of Defense Chief Information Officer; 23 January 2013, subject: Mandating the Use of Department of Defense Enterprise Directory Services.

## UNCLASSIFIED

strategic and tactical communities where feasible, and update the IdAM Reference Architecture as required.

Enterprise IdAM also will allow the Army to begin in FY16 to transition applications from AKO Single Sign-On to a common enterprise authentication and authorization service, such as direct Public Key Infrastructure (PKI) or DoD identity web services. Once completed, the Army will be able to decommission AKO. Additionally, the Army will continue activities supporting the switch to Secure Hash Algorithm 256.

In FY17, the Army will continue to enhance its enterprise, service-based access management capability by building upon the integrated IdAM framework. This framework will provide seamless network access for identification, authentication, authorization and accountability of personnel (military, civilian, contractor) accessing logical and physical resources. This capability will also allow the Army to reduce the standalone access control mechanisms for applications, systems and networks that are often insecure, inefficient and redundant.

The enterprise IdAM framework will support the following actions for all Army logical and physical resources.

- Continue to transition remaining applications from use of Army Single Sign On to a common enterprise authentication service.
- Implement privileged identity credential services, and assess options for role-based access control solutions and auditing of privileged user sessions.
- Continue efforts to integrate, resource and/or align strategic and tactical IdAM environments; develop an integrated way forward that encompasses directory services, PKI and cloud services.
- Begin to decouple applications from existing directories to enable users to access IT resources across different security and organizational boundaries by leveraging authoritative attributes from the Defense Manpower Data Center.
- Oversee efforts to make currently incompatible applications and systems compatible with Secure Hash Algorithm 256.

### *Execute Army Proponent Activities for CAC/PKI*

The DoD CIO has mandated the use of PKI on the NIPRNet and SIPRNet. Currently, NIPRNet users use a CAC and/or an Alternate Smartcard Login (ASCL) hardware token; SIPRNet users utilize a SIPRNet hardware token. These cards and tokens provide identity proofing, registration, credential management and multifactor authentication, resulting in data integrity, non-repudiation and confidentiality of information for individual users, organizations and groups. They also enhance cybersecurity of the DoDIN by denying access to adversaries who do not possess a valid token. PKI allows authenticated users to initiate secure sessions on DoD information systems within the strategic, tactical and personal home or public facility environments. It also enables users to initiate secure sessions using different computing platforms, such as personal/public computers, DoD workstations and mobile devices.

## UNCLASSIFIED

The Army's CAC program, through the use of Defense Enrollment Eligibility Reporting System (DEERS) and the Real-Time Automated Personnel Identification System (RAPIDS), is used to generate CACs globally for more than one million users. The Army's PKI program uses the DoD-provided Token Management System and Integrated Logistics Systems to provide round-the-clock operational support to ensure the timely issuance of NIPRNet ASCL tokens and SIPRNet tokens for more than a quarter-million non-person and person users. Additionally, support is provided to non-person entity (NPE) systems and applications to ensure their authentication to the network.

In FY15, the Army CAC/PKI program provided robust 24-hours-per-day, seven-days-per-week support for approximately one million CAC and NIPRNet ASCL token users and more than 130,000 SIPRNet token users to uniquely identify each user across the network and ensure data integrity, non-repudiation and confidentiality of information. The Army Registration Authority successfully completed a DISA audit with no deficiencies and no significant comments, demonstrating that the program was mature and had met all DoD and Committee on National Security Systems requirements. Additionally, CIO/G-6 established an audit program to verify the compliance and security of the Army CAC/PKI program and ensure its ongoing integrity. Operation of the Army Registration Authority and daily operation of the Army CAC/PKI program were transferred to Second Army.

Large numbers of SIPRNet token failures were reported throughout the year. CIO/G-6 performed joint on-site investigations into the high failure rates in concert with the DoD PKI Program Management Office (PMO). Most of the failures were due to system configuration and procedural issues, which were addressed by on-site training and reconfiguration. CIO/G-6 also tested, initiated infrastructure updates for and started delivery of a new version of the SIPRNet token card stock to address reliability issues.

CIO/G-6 has continued to support the efforts of the DoD PKI PMO to update the Token Management System (TMS) to improve its reliability and implement new capability that supports Army requirements. In FY15, this included completion of developmental and operational testing of TMS version 3.0. This TMS update provided the capability to issue system administrator tokens with only identity certificates, which is key to improving SIPRNet security.

In FY16-17, the Army CAC/PKI program will continue to ensure data integrity, non-repudiation and confidentiality of information and to uniquely identify each person and NPE. The Army will also continue to support the CAC program and NIPRNet ASCL and SIPRNet tokens. In coordination with the DoD PKI PMO and the other Services, the Army will develop a medium-assurance solution on the SIPRNet for NPEs, such as computers, applications and devices. This capability will allow NPEs to be issued credentials dynamically, which will enable secure connections to the tactical network and between tactical entities in the unit, creating a secure network operations environment.

### Secure Hash Algorithm (SHA) 256 Migration

In FY16-19, the Army will migrate PK-enabled systems and applications from use of SHA-1, which has reached the end of its security life cycle, to SHA-256 in accordance with federal government Public Key Infrastructure mandates. This migration will affect all trusted virtual network transactions done via CACs, such as digital signatures, network logon, web

## UNCLASSIFIED

authentication, email signatures and email encryption. Transition to SHA-256 will enhance mission assurance and ensure secure information sharing with unified action partners. Starting 1 January 2016, only SHA-256 Secure Socket Layer (SSL) device certificates used to establish secure Internet sessions can be issued. By 1 January 2017, all SHA-1 SSL device certificates issued prior to 1 January 2016 must be replaced by SHA-256 SSL device certificates. Beginning in April 2016, all SHA-1 CACs that expire will be replaced by SHA-256 CACs. By April 2019, all SHA-1 CACs will be retired from DoD.

### **Cryptographic Modernization Initiative (CMI)**

The Cryptographic Modernization Initiative (CMI) is a DoD CIO-led effort, worked in close collaboration with the Services, the National Security Agency (NSA) and the Joint Staff, to assess and modernize cryptographic capabilities (embedded and standalone) that protect National Security Systems (NSS) and National Security Information (NSI). Cryptographic modernization must occur continuously to respond to and counter technological obsolescence, adversaries' technological advances in crypto-analytic capabilities and the financial 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 authenticity of command, control, communications, computers, intelligence, surveillance and reconnaissance capabilities. As a result, this effort is spread over multiple Future Years Defense Programs to prioritize the most critical efforts and to determine when to accept risk in operating cryptographic solutions beyond the NSA-approved useful life.

At the end of FY15, the CMI had:

- Evaluated four emerging commercially developed cryptographic capabilities, and validated security, interoperability and suitability for the Army network.
- Conducted 46 global crypto modernization device training and integration visits.
- Procured more than 600 multifunction crypto solutions to improve security and bandwidth capacity.
- Began initial technical design for modernization of legacy UHF radios.

In FY16-17, the CMI will balance funding constraints against available technology and risk management by focusing on:

- Developing a technology roadmap that establishes the demilitarization and divestiture of cryptographic equipment (due to technology convergence, replacement of legacy equipment and network modernization).
- Implementing advanced encryption standards and replacing legacy technology, waveforms and obsolete algorithms in preparation for implementing Advanced Cryptographic Capabilities (ACC) in accordance with NSA mandates.
- Modernizing nuclear command, control and communications cryptographic capabilities by replacing legacy cryptographic components in accordance with DoD CIO-directed targets.

## UNCLASSIFIED

- Leveraging NSA's commercial solutions for classified mobile devices that support on-the-move command and control to dramatically increase real-time information flow of secure voice, video and data from knowledge centers at various security levels (unclassified to TS/SCI).
- Re-baselining and setting the conditions for the Army's embedded requirements.
- Developing and defining strategic priorities.

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 technological capabilities that provide security, scalability, interoperability and reliability for the exchange of authentic 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 and coalition interoperability. The Army will account for all legacy crypto devices and track the transition to modernized capabilities.

### Transition to Key Management Infrastructure

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 a critical enabler for providing confidentiality and integrity of secure communications (voice, video, data, etc.). The Army is currently migrating from the legacy Electronic Key Management System (EKMS) Tier 2 to a modernized Key Management Infrastructure (KMI). KMI will provide a unified, interoperable and trusted infrastructure for establishing, using, operating and managing cryptographic products and services in a net-centric environment.

At the end of FY15, KMI-related accomplishments include:

- Transitioned eight additional EKMS COMSEC account to KMI accounts as part of the KMI Spiral 2 Spin 1 performance test.
- Stood up the first of three Army KMI training classes to support new KMI Management Client (MGC) hardware fielding across Army.
- Conducted life-cycle support for Tier 3 key load devices to improve ruggedness.
- Tested and approved information assurance vulnerability assessments for key management systems.

In FY16, the Army will transition approximately one-third of EKMS Tier 2 accounts to KMI MGCs in accordance with delivered capabilities and the FY15 sustainment, restoration and modernization cycle. This net-centric capability will provide warfighters an enterprise-wide service, allowing them to generate, distribute and account for the status of cryptographic

## UNCLASSIFIED

products. Additionally, it will enable approved Mission Planning Management Support Systems (MPMSS) to integrate key distribution with other information management functions required by the system the MPMSS supports.

By the end of FY17, it is projected that the Army will have transitioned approximately 300 of 405 EKMS Tier 2 accounts to KMI MGCs. This capability will eliminate physical delivery of cryptographic material, which will take warfighters out of harm's way. With the implementation of KMI, the Army will have an enterprise solution that delivers cryptographic keys and products over the network, which will enhance the ability to electronically field, receive and track cryptographic products.

### Organize and Advance Mobility

As part of the overall Army mobility capability, NSD will focus on enabling mobile users to perform work functions over a secure network at any time, from anywhere. A robust network infrastructure, reliable enterprise services and dependable mobile end-user devices are all necessary components to make Army mobility successful. Mobile end-user devices will augment the traditional desktop infrastructure, and replicate or utilize many of the same technologies necessary to operate in the current workplace environment.

At the end of FY15, mobility advancements included:

- Participating in the DoD Mobility Unclassified Capability Service.
- Enabling government-furnished equipment (GFE) mobile communication devices to access classified knowledge centers and collaboration websites.
- Participating in the DoD Mobility Classified Capability (DMCC) Pilot, with initial operating capability achieved by end of FY15 for DMCC (Secret and Top Secret).
- Providing an online unclassified mobile device manager.

A key focus in FY16-17 will be the development of the Army Mobility Strategy, which will enable the Army to perform mission functions and execute tasks anytime, anywhere on any device. 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. The Army Mobility Strategy will address five key areas.

- Goal: *Advance and Evolve the Army Information Enterprise Infrastructure to Support Mobile*
- Goal: *Institute Mobile Policies and Standards*
- Goal: *Promote the Development and Use of DoD Mobile and Web-Enabled Application*
- Goal: *Establish a Mobility Security Architecture*
- Goal: *Establish a Mobile Acquisition Framework*

The Army Mobility Strategy, aligned with those DoD and the other Services, will be the foundation for capability development and implementation moving forward. While developing

## UNCLASSIFIED

and establishing the strategy is a key focus, other mobility activities in the near term include the following.

In FY16:

- Reaching full operating capability (FOC) for the DoD Mobile Unclassified Capability Service with an online unclassified Mobile Application Store.
- Delivering initial mobile access to unclassified data and information.
- Using government-furnished mobile communication devices to access classified knowledge centers and collaboration websites through multiple classification levels.
- Providing an online classified mobile device manager.

In FY17:

- Integrating Unified Capabilities into the Mobile Enterprise Unclassified Capability.
- Establishing commercial carrier contracts, which will be available through the Next-Generation Blanket Purchase Agreements managed by NETCOM.
- Delivering initial mobile access to classified data and information.

The Army will satisfy generating and operating force requirements for a mobile capability that can provide unclassified and classified information sharing via voice, video and data. The Army workforce will have transitioned to an IT platform that allows users to perform work-related activities regardless of physical location. This will be accomplished over secure connections by an authenticated user at a classification level appropriate to the mission and the data content (e.g., public, unclassified or classified).

Generating force users will continue to employ government-furnished computing and mobile devices, which will allow operational assessments and evaluations. The validation and widespread adoption of mobility across the generating force will depend on several policy, cost, risk, performance and legal tradeoffs. Deployed operating force users will eventually be able to use militarized, government-issued, classified mobile devices that meet affordability, technical and security requirements. DISA and the NSA have published a plan outlining commercial mobile solutions for a classified capability.

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

Continuous monitoring is defined by DoD as the “ongoing observation, assessment, analysis and diagnosis of an organization’s cybersecurity posture, hygiene and operational readiness.”<sup>4</sup> 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.

---

<sup>4</sup> DoDI 8510.01, Risk Management Framework for DoD Information Technology, 12 March 2014.

## UNCLASSIFIED

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

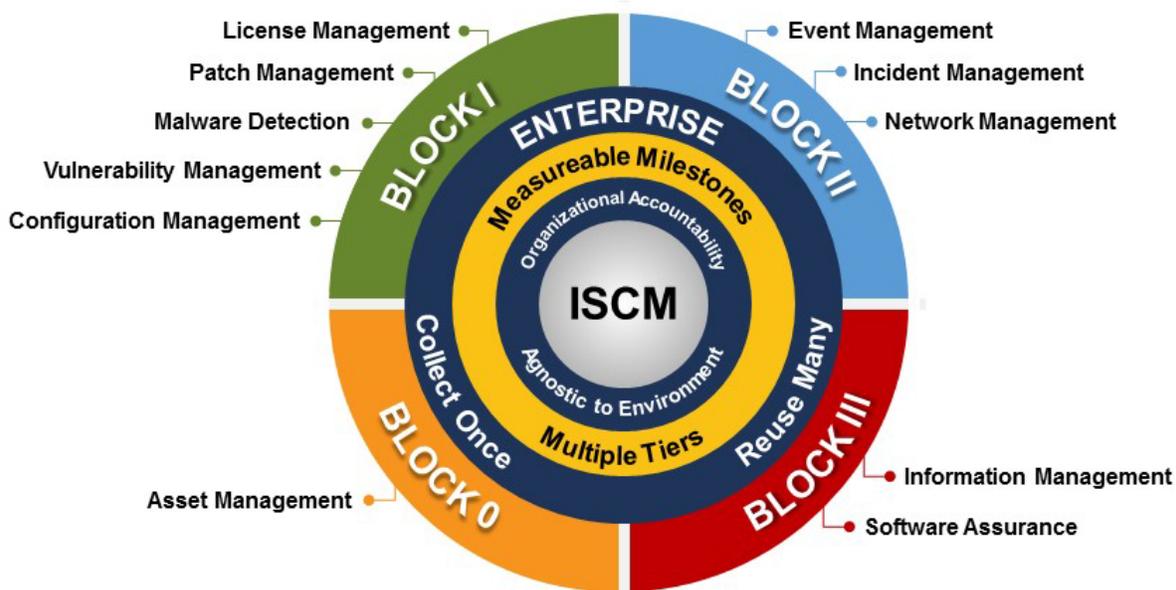


Figure 4: The DoD ISCM Framework

The first two blocks (0-1) depict the groups of activities that the Army will follow, in conjunction with the DoD ISCM Implementation Plan, to support the network activities outlined in this guidance. The remaining blocks (2-3) will be achieved and addressed in out-year implementation planning.

- Block 0, Characterizing the Attack Surface, encompasses the security automation domain of asset management.
- Block 1, Reducing the Attack Surface by Driving Down Vulnerabilities, encompasses the security automation domains of configuration management, vulnerability management, malware detection, patch management and license management (FY16-17).
- Block 2, Sensing and Recognizing Adversarial Behavior, encompasses the security automation domains of event management, incident management and network management (FY17-18).
- Block 3, Managing Information - Measuring the Trustworthiness of Software Processes and Products, encompasses the security automation domains of information management and software assurance (FY19-20).

Incrementally, as each new block is implemented, ISCM knowledge sharing will expand. Once full operating capability is achieved, all information relevant to the 11 security automation

## UNCLASSIFIED

domains will be harvested by the distributed cloud environment. These harvested data, once correlated with policy and threat information, and analyzed for risk management, form the ISCM baseline.

The Army ISCM strategy will align and integrate into the DoD-wide ISCM program. The Army ISCM strategy will:

1. Maintain ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions by producing risk scores.
2. Drive down vulnerabilities in Army information systems via proper system configuration.
3. Create efficiencies through automation and processes.
4. Create a top-down culture of cybersecurity compliance.
5. Provide a supporting structure for the insider threat mitigation initiative.

In FY15, the Army optimized the Host-Based Security System (HBSS) SIPR baseline, through deployment of the Device Control Module, and began reporting the required information to align with ISCM. The Army also deployed the Assured Compliance Assessment Solution (ACAS) Security Center and Nessus modules, as well as 50 percent of SIPRNet User Account Management clients (to support the insider threat mitigation initiative). Additionally, the ISCM team participated in DoD CIO working groups to shape the Army Continuous Monitoring and Risk Scoring (CMRS) solution.

In FY16, the Army will develop an ISCM Strategy based on final guidance from the DoD CIO. The Army also will complete implementation of SIPR HBSS modules, an ACAS baseline across the Army and deployment of user account management on the SIPRNet. In addition, the Army will continue to coordinate with DoD and DISA to define the CMRS solution. Through FY17, Army implementation activities will build on the asset management security automation domain and implement Blocks 1 and 2 of the DoD ISCM Implementation Plan.

### **Army Insider Threat Program (InT)**

The Army Insider Threat (InT) Program is an enhancing capability to provide 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 an 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 user activity monitoring (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 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.

## UNCLASSIFIED

In FY16-17, 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 networks. UAM capabilities will enable the Army to gather information from multiple federal, Department of Defense and local sources to support the following mission tasks.

- Receive, access, integrate and analyze insider threat indicators as authorized and applicable from Army UAM, personnel security, counterintelligence and law enforcement information, 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 Management and Analytic Center in order to support risk decisions, response and mitigation efforts.
- Monitor response and risk mitigation efforts in order to protect against current and emerging threats.

### **Provide Army Enterprise Service Management (AESM)**

As the Army re-engineers and modernizes the network to be more efficient and secure, it will be able to declare cost management success via continuous improvements in efficiency and security. AESM is the Army's ITSM solution, which adopts and adapts best-practice principles and methodologies. By incorporating an Enterprise Service Management as a Service (ESMSaaS) solution, rather than continuing to own and operate costly and disparate instantiations of ITSM tools, the Army will operate as prescribed by the AESMF. The Army's ultimate goal is to manage IT services across the network and to integrate AESM with tactical and Joint ITSM services that have standard platforms. Standardized ITSM will be provided for network operations staff and end users across all Major Commands. Additionally, standardized ITSM functionality will interface with existing and future network operations systems and services. Situational awareness dashboards will be configured for installations, Regional Cyber Centers, the Army Cyberspace Operations and Integration Center, functional commands and other designated commands. The Army expects to save millions in operation and maintenance costs by adopting a cloud solution, though that will require a paradigm shift.

ESMSaaS will simplify the business processes for network management and other support personnel. A global system will improve situational awareness of hardware and software issues on the enterprise network, and licensing costs should significantly decrease as other software is retired and decommissioned. Migrating to a SaaS-based delivery model also will enable Major Commands to eliminate the time, cost, effort and distraction associated with running local and internal service management platforms while still leveraging existing key service management capabilities, enhancing network security, increasing reliability and facilitating information sharing across the enterprise. The training costs associated with staff moving from one organization to another will decrease over time. In addition, the acquisition community and

## UNCLASSIFIED

Army Program Executive Offices will become the offices of primary responsibility for procurement of enterprise-wide ITSM and network operations technologies and services.

In FY15, the PEO EIS Tiger Team published the Army's as-is service management processes and enterprise network operations tools list, and completed product-neutral service work flows for ESMSaaS and market research for existing service providers. CIO/G-6 published the AESM Reference Architecture, AESM Framework and ITSM Policy; Army Cyber Command and Second Army published the AESM CONOPS; and NETCOM published the ESMSaaS CONOPS.

In FY16, the Army will pursue an ESMSaaS materiel development decision, which includes capabilities documents validation and a business case analysis. The Army will conduct an analysis of alternatives between NETCOM's ESM version 8.1 hubs-and-spokes implementation and software as a service, as well as additional market research. The Army will determine a funding bridge strategy for FY17-18 and will allocate future resources as part of the Program Objective Memorandum 18-22 process.

In FY17, the Army will make a decision regarding refresh of NETCOM ESM version 8.1 technology and whether to on-board other major functional commands or migrate them as they are to ESMSaaS. The initial proof-of-concept fielding will occur and the Army will commence systems integration via the Application Programming Interface.

### Standardize Network Operations

Network operations are a core competency of Signal Regiment support to the Army. Network operations entail engineering, installing, operating, maintaining and securing the Army's portion of the DoDIN. They encompass three core areas: enterprise management, net assurance and content management. Network operations capabilities support a wide range of network security and operations functions, including: providing situational awareness; detecting, reporting and resolving security issues; and facilitating the visibility and accessibility of information across the network. They also include technical functions, such as configuration control, system patching, cybersecurity/IA measures, security architecture design, technical specifications and standards development and compliance, operation of HBSS and firewalls.

To enhance standardization of network operations processes and IT across the Army network, the CIO/G-6 and the network operations community developed an authoritative CONOPS, metadata requirements and technical information exchange specifications. Additionally, CIO/G-6 has undertaken a multi-year effort to converge network operations tools across the Army.

The network operations metadata requirements will support implementation of DoD and Army information-sharing objectives, as directed by DoD Instruction 8320.02 (Sharing Data, Information, and Information Technology Services), which will help make the network's data visible, understandable, accessible, trusted and interoperable. The Army is still determining how best to integrate program-of-record (POR) and non-POR tools across the institutional and tactical environments.

## UNCLASSIFIED

In FY15, the Army published the authoritative Army Network Operations Concept of Operations (Network Operations from the Enterprise to the Deployed Environment) and a reference architecture, which includes metadata requirements that support the DoD network operations strategic vision and technical information exchange specifications. An Army networks operations tools convergence strategy and an enterprise-wide network operations tools framework also were released. The framework identifies and defines the fields necessary to collect tools information and to conduct analysis of the network operations tools standardization process. A recurring enterprise-wide network operation tools IPT will focus on standardization activities.

In FY16, the Army will implement the Network Operations CONOPs and the prescribed technical information exchange specifications, and update the reference architecture as needed. Leveraging the network operations tools framework and information collected in FY15, the Army will complete the tools collection process and begin to analyze the data set, identifying redundant tools for possible elimination and prioritizing bridging capabilities between the institutional and tactical environments for end-to-end interoperable network operations. The IPT will continue the collaborative effort to synchronize, prioritize and document the collapse and convergence of tools and applications. The Army also will investigate options for an online enterprise network operations tools repository to store, update and validate network operations tools data.

In FY17, the Army intends to establish the selected online network operations tools database and will continue to standardize (converge) network operations tools Army-wide. The Army also will develop a strategy for compliance with technical information exchange specifications, using a configuration control process. Network operations tools policies and guidance will be updated, as necessary.

### **Increase the Agility of Spectrum Management Operations**

The electromagnetic spectrum is increasingly congested due to expanding DoD and commercial use, and contested by adversarial use and actions. Further, the Army may not have full control of the electromagnetic spectrum in a particular operating environment.

Spectrum management consists of synchronizing, coordinating and managing all elements of the electromagnetic spectrum through engineering and administrative tools and procedures. Spectrum management operations encompass three core areas: spectrum assignment, spectrum deconfliction and spectrum monitoring. Spectrum management operations capabilities support a wide range of network operations functions, including: providing situational awareness; detecting, reporting and resolving electromagnetic interference issues; and facilitating the transport of information across the network.

In FY15, the Army began using the DISA Coalition Joint Spectrum Management Tool as a bridge solution until the Electronic Warfare Planning and Management Tool (EWPMT) with Capability Drop 2 can be implemented. The Army also improved electromagnetic spectrum data accuracy and compliance with the XML data standard from Military Command, Control, Communications and Computers Executive Board (MC4EB) Publication 8, Standard Spectrum Resource Format (SSRF) Version 3.1.

## UNCLASSIFIED

In FY16, the Army will implement an initial EWPMT with spectrum visualization and an initial electromagnetic spectrum deconfliction capability. Additionally, the Army will improve electromagnetic spectrum data accuracy and standardization by migrating all legacy EMS data to the XML data standard in MC4EB Publication 8, SSRF Version 3.1.

The Army will continue deployment and improvement of EWPMT Capability Drop 1 in FY17, and will begin to implement Capability Drop 2 functions on the existing tool. Validation of existing EMS data in SSRF V3.1 will continue, and the Army will begin to capture new data in this format to populate the DISA Joint Spectrum Data Repository. The Army also will explore emerging monitoring capabilities to increase situational awareness, mitigate potential electromagnetic interference and improve the overall health of the network.

The aforementioned spectrum management operations activities in the FY16-17 timeframe will help shape the development of emerging network capabilities. The overall goal, and benefit to the Army, is to ensure that Army forces have the ability to manage spectrum effectively and efficiently, to identify and mitigate interference, and to execute network operations, all of which are critical to maintaining freedom of maneuver and operational efficacy within the electromagnetic spectrum.

### **Enhance Cyber Situational Awareness by Leveraging Big Data/Cyber Analytics**

Big Data/cyber analytics is the process of analyzing and mining massive amounts of data, which can be leveraged to enhance cyber situational awareness. Large amounts of data are examined to uncover hidden patterns, unknown correlations and other useful information. Current advances in sharing and fusing cyber-threat indicator data in near-real time will enable the Army to employ active cyber defense operations, improving protection, detection, response and situational awareness. Similarly, advances in analyzing traffic flow data open new possibilities for detecting anomalous activity, including risk-assessment outcome-based performance metrics.

### ***Integrate Big Data Management into the Army Data Strategy***

Army Big Data management for decision analytics and cloud computing, a component of the Army Data Strategy, will establish an effects-based approach to ensure that Army resources are aligned with Army objectives and compliance criteria. In FY16, the Army will publish an overall data strategy to guide development of Big Data-centric capabilities for management, advanced analytics and decision making. The Army will also continue analyzing, planning and conducting a series of Big Data/cyber analytics pilots to verify and validate that Big Data solutions can be operationalized across the force to enhance real-time situational awareness for cyberspace operations.

There are several Big Data/cyber analytics efforts across DoD focused on enabling cyberspace situational awareness. The most significant effort is with DISA, which has developed the Cyber Situational Awareness and Analytic Capabilities (CSAAC) that execute on the new Big Data Platform (BDP), formerly known as the Rapid Deployment Kit (RDK). Both CSAAC and BDP are accredited and operationally deployed in the Acropolis unclassified and Secret environments at DISA's St. Louis data center. Some Army-specific pilot projects are detailed below.

## UNCLASSIFIED

### *Army Cyber Research and Analytics Lab (ACAL) Big Data/Cyber Analytics Pilot I*

ARCYBER is building a high-capacity storage and computing cluster (Big Data architecture) at the Army Research Lab (ARL). ACAL efforts so far have focused on establishing a Big Data/cyber analytical environment that provides a consistent platform and facility for distributed development of Army cyberspace tools by its partners. As ACAL matures, the intent is to support rapid development of requirements for the Army's computer network defense analytic capabilities across ARL, ARCYBER, NETCOM and their partners.

By the end of FY15, ARL had collaborated with multiple organizations, including government, national laboratories, federally funded research and development centers, academia and industry, to develop multiple cyber analytic capabilities. For example, the Army and its partners are working on preemptively detecting SQL injection attempts against externally facing web servers in order to prevent unauthorized modification of data and to help determine the specific target of and attribution for potential attacks.

Other efforts focus on developing and employing a risk-scoring algorithm to identify systems likely to be targeted by the enemy, and to prioritize remediation efforts for the operational force. The Army will continue to upgrade existing systems to track cyberspace incidents and to convert existing cloud-based analytics for compliance monitoring and system vulnerability detection. Detecting and identifying suspicious Domain Name System requests, which will help focus analysis of potential malicious activity, and instituting continuous monitoring are priorities, as well.

### *Defensive Cyberspace Operations Big Data/Cyber Analytics Pilot II*

The Army's JRSS Big Data Pilot II builds on the achievements and accomplishments of the Army's Big Data/Cyber Analytics Pilot I, which continues exploration of Big Data platforms and Big Data analytics within the context of defensive cyberspace operations and the DISA Big Data Platform/Cybersecurity Situational Awareness Analytic Cloud (BDP/CSAAC).

With the implementation of Pilot II, the Army will improve both DoDIN and defensive cyberspace operations through the use of Big Data analytics, enhancing situational awareness, continuous monitoring and insider threat detection. Pilot II will use Big Data/cyber analytics to identify cyberspace vulnerabilities and threats through DISA's BDP platform, whose functionality, capability and efficiency will be augmented via a series of architectural, design and implementation changes. The pilot will improve the Army's understanding of requirements and constraints related to the collection and analysis of information using Big Data platforms, demonstrating how data from multiple sources can be collected and stored and how the analytics development strategy impacts the efficiency and effectiveness of defensive cyberspace operations analytics.

In FY16, the Army plans to deploy Rapid Deployment Kit 2.2 into Acropolis at the St. Louis Defense Enterprise Computing Center, and to ingest data from five data sources. The Army and its partners will develop and demonstrate advanced analytics on both Acropolis and DREN platforms, and improve solution strategy and technical requirements relative to data value, veracity, velocity, variety and volume.

## UNCLASSIFIED

In FY17, the Army will begin to add Big Data efforts into its defensive cyberspace operations program and deploy additional Big Data/cyber analytics platforms to JRSS sites. It also will examine architecture and design options for alternative Big Data/cyber analytics solutions.

### **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 that are 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 future operations; and project power in or through cyberspace.

Operational planning teams have identified a set of workforce-related topics they will address and have validated certain work roles (core, direct support and specialized support) within the context of the DoD Cyberspace Workforce Framework. In FY16-17, cyberspace workforce refinement activities will continue to identify, shape and track the civilian cyberspace workforce, define work roles and align civilian workforce roles with the uniformed Career Field 17 structure.

#### *Identify, Shape and Track the Civilian Cyberspace Workforce*

In FY16-17, the Army will progressively 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.

#### *Define Work Roles*

By the end of FY16, the Army will establish a comprehensive career management plan for its cyberspace workforce. This plan will identify strategies to designate, recruit, develop, credential and retain the cyberspace workforce.

#### *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 FY17, 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

## UNCLASSIFIED

sets with work role requirements in order to ensure that the most qualified personnel are assigned to the right work roles.

### Summary

NSD FY16-17 targeted priorities are intended to satisfy the security attributes of confidentiality, integrity and availability of data for information systems and networks. NSD initiatives will support both the operational and institutional environments, and set the stage for future DoDIN operations and cybersecurity enhancements. The resulting strategic effects of improved DoDIN operations, security, information sharing and data protection lay the framework for capability gap mitigation and meeting the projected end states in the FY18-22 timeframe.

## Appendix 4 – Glossary

TERM	DEFINITION
Assure Access	The ability to identify and authenticate individuals, groups and entities, and provide authorization to services and information. (JCA 6.1.3.1.1)
Assure Transfer	The ability to exchange authentic data, information and knowledge 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)
Cybersecurity	The ability to provide the measures that protect, defend and restore information and information systems. (JCA 6.1.3)
Data Center / Cloud / Generating Force (DC/C/GF)	Provides IT service capabilities in four environments that, within a security classification level, are able to share the same DC and non-server infrastructure. The environments are: <ol style="list-style-type: none"> <li>1) Cloud environment, which shares hardware resources through contemporary virtualization technologies, and automates provisioning and management of resources using modern cloud technologies.</li> <li>2) Enterprise resource planning (ERP) enclave environment, which contains ERP technologies using virtualized and dedicated servers.</li> <li>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.</li> <li>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.</li> </ol>
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)

**UNCLASSIFIED**

<b>TERM</b>	<b>DEFINITION</b>
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) or 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 or receive voice, data, video and integrated telecommunications via wire or optical means within the confines of a platform or an installation (e.g., command post, installation, headquarters or federal building). (JCA 6.1.1.1.1)
Long-Haul Telecommunications	The ability to disseminate, transmit or receive voice, data, video and integrated telecommunications via wire or optical means to, from and between platforms and/or 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 and the underlying physical assets that provide end-user services, as well as connectivity to enterprise application services. (JCA 6.1.2)
Network Resource Visibility	The ability to determine 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)
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)

**UNCLASSIFIED**

<b>TERM</b>	<b>DEFINITION</b>
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.
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 a 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)
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)

**UNCLASSIFIED**

## Appendix 5 – Acronyms

<b>ACRONYM</b>	<b>DEFINITION</b>
ACAS	Assured Compliance Assessment Solution
ACS	Area Core Switches
ADMP	Army Data Management Program
AEN	Army Enterprise Network
AENC	Army Enterprise Network Council
AESD	Army Enterprise Service Desk
AESMF	Army Enterprise Service Management Framework
AIA	Army Information Architecture
AKO	Army Knowledge Online
ANCP	Army Network Campaign Plan
ARNG	Army National Guard
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
AWFC	Army Warfighting Challenge
BCT	Brigade Combat Team
BMA	Business Mission Area
BPA	Blanket Purchase Agreement
C2	Command and Control
C4IM	Command, Control, Communications, Computers and Information Management
CDC	Core Data Center
CDF	COE Data Foundation
CE	Computing Environment
CHESS	Computer Hardware, Enterprise Software and Solutions
CIO	Chief Information Officer
CMI	Cryptographic Modernization Initiative
CMRS	Continuous Monitoring and Risk Scoring
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
DCO-IDM	Defensive Cyberspace Operations – Internal Defensive Measures
DEE	Defense Enterprise Email
DEPS	Defense Enterprise Portal Service
DIMA	Defense Intelligence Mission Area
DISA	Defense Information Systems Agency
DMCC	DoD Mobility Classified Capability
DoD	Department of Defense
DoDIN	DoD Information Network
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy
EAS	Edge Access Switch
ECMCS	Enterprise Content Management and Collaboration Services
EDS	Enterprise Directory Service
EIE	Enterprise Information Environment
EIEMA	Enterprise Information Environment Mission Area
EHF	Enterprise Hosting Facility
EKMS	Electronic Key Management System
ELA	Enterprise License Agreement
ESD	Enterprise Services Domain
ESMSaaS	Enterprise Service Management System as a Service
EUD	End-User Device
EXORD	Execute Order
FOC	Full Operating Capability

**UNCLASSIFIED**

<b>ACRONYM</b>	<b>DEFINITION</b>
FRAGO	Fragmentary Order
FY	Fiscal Year
GAL	Global Address List
Gbps	Gigabits per second
GFE	Government-Furnished Equipment
GOSC	General Officer Steering Committee
GPS	Global Positioning System
GVS	Global Video Service
HBSS	Host-Based Security System
HSMCC	Home-Station Mission Command Center
IaaDS	Installation as a Docking Station
IC	Intelligence Community
ICAN	Installation Campus Area Network
IC-ITE	Intelligence Community Information Technology Enterprise
ICS	Institutional Capability Set
IdAM	Identity and Access Management
IES	Information Exchange Specifications
IOC	Initial Operating Capability
IP	Internet Protocol
IPN	Installation Processing Node
IPT	Integrated Project Team
ISCM	Information Security Continuous Monitoring
ISN	Installation Service Node
IT	Information Technology
ITSM	Information Technology Service Management
JIE	Joint Information Environment
JMT	Joint Migration Team
JRSS	Joint Regional Security Stack
JWICS	Joint Worldwide Intelligence Communications System
KMI	Key Management Infrastructure
L/V/C/G	Live/Virtual/Constructive/Gaming
LOE	Line of Effort
MC	Mission Command
MGC	Management Client
MNVR	Mid-Tier Networking Vehicular Radio
MPE	Mission Partner Environment
MPLS	Multi-Protocol Label Switching
MUOS	Mobile User Objective System
NCD	Network Capacity Domain
NETCOM	Network Enterprise Technology Command
NIEM	National Information Exchange Model
NIPR	Non-Secure Internet Protocol Router
NIPRNet	Non-Secure Internet Protocol Router Network
NOC	Network Operations Center
NOSEC-L	Network Operations and Security Center - Light
NSA	National Security Agency
NSD	Network Operations and Security Domain
NSS	National Security System
O365	Microsoft Office 365
O&M	Operation and Maintenance
OCONUS	Outside the Continental United States
OCS	Operational Capability Set
OMB	Office of Management and Budget
OTM	On the Move

**UNCLASSIFIED**

<b>ACRONYM</b>	<b>DEFINITION</b>
OTNK	Over-the-Network Keying
PACOM	Pacific Command
PfM	Portfolio Management
RAF	Regionally Aligned Forces
RCC	Regional Cyber Center
RFI	Request for Information
RHN	Regional Hub Node
SIPR	Secure Internet Protocol Router
SIPRNet	Secure Internet Protocol Router Network
SMT	Service Migration Team
SONET	Synchronous Optical Network
SPPN	Special Purpose Processing Node
SRM	Sustainment Readiness Model
STaaS	Storage as a Service
SWA	Southwest Asia
T2C2	Tactical Transportable Command and Control
TDM	Time Division Multiplexing
TLA	Top-Level Architecture
TRADOC	Training and Doctrine Command
UAP	Unified Action Partner
UC	Unified Capabilities
USAR	U.S. Army Reserve
VoIP	Voice over Internet Protocol
VTC	Video Teleconference
WAN	Wide Area Network
WGS	Wideband Global SATCOM
WIN-T	Warfighter Information Network - Tactical
WMA	Warfighting Mission Area