Office of the Army Chief Information Officer/G-6

ARMY NETWORK CAMPAIGN PLAN 2020 & BEYOND

Implementation Guidance

NEAR-TERM

2015-2016

February 2015

CIO/G-6

ENABLING SUCCESS For Today & Tomorrow

U.S.ARMY

CIOG6.ARMY.MIL

DISCLAIMER

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 Do not cite this document for the purpose of advertisement.

CHANGES

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

Executive Summary

Over the last decade, the Army has invested heavily in augmenting and integrating the network's operational component capabilities while investments in the enterprise and installation components have remained relatively stagnant, fostering significant disparities. To enable the Army of 2020 and Beyond to meet the challenges of the 21st century, it is essential for the Army to rebalance and unify the network into an end-to-end capability. The *Army Network Campaign Plan (ANCP) – Implementation Guidance, Near-Term* frames the planning to support the design, development and fielding of network capability enhancements.

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 process[1], the Army will maintain and modernize the network in fiscal years (FY) 2015-2016.

This document describes how planned execution initiatives in FY 2015-2016 will enable the network end states envisioned in the ANCP. The near-term implementation guidance provides direction and insight to align the development of the Army enterprise, systems of systems and system architectures with Army network strategy and IT portfolio planning. This document will set the conditions for the mid-term implementation guidance, which covers capability modernization and associated activities in FY 2017-2021.

The initiatives being executed during FY 2015-2016 enable network advancements to support future mission operations and bring the enterprise to the Soldier. Activities are occurring through programs of record and other initiatives to ensure that the institutional network infrastructure is proactively modernized to seamlessly integrate with operational network initiatives. Near-term efforts focus on transitioning Army users from disjointed systems to an enhanced, centralized service and will return tangible benefits to the user as the Army increases bandwidth, improves security and deploys enterprise services.

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

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

This page intentionally left blank.

Table of Contents

Executive Summary 3
Table of Contents 5
Introduction 7
Army Network Campaign Plan (ANCP) Construct 7
ANCP, Near-Term Construct 7-8
FY 15–16 Activities 9
FY 15–16 Primary Efforts 10-15
FY 15–16 Supporting Efforts 16-19
Summary 19
Appendix 1 – Network Capacity Domain 1-1
FY 15–16 Targeted Priorities 1-2
Summary 1-8
Appendix 2 – Enterprise Services Domain 2-1
FY 15–16 Targeted Priorities 2-1
Summary 2-10
Appendix 3 – Network Operations & Security Domain 3-1
FY 15–16 Targeted Priorities 3-2
Summary 3-11
Appendix 4 – Capability Taxonomy 4-1
Appendix 5 – Acronyms 5-1

This page intentionally left blank.

Introduction

Building on the momentum and network-related efforts of fiscal year (FY) 2014, CIO/G-6 is leading near-term activities in FY 2015-2016 to continue modernization necessary to support Army strategy and missions. The *ANCP – Implementation Guidance, Near-Term* captures the major activities within the FY 15-16 timeframe and sets conditions for the *ANCP – Implementation Guidance, Mid-Term*.

Army Network Campaign Plan (ANCP) Construct

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

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

Table 1: ANCP Construct

ANCP Near-Term Construct

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

The *ANCP – Implementation Guidance, Near-Term* is developed by the Army Enterprise Network (AEN) domains (Network Capacity, Enterprise Services and Network Operations and Security) in coordination with multiple communities of practice, including functional experts,

mission area representatives, information technology (IT) strategic planners, resource planners and managers, and acquisition experts. The AEN domains conduct cross-cutting analysis, utilizing multiple data sources that include: Army strategic guidance, senior leader goals and objectives, current Army mission obligations, the status of Enterprise Information Environment Mission Area IT investments, acquisition plans and resourcing plans. Near- to mid-term activities, supported through IT investments, will be aligned, managed and tracked through five Lines of Effort.

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

The goals of the Lines of Effort are outlined below.

LOE 1 – 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 both the operating and generating forces.

LOE 2 – Optimize Defensive Cyber 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 – Lead and integrate Army strategy, policy and resourcing to deliver a robust and secure transport and computing infrastructure that will enable assured warfighting and business operations.

LOE 4 – Provide a consistent, end-to-end user experience by developing strategy, policy, resources and change management for the transition of IT services from local implementations to enterprise capabilities.

LOE 5 – 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, and simplify and standardize network operations capabilities in support of and integrated with DoDIN Operations.

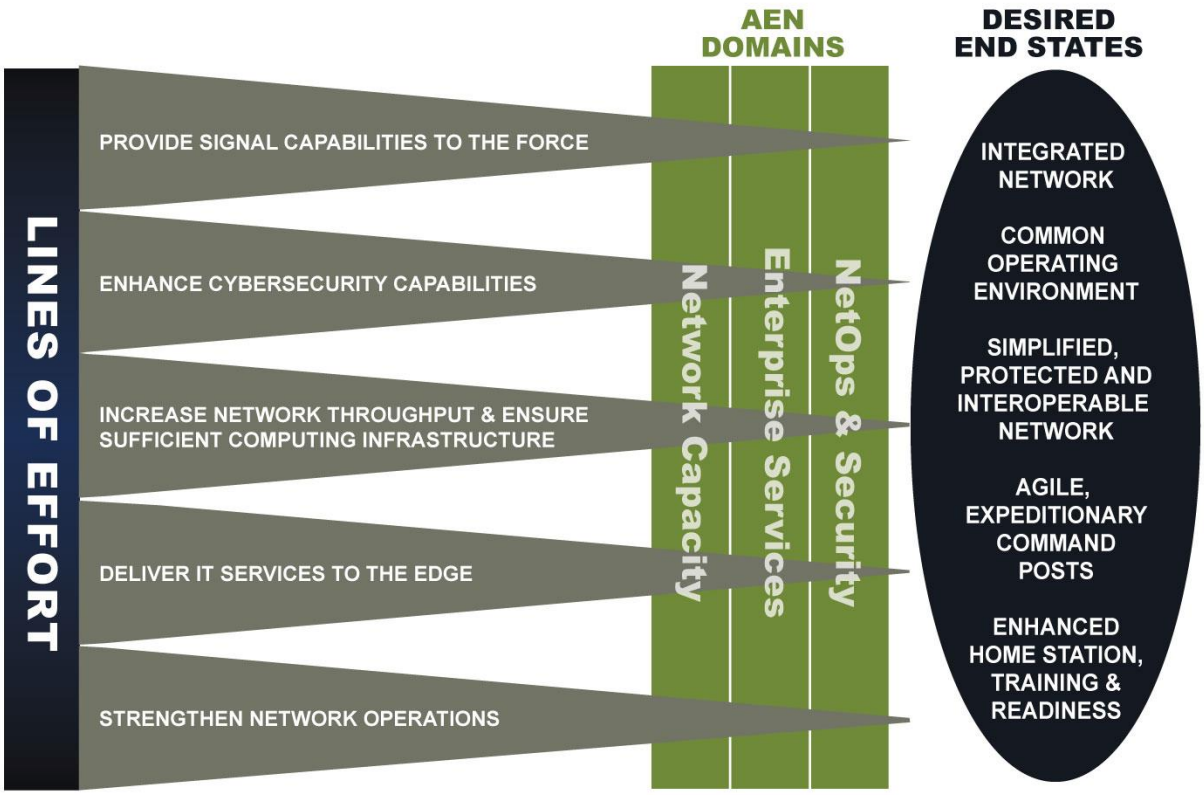

Figure 1: ANCP Operating Construct

The initiatives being executed during FY 2015-2016 enable network advancements to support future mission operations and bring the enterprise to the Soldier. Activities are occurring through programs of record and other initiatives to ensure that the institutional network infrastructure is proactively modernized to seamlessly integrate with operational capability set efforts (OCS). Near-term efforts focus on transitioning Army users from disjointed systems to an enhanced, centralized service through the implementation of unified capabilities (UC) and 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.

FY 15-16 Activities

AEN domains assess, plan and orchestrate investments within their respective portfolios. The Network Capacity Domain (NCD) portfolio encompasses network and computing infrastructure; the Enterprise Services Domain (ESD) portfolio encompasses enterprise-level services across the Army network; and the Network Operations and Security Domain (NSD) portfolio encompasses cybersecurity and network operations, as depicted in Figure 2. 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 LOEs.

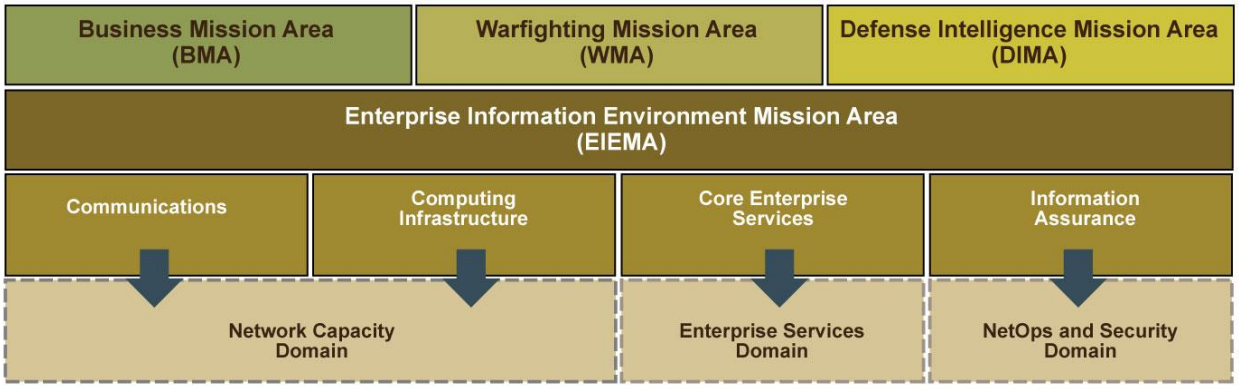

Figure 2: Army IT Portfolio Management Construct

The AEN domain efforts retain complex relationships, which are critical to reaching desired end states in the near-term timeframe to provide the necessary alignment to allow the network to eventually achieve end states in the mid and long term. Primary efforts are critical to enabling the network to achieve either end states in the near term or to set conditions for modernization in follow-on years, e.g., FY 17-21. While still important, supporting efforts enable primary efforts, bolster planned initiatives or deliver forecasted efficiencies. Primary and supporting efforts may occur only within a specific AEN domain or, due to interdependencies, may span multiple AEN domains 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.

FY 15-16 Primary Efforts

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

- Common Operating Environment (COE)
- Unified Capabilities (UC)
- Operational Component Modernization
- Infrastructure Modernization & Network Consolidation
- Cyber Attack Surface Reduction
- Structure Authorized Hosting Environments
- Organize and Advance Mobility
- Information Security Continuous Monitoring
- Enhance Cyber Situational Awareness by Leveraging Big Data Analytics
- Refining the Role of Cyber Workforce

Common Operating Environment

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. Computing environments (CEs) are logical groupings of systems with similar characteristics used to organize the COE (data center/cloud/generating force, command post, mounted, mobile/handheld, sensor, and real-time/safety critical/embedded). A CE comprises the

hardware, operating systems, libraries and software required to run applications within the COE. The COE sets the conditions for the Army to produce high-quality applications rapidly, while reducing the complexities imbedded in the design, development, testing and deployment cycle. It also offers the promise of transforming 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 develop, test, certify and deploy software capabilities rapidly and efficiently while mitigating the introduction of harmful or unexpected behavior.

While the COE is not a system or program in the traditional DoD acquisition sense, it will provide overarching governance, technical guidance and a set of validated technical and non-functional requirements for the development of IT infrastructure and business or mission capabilities. Those requirements will be implemented in an incremental fashion across successive versions of the COE. Detailed implementation activities for the COE are captured in the 10 September 2014 COE Implementation in Support of the Operational Force Execution Order.

Network Activities	LOEs	AEN Domains	Army Benefits
• Develop set of validated top-level COE requirements to guide the design and architectures of the individual CEs. • Implementation of open standards within the CE architecture. • Implement and field COE version 2.	**3** 4 2 5 1	• NCD • ESD • NSD	• Ensure interoperability across environments and foster reuse of common components. • Enable device-agnostic capabilities. • Increased capability agility. • Reduced lifecycle costs through standardized applications and unity of effort. • Flexible infrastructure that evolves to rapidly emerging standards. • Enhanced cyber protection.

Unified Capabilities

Unified capabilities (UC) provide the Army an enterprise-level solution that enables universal collaboration through voice, video and/or data. In FY 15-16, the Army will analyze and plan for consolidation of communications media, reducing reliance on disparate and legacy communication methods while simplifying the user experience.

Network Activities	LOEs	AEN Domains	Army Benefits
• Deploy UC: Soft Client bridging solution, Voice Over Internet Protocol (VoIP) and Global Video Services (GVS).	**4** 3 2 5	• ESD	• Improve user experience with timely access to data at the point of need. • Standardize and improve ease of use for network users. • Reduce operating and sustainment costs.

Operational Component Modernization

Concerted efforts are under way in FY 15-16 to begin aligning the operational and institutional components of network modernization. This alignment, through various planning efforts such as the Army Network Synchronization Working Group and Army Enterprise Network Synchronization Conference, will result in a synchronized and interoperable network. The end-to-end alignment of the network's operational and institutional components will improve network support of readiness, training and home-station mission command (MC) operations. Soldiers and units will experience enhanced capabilities across the network, specifically, more direct and transparent access to enterprise-level services utilizing Installation as a Docking Station (IaaDS) and the Integrated Training Environment (ITE). The table below describes some of the first activities that demonstrate this alignment, which will grow and improve in the future.

Network Activities	LOEs	AEN Domains	Army Benefits
• Warfighter Information Network – Tactical (WIN-T) Increment 2 fielding. • CP CE 1.0 & 2.0 • Institutionalize IaaDS concept • Interim en route MC capability	**1** 3 2 4 5	• NCD	• Provide more reliable and versatile on-the-move tactical communications, improving collaboration among forces at all levels. • Simplify the network – ease of use, reduced number of systems, more agile Command Posts. • Improve force readiness for no-notice deployments. • Enable deploying forces to develop situational understanding and continue to plan while embarked on strategic airlift.

Infrastructure Modernization, Network Consolidation

In FY 15-16, the Army will continue to improve the institutional network infrastructure while converging and integrating separate networks. By increasing the available throughput, the network will have the capacity necessary to: fully leverage enterprise services and support UC; improve the user experience with timely access to data at the point of need; enhance visibility of the network; and simplify network management and defense. These infrastructure upgrades will enable the divestiture of redundant legacy systems, leading to significant cost savings.

Network Activities	LOEs	AEN Domains	Army Benefits
• Continue deployment of Multi-Protocol Label Switching (MPLS) to Continental United States (CONUS) & Outside the Continental United States (OCONUS) installations. • Continue the technical integration of separate networks, e.g., Army Reserve, Army National Guard, Corps of Engineers, ITE, Army Materiel Command and Medical Command. • Continue implementation of intra-installation network infrastructure modernization (Area Dissemination Node/End-User Building upgrades).	**3** 2 5	• NCD	• Provide sufficient throughput to fully leverage enterprise services and support UC. • Increase reliability, availability and flexibility to enable garrison-based MC operations and live, virtual, constructive and gaming (L/V/C/G) training. • Improve user experience with timely access to data at the point of need. • Reduce operating and sustainment costs.

Cyber Attack Surface Consolidation

The Army will continue efforts to reduce duplicative legacy systems. The consolidation of network points of presence associated with commercial networks will reduce the potential exposure to cyber threats and attacks, and simplify network management and network defense.

Network Activities	LOEs	AEN Domains	Army Benefits
• Converge and consolidate Top Level Architecture (TLA) Stacks into Joint Regional Security Stacks (JRSS).	**2** 5 3	• NSD	• Simplify network complexity, reduce the attack surface of the network and standardize network security.

Structure Authorized Hosting Environments

To adhere to DoD mandates and lay the foundation for future cloud computing capabilities, the Army will continue to consolidate and transition standalone data center solutions to DoD-authorized enterprise hosting environments. The Army will undertake a major rationalization effort for current applications to prepare for and enable this transition. These initiatives will lay the computing foundation for future-year data support and data analytics across the network. They also will enable the retirement and divestiture of standalone data centers, redundant applications and obsolete support infrastructure to reduce or avoid unnecessary costs for sustainment and modernization. The Army will concentrate its efforts to deliver enterprise services, such as email, UC, file sharing and Army Software Marketplace, via the cloud. In FY 15, the Army will be refine requirements, policy development, resourcing and transition planning, and in FY 16 pursue acquisition of the services.

Network Activities	LOEs	AEN Domains	Army Benefits
• Continue to transition standalone data centers to DoD-authorized hosting environments. • Establish Installation Processing Nodes (IPN) and Installation Service Nodes (ISN). • Rationalize, modernize and migrate applications to DoD-authorized hosting environments (application migration to NIPRNet enclave in commercial and DoD hosting environments). • Shape the standardization of Core Data Centers (CDCs). • Develop and publish an Army application hosting methodology.	**3** 4 2 5 1	• NCD • ESD • NSD	• Provide robust data storage, on-demand computing, elastic capacity, improved security and more efficient operation and maintenance. • Reduce the operating force footprint in theater. • Enable rapid and more efficient evolution of applications, minimizing costs and speeding dissemination of application enhancements. • Support the processing of large amounts of data to improve decision-support cycles.

Organize and Advance Mobility

Creating an End User Device (EUD) Strategy and associated execution plans is a major initiative in the FY 15-16 timeframe. While an optimal enterprise mobility capability will not be fully achieved in FY 15-16, 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
• Develop and publish an EUD Strategy that supports the Army, to include traditional reserve component Soldiers. • Select, standardize and certify EUD platforms across the Army, with a focus on commercial devices. • Rationalize commercial contracts that provide devices and transport infrastructure to the Army. • Establish a mobile device store to centralize the hosting and availability of vetted applications that support Army users. • Establish a mobile device manager (MDM) to manage devices and the transport infrastructure.	**3** 4 2 1 5	• NCD • ESD • NSD	• Ensure that the Army is on a modernization path that keeps pace with the evolving technology environment. • Provide an efficient, consistent, secure and reliable mobile device management process, resulting in cost savings and collaboration. • Standardize and simplify the end-user experience across devices.

Information Security Continuous Monitoring

The Army is establishing the Information Security Continuous Monitoring (ISCM) Framework, which will be achieved in a multi-year, iterative effort that leverages current investments in enterprise and non-enterprise cybersecurity tools and capabilities.

Network Activities	LOEs	AEN Domains	Army Benefits
• Host-Based Security System implementation optimized. • Reporting asset information. • Operationalize continuous monitoring risk scoring (CMRS). • Operationalize assured compliance assessment solution (ACAS). • Reduce self-reporting. • Correlate operational attributes. • Initial correlation of vulnerability configuration data. • Program of record reporting. • Convergence compliance scoring.	**2** 5	• NSD	• Provide the Army the ability to make near-real-time risk management and ongoing authorization decisions. • Maintain ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions by producing risk scores. • Drive down vulnerabilities in Army information systems. • Create a top-down culture of cybersecurity compliance.

Enhance Cyber Situational Awareness by Leveraging Big Data Analytics

Big Data analytics are the process of examining very large amounts of data to uncover hidden patterns, unknown correlations and other useful information. Current advances in sharing and fusing cyber-threat indicator data will enable the Army to employ active cyber defense operations, in which increasing amounts of threat indicator data will be available in near-real-time for 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. In FY 15-16, the Army will develop a Big Data Strategy to guide development of data-centric capabilities for management, advanced analytics and decision making. The Army will also analyze, plan and conduct a series of Big Data pilots to verify and validate that Big Data solutions can be operationalized across the force to enhance real-time situational awareness for cyberspace operations (CO).

Network Activities	LOEs	AEN Domains	Army Benefits
• Develop Army Big Data Strategy. • Conduct Big Data pilots.	**2** 5	• NSD	• Improve cyber workforce experience by providing timely access to data to make informed and actionable risk-management decisions. • Reduce time required to perform cyber analytics and forensics. • Provide leadership near-real time risk information to make informed decisions.

Refining the Role of Cyber Workforce

The cyber workforce is closely nested with the broader cyberspace operations workforce and is comprised of Soldiers, civilians and contractors.

The Army must focus on establishing a framework for identifying, shaping and tracking the civilian cyberspace workforce and aligning it with the military structure of Career Field 17. Additionally, roles must be identified to ensure that items not defined in JP 3-12 (cyberspace effects, cybersecurity, intelligence workforce and cyberspace IT) are captured.

Network Activities	LOEs	AEN Domains	Army Benefits
• Align the cyber civilian workforce with the military. • Identify the work roles.	**2** 5	• NSD	• The development and retention of an exceptional cyber workforce is central to DoD's strategic success in cyberspace.

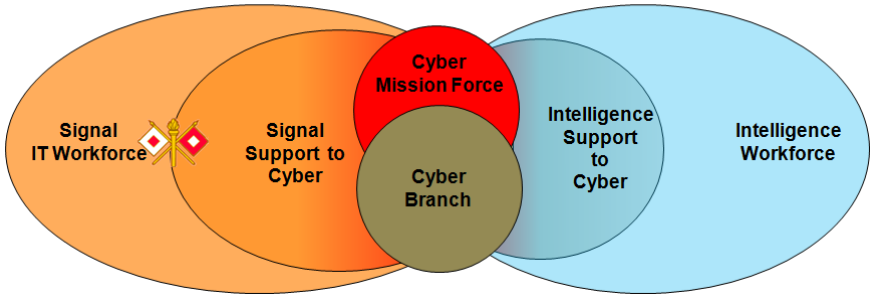

Figure 3: Organization of IT and Cyber Workforce

FY 15-16 Supporting Efforts

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

- Network Operations and Monitoring
- Key Management and Cryptographic Modernization
- Service Management
- Identity Management and Directory Services
- Enterprise License Agreements

Supporting efforts bolster planned initiatives (e.g., primary efforts) or deliver forecasted efficiencies.

Network Operations & Monitoring

FY 15-16 will see a concerted effort to simplify network management tools. The convergence of multiple tools to enterprise-level solutions will provide network managers with greater visibility of the network to identify and mitigate both internal and external threats. Additionally, the Army will be able to divest standalone, redundant network operations and management solutions.

Network Activities	LOEs	AEN Domains	Army Benefits
• Transition multiple network operations tools to enterprise-level network operations tool solutions. • Continue to develop Information Security Continuous Monitoring.	5 2	• NSD	• Simplify network management. • Provide automated network monitoring and reporting capabilities.

Key Management & Cryptographic Modernization

Within the FY 15-16 timeframe, the Army will support the establishment of a single authoritative digital identity for users throughout their career. The use of a single digital identity will set conditions for unified capabilities, enterprise collaboration services (ECS), enterprise attribute-based access control (ABAC) and lifecycle management of person and non-person entity accounts. In addition, this capability will enable the Army to decrease the time users spend establishing network connectivity while transitioning between duty locations.

Continuous upgrade and improvement of key management systems will reduce physical exposure to hostile threats while the Soldier executes network security tasks. Modernizing cryptographic legacy systems position the Army to manage JRSS, leverage enhanced network throughput to deliver over-the-network keys, and improve cyber defense of and support to operational forces.

Network Activities	LOEs	AEN Domains	Army Benefits
• Provide an "over-the-network-keying" (OTNK) management capability. • Modernization of cryptographic capabilities (devices, waveforms, algorithms, etc.).	**2** 5 1	• NSD	• Decrease manual key delivery, which minimizes the number of Soldiers placed in harm's way. • Provide programmable and interoperable encryption capability to ensure exchange of authentic data, information and knowledge between authorized individuals, groups and entities. • Enhance network encryption capability for improved network performance.

Enterprise Service Management

Improvements in service management will align the Army with DoD and joint efforts while providing the user additional responsive services, improved automated ticketing and enhanced tracking and management and support analytics to gauge network performance and provide faster issue resolution.

Network Activities	LOEs	AEN Domains	Army Benefits
• Enhance Army Enterprise Service Desk (AESD) to improve Tier 0 and Tier 1 services to end users. • Deliver Enterprise Service Management System as a Service (ESMSaaS) to improve Tier 2 and above services.	**5** 4 3 2 1	• NSD	• Eliminate the time, cost, effort and distraction associated with running local and internal service management platforms.

Identity Management and Directory Services

Within the FY 15-16 timeframe, the Army will 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. The Army also will leverage identity management solutions to enhance users' ability to search for personnel on the network.

Network Activities	LOEs	AEN Domains	Army Benefits
• Continue Identity and Access Management (IdAM) efforts to establish lifecycle management for user identities. • Leverage user identity solutions to support directory services.	**2** 4 5	• NSD • ESD	• Improved security for authentication, authorization and accountability of user network transactions. • Decrease the time users are without network connectivity while transitioning between duty stations. • Provide a reliable directory to locate users.

Enterprise License Agreements (ELAs)

Network modernization efforts will include consolidating the Army's negotiating and buying power to fully leverage commercial providers for network services.

Network Activities	LOEs	AEN Domains	Army Benefits
• Negotiate and maintain ELAs with vendors that support the network.	**4** 3 5	• ESD	• Centralize the Army's purchasing power to potentially provide the Army larger amounts of software/equipment at a lower cost per item.

Summary

To enable the Army of 2020 and Beyond to meet the challenges of the 21st century, it is essential that the Army rebalance and unify the network into an end-to-end network. The *ANCP – Implementation Guidance, Near-Term* frames planning to support the design, development and fielding of network capability 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 FY 15-16. By synchronizing planning with the realities associated with Army mission obligations, the resourcing picture and changes in acquisition planning, this document serves as the foundation for the design of capability packages and near-term implementation planning. 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.

Appendix 1 – Network Capacity Domain

The Network Capacity Domain (NCD) portfolio includes the physical infrastructure necessary for all services and information-based activities to pass through the network. The portfolio encompasses the foundational infrastructure upon which enterprise services and network operations and security solutions reside. The goal of the NCD portfolio is to provide the optimized set of investments necessary for provisioning the transport and computing infrastructure of a modernized, global and versatile network that gives regionally aligned forces (RAF) and unified action partners (UAPs) the full range of military and business operational advantages across all joint operational phases. The NCD will leverage existing capabilities and assess portfolio investments based on implementing the Army's Network 2020 and DoD's Joint Vision 2020 architectures. Within the FY 15-16 timeframe, NCD will focus on network infrastructure modernization, data center consolidation and end-user environment requirement maturation within the enterprise, installation and deployed mission environments, as well as the intersection of modernization requirements across these mission environments.

These efforts 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*. It identifies the need for a robust transport infrastructure that provides sufficient, modern, resilient and reliable computing and storage capacity, in addition to enabling EUD and mobile capabilities. The DoD CIO memorandum mandates migration of applications, systems and data to DoD-approved enterprise hosting facilities by the end of FY 18, thus driving FY 15-16 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.

FY 15-16 Targeted Priorities

The table below lists FY 15-16 NCD activities and shows which JCA they impact.

FY 15–16 NCD Activities	Joint Capability Area 6 Net-Centric									
	6.1 Information Transport						6.2 Enterprise Services			
	6.1.1 Wired Transport		6.1.2 Wireless Transmission		6.1.3 Switching and Routing		6.2.2 Computing Services			
	6.1.1.1 Localized Communications	6.1.1.2 Long-Haul Telecom-munications	6.1.2.1 Line of Sight	6.1.2.2 Beyond Line of Sight	6.1.3.1 Communication Bridge	6.1.3.2 Communication Gateway	6.2.2.1 Shared Computing	6.2.2.2 Distributed Computing	6.2.2.3 Server Services	6.2.2.4 End-User Services
Network Infrastructure Modernization and Path Diversity	●	●	●	●	●	●				
Integrate Separate Networks	●	●	●	●	●	●				
Improve Transport Capacity for Deployable Forces			●	●	●	●				
Data Center Consolidation & IPN/ISN/SPPN Standardization							●	●	●	
EUD Strategy										●
Divestiture Planning	●	●	●	●	●	●	●	●	●	●

Network Infrastructure Modernization

Network infrastructure modernization involves increasing the throughput and resiliency on installations, deploying MPLS at major installations and ensuring that installations have dual-path diversity to minimize or eliminate the impact of network transport interruptions on critical user communities. With Army National Guard (ARNG) and United States Army Reserve (USAR) concurrence, all Army components will be integrated into the enterprise network architecture, improving throughput/connectivity for National Guard, Joint Forces Headquarters (JFHQs), armories, Reserve centers and active component installations. These efforts will minimize throughput as a limiting factor in the execution of information-based mission activities and will strengthen network security.

In FY 15, network infrastructure modernization activities include:

- Deploying MPLS upgrades and implementing dual-path diversity for the remaining major CONUS, Southwest Asia (SWA) and Europe installations.
- Initiating installation of MPLS upgrades and dual-path diversity in the Pacific Command (PACOM) theater.
- Increasing throughput for Installation Campus Area Networks (ICANs) via area core switches (ACS) and edge access switches (EAS) on CONUS installations, in accordance with G-3/5/7 priorities, by leveraging commodity buys and supporting signal organizations.

- Improving inside/outside plant cabling for installations (~ 4/5 installations per year based on resources).

In FY 16, network infrastructure modernization activities include:

- Continuing to increase throughput for ICANs via ACSs and EASs on CONUS installations (as resources allow).
- Continuing deployment of MPLS upgrades for any remaining CONUS, Europe, SWA and PACOM installations (as resources allow).
- Continuing improvement of inside/outside plant cabling for installations (~ 4/5 installations per year based on resources).

By the end of FY 16, installation infrastructure will be sufficiently modernized (i.e., switching throughput increased to 10 gigabits per second (Gbps), switching capacity for the installation wide area network increased to one gigabit and more switching capacity for every end-user building) to accommodate the increased capacity levels needed to utilize the additional applications and services offered by DoD-approved enterprise hosting facilities. 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 MC 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, incremental transport network capacity increases to meet growing demand, and flexibility to scale bandwidth throughput up or down based on network demands and available resources. Additionally, network infrastructure upgrades will ensure that the Army is positioned to adopt cloud-based enterprise business systems and UC.

Dual-path diversity and infrastructure modernization enable the removal of legacy switching equipment, reducing operating and sustainment costs. Building out the network transport infrastructure ensures that users can connect to requisite information at the point of need, which sets the conditions for cloud-based 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 institutional and tactical networks into one enterprise network, simplifying network management and reducing operations and maintenance (O&M), sustainment and modernization costs. It also ensures that all Army components can connect to Army enterprise services, such as UC, and access critical information.

In FY 15, integrate separate networks activities include:

- Continuing to integrate community of interest networks (e.g., Army Reserve, Corps of Engineers, Army Materiel Command and Medical Command networks).
    - Further detail will be provided in a follow-on CONOP or implementation plan, which will be developed in coordination with all network stakeholders.

- Setting the conditions for integration of deployable network transport solutions into a unified information transport delivery capability.
- Confirming and publishing tactics, techniques and procedures (TTPs) for the use of Wideband Global SATCOM (WGS) with WIN-T systems.

In FY 16 integrate separate networks activities include:

- Continuing the integration of separate institutional networks into the enterprise network.

By the end of FY 16, targeted installations will have one unified transport network, improving network efficiency and effectiveness. This will facilitate faster data transfer; establish data standards; standardize network operations and security tools; and improve the cybersecurity posture, ensuring seamless, secure operations from the enterprise to the tactical edge.

Improve Transport Capacity for Deployable Forces

The Army will continue to enhance tactical network capabilities through the deployment of Operational Capability Sets (OCSs). OCS fielding will be executed in accordance with HQDA Execute Order (EXORD) 244-12, and will incrementally enhance the throughput capacity and agility of the tactical network and extend it further down into tactical formations. In FY 15-16, planned capabilities include MC on-the-move and enhanced command and control/situational awareness (C2/SA) in dismounts down to company level and below.

In FY 15, improve transport capacity for deployable forces activities include:

- Continue fielding operational force units with increased capabilities in accordance with EXORD 244-12.
- Determining and implementing a plan for increasing connectivity between organizations operating on the lower tactical internet (TI) (Mid-Tier Networking Vehicular Radio (MNVR)).
- Continuing development of the Soldier Radio Waveform, Wideband Networking Waveform, Network-Centric Waveform and High-band Networking Waveform.
- Continuing planning for and integration of separate tactical network transport systems (e.g., Trojan Spirit, WIN-T, etc.).
- Determining the impact of the Installation Mobility Strategy on the deployed environment. Determining the way ahead for cellular/wireless communications support in the deployed environment.
- Finalizing garrison-based MC operations network support requirements.
- Standardizing IaaDS operations and supporting infrastructure requirements in order to improve deployable network readiness and support L/V/C/G training.
- Refining L/V/C/G training installation network support requirements.
- Providing secure, robust, jammer-resistant, short-range (<5km) capability between mobile platforms.

In FY 16, improve transport capacity for deployable forces activities include:

- Continuing to modernize tactical formations with WIN-T Increment 2, Rifleman Radio and Handheld, Manpack and Small through the fielding of OCSs (3-4 per year).
- Solidifying the way ahead for MNVR.
- Setting the conditions for implementation of the deployed environment cellular/wireless communications support strategy.
- Setting the conditions for garrison-based MC operations.
- Setting the conditions for L/V/C/G training from the desktop.
- Continuing to operationalize the Army's use and reliance on the WGS and the Mobile User Objective System (MUOS) satellite constellations, improving the efficiency of beyond line-of-sight communications.

Upgrades will ensure more reliable and versatile on-the-move tactical communications in support of on-the-move MC. They also will improve connectivity between the lower and upper TI, increasing a commander's abilities at all levels to collaborate with forces. Greater bandwidth will ensure that all communication forms (e.g., voice, video and data) are available to support MC 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.

Implementation of standardized IaaDS will improve force readiness for no-notice deployments and enhance the security of the network. The modernization of deployable units with OCS will increase tactical users' 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.

Standardized implementation of the IaaDS concept will enhance deployable unit readiness, ensuring that equipment has the latest cybersecurity and operational patches and that units can maximize L/V/C/G training opportunities. Continuing to modernize the Regional Hub Nodes (RHNs) as part of the evolution of WIN-T will ensure connectivity between the deployed tactical network and the enterprise cloud, greatly enhancing accessibility to requisite information at the point of need.

As OCS are fielded to units in accordance with G-3/5/7 priorities, key equipment will be re-allocated to units with older systems scheduled for sunset, thereby improving the modernization level of a greater portion of the force.

Data Center Consolidation and Standardization

The Army will continue to conform to DoD and Office of Management and Budget (OMB) directives to reduce physical IT infrastructure, standardize remaining Army-owned data centers and move as many applications and data centers as possible to DoD Enterprise Hosting Facilities (EHFs). Using the data center consolidation effort (i.e., Army Data Center Consolidation Plan [ADCCP]), the Army will align with the JIE construct for IPNs, ISNs and Special Purpose Processing Nodes (SPPNs). Through an incremental approach, the Army will utilize consolidated data centers to store and process data to support command, staff, mission areas, domains, Soldiers, civilians and contractors across the spectrum of operations.

In FY 15, data center consolidation and standardization activities include:

- Migrating services now in local data centers to DoD CDCs or approved EHFs.
- Closing 80 to 90 local data centers per year.
- Establishing the standard data center computing environment baseline and plan, which enables JIE concepts, supports ISN and IPN implementation, facilitates cloud capability, enforces Army and DoD guidelines, and reinforces joint force interoperability.
- Virtualizing and migrating applications and data to the appropriate hosting facilities (CDCs and DoD-approved EHFs, to include commercial cloud service providers).

In FY 16, data center consolidation and standardization activities include:

- Continuing the standardization and consolidation of data centers to the appropriate DoD-approved EHF, IPN or SPPN.
- Providing the enterprise concept of operations for the streamlined data center and application architecture of FY 18-21.
- Virtualizing and migrating applications and data to the appropriate hosting facilities (CDCs and approved EHFs).
- Implementing Command Post Computing Environment version 2.

By the end of FY 16, plans and processes will be validated for migration of applications, services and data. Data crossing installation boundaries will be migrated only to approved EHFs. Applications, services and data not crossing installation lines will be hosted in either IPNs or ISNs. Those applications with unique information needs will be identified and the conditions will be set to migrate to SPPNs, meeting their unique information support requirements.

This data center consolidation and standardization effort will enable centralized hosting of data and applications. It will provide robust data storage, on-demand computing for the generating force, elastic capacity, improved security and more efficient operations and maintenance (O&M). Virtualizing applications and implementing standardized computing environment specifications enables rapid and more efficient evolution of applications, minimizing costs and speeding dissemination of application enhancements through automated processes. The data center infrastructure will support processing of large amounts of data regardless of location to support knowledge discovery and Big Data analytics.

Data center consolidation and applications virtualization, combined with the transport infrastructure enhancements, enable the staging of information for global access as users move between mission environments. These modernization efforts will enable 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. Additionally, combining data centers will improve the cybersecurity posture by shrinking the data center and network footprint and consolidating information. Consolidated data centers will also provide more services to the global user community.

Rationalization and virtualization of applications will identify unnecessary overlap and help the Army to reduce the number of duplicative applications. In turn, that will increase efficiency, reduce lifecycle sustainment requirements and simplify IT capabilities.

End-User Device (EUD) Strategy

Due to greater interest and demand for mobile EUDs, the Army must develop a standardized strategy for EUD implementation and use.

In FY 15, EUD Strategy activities include:

- Developing an EUD Strategy to define requirements for a common EUD environment.
- Finalizing the EUD reference architecture.
- Beginning implementation of the decisions drawn from Commercial Off-the-Shelf IT Working Group (COTS-IT WG) recommendations.

In FY 16, 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 FY 16 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.

Army organizations will implement a standard suite of EUD systems, resulting in significant cost savings and the ability to collaborate across the force. Soldiers, civilians and contractors performing official Army business will have seamless access to the right information; identification of authoritative documents; automation of business processes; management of workflows, task tracking, personnel and organization; and sharing across functional communities and centers of excellence.

Divestiture

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

In FY 15, divestiture activities include:

- Implementing divestiture plans for unneeded legacy circuits, switches and servers resulting from fielding of MPLS, JRSS and ACS/EAS in CONUS, SWA and Europe.
- Developing and implementing divestiture plans for unneeded command local area networks (LANs), wide area networks (WANs) and transport infrastructure supporting dedicated video teleconference (VTC) networks as they migrate to the enterprise infrastructure.
- Developing and implementing divestiture plans for unneeded servers and storage pods as commands migrate and virtualize applications and data to the appropriate hosting facilities.
- Implementing divestiture of Single Channel Ground and Airborne Radio System (SINCGARS) Models A-D, to be completed no later than FY 18.

In FY 16, divestiture activities include:

- Implementing divestiture plans for unneeded circuits, legacy switches and servers resulting from fielding of MPLS, JRSS and ACS/EAS in PACOM, European Command (EUCOM) and Africa Command (AFRICOM).
- Continuing implementation of divestiture plans for unneeded command LANs, WANs and transport infrastructure supporting dedicated VTC networks as they migrate to the enterprise infrastructure.
- Continuing implementation of divestiture plans for unneeded servers and storage pods as commands migrate and virtualize applications and data to the appropriate hosting facilities.
- Implementing divestiture of the Enhanced Position Location Reporting System (EPLRS) through the fielding of the Joint Battle Command - Platform (JBC-P) system to Brigade Combat Teams, to be completed no later than FY 18.

By the end of FY 16, all unnecessary equipment is removed from the network and appropriately divested in CONUS and SWA. Divestiture activities are fully initiated for Army organizations in Europe, Pacific and Africa.

The Army and commands will be able to reallocate legacy network equipment lifecycle maintenance resources to higher-priority requirements; and facilitate/expedite the migration to the more efficient network, helping the Army to meet its operational and modernization objectives in a resource-constrained environment. Divestiture of unneeded legacy equipment will also improve the effectiveness of the network infrastructure 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 2016, the network infrastructure will be adequately modernized to provide the throughput and computing necessary to extend enterprise services and UC to tactical edge users. The robust approach to IaaDS will empower garrison-based MC operations, enable mobile device usage, distribute training while leveraging a fully networked ITE, and enable the readiness of units, particularly their 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 connectivity to critical information 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 expand, 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 EHFs to accommodate consolidation of applications and data storage, and to meet the DoD CIO's strategic mandates and the Army's vision by FY 18-21. The transport and computing infrastructure will be modernized to support cloud capabilities, which will enable better-informed decision making.

Appendix 2 – Enterprise Services Domain

Army enterprise services must be an easy-to-use, integrated suite of globally available, adaptable solutions that seamlessly supports the Army while working with UAPs. These services, both user-facing and enabling, provide the Army awareness of and access to information. These Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) solutions for the Army Enterprise take into consideration both institutional and operational components.

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

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

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

1. Common Core Enterprise Services
2. Position, Navigation and Timing

Enterprise Services will also play a supporting role in achieving any outcome led by the other AEN domains (Network Capacity and Network Operations and Security).

The ESD will produce two expected outcomes through activities in FY 15-16:

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

FY 15-16 Targeted Priorities

The ESD will focus on several high-priority initiatives that align to ESD capabilities/net-centric JCAs. This alignment is described below.

FY 15-16 ESD Activities	Joint Capability Area 6 Net-Centric							
	6.2 Enterprise Services							
	6.2.3 Core Enterprise Services							6.2.4 Position, Navigation and Timing
	6.2.3.1 User Access (Portal)	6.2.3.2 Collaboration	6.2.3.3 Content Discovery	6.2.3.4 Content Delivery	6.2.3.6 Enterprise Messaging	6.2.3.7 Directory Services	6.2.3.8 Enterprise Application Software	
1. Application Portfolio Rationalization, Standardization and Disposition							●	
2. Army Data Management Program	●	●	●	●	●	●	●	●
3. Army Enterprise Directory Services						●		
4. Army Enterprise Service Desk					●			
5. Army Mobility Services		●			●			
6. Defense Enterprise Email					●			
7. Enterprise Content Management and Collaboration Services	●	●						
8. Enterprise License Agreements							●	
9. Network Services Catalog	●	●	●	●	●	●	●	●
10. milSuite		●						
11. Storage as a Service	●	●	●	●	●	●	●	●
12. Unified Capabilities - Software UC - Hardware Voice - Hardware Video		●						

Application Portfolio Rationalization, Standardization and Disposition

Enterprise applications and systems are defined as those that have users that cross installation boundaries. DoD has mandated that all enterprise applications and systems be migrated to DoD-approved EHFs by the end of FY 18. Consolidation of data centers, operations centers and help desks will enable users and systems to have 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 (PfM), allows the Army to simplify and streamline information technology infrastructure while delivering mission-essential

capabilities. Application disposition enables an effective balance of cost, benefit, risk and dependencies. Application migration follows a standardization path toward the COE. As applications are standardized to operate in the COE, 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, these efforts will modernize the network, support the ITE, support mobility and enable realization of the IaaDS Concept of Operations (CONOPS). Through a systematic and iterative rationalization process that reviews the capability of an application, not just the mission it supports, the Army will begin to identify services to be redeployed as an enterprise service.

In FY 15, application portfolio rationalization, standardization and disposition will establish a foundation for migrating applications and services to approved data centers. This will reduce unnecessary redundancy across the network, enable the standardization of services and applications, and establish responsibilities to support the application lifecycle. At the end of FY 15, processes and plans to migrate enterprise applications and settle application disposition will be in place.

In FY 16, the Army will continue rationalization, standardization and disposition activities. Enterprise applications will migrate to approved data centers, eliminating unnecessary redundancy across the network. At the end of FY 16, 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

The Army CIO is responsible for and prescribes the Army's information management policy and guidance. The Army CIO oversees data management through the Army Data Management Program (ADMP). Army Data Strategy guidance and compliance requirements will enable 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 is focused on three 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.
- 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 goal of the Army Data Strategy in FY 15-16 will be to develop 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 facilitates 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. An additional goal is to develop a Unified Cloud Data (UCD)-CDF Integration and UCD Extension Strategy to provide Big Data interoperability and understandability among Big Data and non-Big Data systems.

In FY 15 and FY 16, the CIO/G-6 may 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.

- AIA
- AIA Compliance Tool and AIA Assessment Process
- ADMP Vol. 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

In FY 15 and FY 16, the 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 (ADC)/Army Data Board (ADB) direction. The Army CIO/G-6 will establish the Army position on the National Information Exchange Model (NIEM).

The goal of the Army Data Strategy is to enable the Army data stakeholder community to develop systems that are visible, accessible, understandable, trusted and interoperable (VAUTI); and to achieve compliance through updated, more specific strategic guidance, increased 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 provide, operate and maintain a centralized global directory of users and resources that can be accessed through a single interface. These services directly support JCA 6.2.3.7 (Directory Services) and include directory synchronization with other lower-level directories across the Army network.

In FY 15, Enterprise Directory Services will continue to identify ways to improve the Global Address List (GAL), which is utilized via the global directory. Enterprise Directory Services will update policy to ensure that individuals continuously maintain user attributes, as well as identify and prioritize attributes based on mission for both access and display to users.

In FY 16, Enterprise Directory Services 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 FY 16, Enterprise Directory Services 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 (POA&M) and implementation guidance. However, all directories must be able to utilize enterprise identity attributes by the end of FY 15, in accordance with USCYBERCOM TASKORD 14-0025.

With Enterprise Directory Services, the Army will have a single source for directory information that will provide users global access to directory and resource information on the Army network. The consistent user experience and interface offered by Enterprise Directory Services will reduce time spent employing multiple systems to search for and maintain personnel data, reducing overall costs to the Army. Enterprise Directory Services attributes will provide information for the GAL, through the IdAM initiative led by NSD (see Appendix 3).

Implementation of Army Enterprise Directory Service will reduce the need for local directory service solutions at posts, camps and stations, constituting an overall reduction in directory maintenance costs. Through synchronization with lower-level directories, Enterprise Directory Services 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 directory systems.

Army Enterprise Service Desk

The 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, email or through self-service at the AESD web portal. The AESD is supported by the ESMSaaS tool, which will be discussed in the Network Operations and Security Domain Appendix (see Appendix 3). 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. Theater service desks aligned to the five Regional Cyber Centers (RCCs) in CONUS, Europe, SWA, Pacific and Korea are considered part of a federation of Army service desks, designated as the AESD Federation. Until otherwise consolidated under a single responsible authority, these theater service desks are designated within AESD operations as follows: AESD-W (CONUS-based AESD supporting worldwide enterprise services and 7th Signal Command (Theater)/CONUS-based services), AESD-E (the 5th SC(T)/RCC Europe Service Desk), AESD-P (the 311th SC(T)/RCC Pacific Service Desk), AESD-S (the 335th SC(T)/RCC SWA Service Desk), and AESD-K (the 1st Signal Brigade/RCC Korea Service Desk). In addition, mature service desk capabilities supporting the Defense Health Agency (DHA), the USAR, the ARNG, the Military Entrance Processing Command and the Information Technology Agency participate in the AESD Federation as AESD-M, AESD-R, AESD-G, AESD-MP and AESD-I, respectively. AESD supports the enterprise messaging capability (JCA 6.2.3.6).

In CONUS, AESD currently provides Tier 1 support for command, control, communications, computers, and information management (C4IM) services for end users at 37 Network Enterprise Centers (NECs) and will continue to on-board CONUS NECs to use AESD in FY 15-16 in order to complete AESD CONUS deployment. AESD provides global support for enterprise services, such as Defense Enterprise Email (DEE), Enterprise Collaboration and Content Management Services (ECMCS) and Army Knowledge Online (AKO).

In FY 15, AESD will reach initial operating capability (IOC) for soft UC client, begin supporting the TRADOC Capability Manager Cyber (TCM Cyber) National Security System (NSS), and improve the quality of service. To accomplish the latter, AESD will standardize internal service desk processes and tools, utilizing a new incident ticket exchange (ESMSaaS, see Appendix 3), and increase user access to self-service features.

In FY 16, AESD will continue to increase support for the soft UC client. At the end of FY 16, AESD will provide Tier 0 (self-service) and Tier 1 support for IT globally for some C4IM services, as well as selected functional commands and applications.

A full-support service desk will help to provide users services at the appropriate level, and to resolve issues and problems quickly. By the end of FY 16, AESD will improve network availability to Army end users, synchronize institutional and operational components, and provide situational awareness through coordination of AESD, NECs/local operations, RCCs and the Army Cyber Operations Integration Center (ACOIC).

Army Mobility Services

Individual mobility is increasing across the Army. Army mobility services have become a key initiative supported by all three AEN domains. ESD's main focus for this initiative is to provide enterprise applications and services to the user via the Army Software Marketplace. It directly supports collaboration (JCA 6.2.3.2) and enterprise messaging (JCA 6.2.3.6) capabilities.

Army mobility services will provide service and application provisioning, as well as enterprise agreements for mobile data and cellular service. In addition, they will offer blanket purchase agreements (BPA) with various commercial carriers so that each command can select approved devices and the carrier plan that best meets mission needs. In FY 15, the Army will initiate BPAs in CONUS and make them available via the Computer Hardware Enterprise Software and Solutions (CHESS) website. Mobility services will also host a mobility application store where users will have access to a wide variety of applications for download and use.

In FY 16, Army mobility services will provide multiple BPAs with commercial carriers. It will also provision and manage applications and services to trusted mobile devices through a mobile application store (MAS) model and a managed mobile catalog. By the end of FY 16, 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 enable the Army to conduct mission and business functions globally.

The Army will achieve significant efficiencies by consolidating the use of various individual command mobile subscriber contracts into several enterprise BPAs for wireless devices, to include cost savings for implementation and maintenance of these devices. Additionally, with one central location to assist with acquisition of services and equipment, commands will have better, easier access to this capability.

Defense Enterprise Email (DEE)

DEE provides secure email, hosted by the Defense Information Systems Agency (DISA), for the Army and DoD. Recent efforts have focused on service implementation and shutting down disparate email servers. In FY 15-16, a technical feasibility analysis will be conducted to determine whether it is possible to provide users a single identity (CONUS or deployed), the perception of one mailbox, and hosting of enterprise services at the tactical edge.

In FY 15, DEE will be in sustainment and will be focused on adding features, such as journaling (i.e., the ability to retain copies of correspondence in accordance with Army CIO/G-6 policy). Support features such as journaling will only be available to select senior leaders to support routine Freedom of Information Act (FOIA) requests, congressional inquiries and statutory compliance investigations. The Army will begin planning for the implementation of a centralized, dynamic, tiered storage with global search. This will lay the foundation for the Army to meet OMB's directive to place electronic content under records management by FY 17. In FY 16, DEE will determine whether extending email to the tactical edge is feasible and reach a decision point. DEE will continue to serve as the primary email provider within the Army and across DoD. Should DEE be extended to the tactical edge and become completely operational, all standalone email services will be retired, providing the Army cost recovery opportunities. In FY 16, DEE will begin transition and integration activities with the storage environment to gain records management compliance and create savings.

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. ECMCS can only be accessed via Common Access Card (CAC). This initiative supports two ESD capabilities: user access portal (JCA 6.2.3.1) and collaboration (JCA 6.2.3.2).

In FY 15, a replacement service for AKO collaboration will be identified and AKO will divest itself of the AKO 1.0 For Official Use Only (FOUO) portal. The AKO sunset date is still being determined; a replacement will be identified first and organizations will be given time to transition users and content before AKO's sunset. ECMCS will continue the pilot program for organizations on the Defense Enterprise Portal Service (DEPS), with a total of up to 100,000 participants. ECMCS is available to onboard users to an enterprise-level service and start future divestiture planning for legacy systems in FY 16. The Army will increase the use of DEPS with the primary intent of further refining requirements for an integrated solution, to be fielded in FY 17-18. The Army expects to fully transition to the integrated solution in FY 18. The CIO/G-6 continues to analyze alternative solutions for Non-Secure Internet Protocol Router (NIPR) collaboration and will implement Army Secure Internet Protocol Router (SIPR) collaboration through the Network Enterprise Technology Command (NETCOM) at Rock Island Arsenal using SharePoint 2013.

Enterprise License Agreements

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 ELA initiative directly supports the Enterprise Application Software capability (JCA 6.2.3.8). The Army will continue to work closely with DoD partners to ensure alignment with JIE strategies and the Better Buying Power initiative.

By the end of FY 15, the Army will have 16 ELAs in place to eliminate redundant or unnecessary purchases.

By the end of FY 16, the Army will maintain the 16 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 user experience for software.

C4IM Services Catalog

The C4IM Services Catalog provides a customer view of C4IM Services that are managed and delivered by the C4IM/IT Service Provider over the network. Service-level IT entitlements depend on Army priorities and resources, and are adjusted annually. This is a crosscutting initiative that affects and impacts all capabilities under ESD.

In FY 15, the Army will publish C4IM Services Catalog version 4.0, which will include both customer-facing and enabling IT services. In FY 16, the Army will produce an online version of the catalog, which will include both customer-facing and enabling IT services. The catalog will utilize user attributes to enable a dynamic experience where users can view available services based on an individual’s role, responsibilities and authorities.

The C4IM Services Catalog serves as an important component of the Army Baseline Information Technology Services (ABITS) effort, which is designed to improve the quality, efficiency and timeliness of C4IM communications systems and systems support. The C4IM Services Catalog will enable essential IT services for mission command success and ensure flexibility to account for emerging requirements. A complete service catalog is essential for effective mission planning and Army business processes because it lets leaders know what to expect from the network.

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-based 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 this new knowledge. MilSuite 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.

By the end of FY 15, the DISA Defense Collaboration Service Portfolio Council will determine whether milSuite will be designated as a DoD enterprise service. If milSuite is granted this designation, planning responsibilities will be assumed by DISA.

By the end of FY 16, milSuite will either be funded by DoD and used as a DoD enterprise service or funded by the Army and provided as an Army enterprise service. If milSuite does not receive funding from either DoD or the Army, it will be targeted for sunset.

Storage as a Service (STaaS)

The Army is experiencing unsustainable growth in data storage and requires a cost-effective, capacity-on-demand solution that collapses data stores from installations across the Army into a consolidated storage environment, delivered as a service, for unclassified and classified data. Army organizations and end users require secure access to files, data sets and information from whatever device they are using. STaaS includes 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 COE. Access to STaaS and data will be controlled via attribute-based and role-based control methodologies through the DoD Enterprise Directory Service.

In FY 15, Army STaaS will create integrated project teams (IPTs) to gather requirements and get them validated by Army Commands, Army Service Component Commands and direct reporting units. The Army STaaS IPT will also create email records management and retention policies and business rules to maintain governance of and a compliance check on storage capacities.

In FY 16, the Army STaaS IPT 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 cost effective, scalable, secure and available on both the NIPRNet and the Secure Internet Protocol Router Network (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 directly support collaboration (JCA 6.2.3.2) by providing the Army access to media, such as voice, video and data. In FY 15-16, the Army will consolidate and standardize the way it communicates by focusing on three LOEs for this initiative:

- Providing an enterprise-wide UC client
- Transitioning to VoIP
- Transitioning to IP VTC

By focusing on these three efforts, the Army will reduce its reliance on traditional telecommunications and disparate implementations of UC. To achieve these goals, UC has established near-term objectives to ensure that these LOEs are completed and bring a much-needed enterprise solution.

In FY 15, the Army will divest AKO instant messaging and begin deploying a UC soft client to standardize and consolidate the way the Army communicates. While the soft client is being deployed, UC will also continue transitioning to VoIP telephones in CONUS; half of CONUS will have VoIP phones by the end of FY 15. UC will begin transitioning to IP VTC in select locations during FY 15, as well. By the end of FY 16, all users will operate on the soft client, all of CONUS will have VoIP phones and the majority of CONUS will utilize IP VTC. In FY 15, the UC team will work with the CP CE to integrate and extend UC as a Service (UCaaS) to the tactical network.

By transitioning to an enterprise-wide soft client, the network will be more resilient and offer better availability. The Army also will increase security and save money. The Army will not decommission legacy systems until the deployment of soft client, hardware voice upgrades (e.g., VoIP phones) and hardware video (e.g., GVS) 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
- Defense Connect Online (DCO)

Soft client, hardware voice and hardware video will improve the Army’snetwork defense posture by standardizing cyber solutions and minimizing connections to the network, which reduces the attack surface. Although all three areas will not be complete by FY 16, the Army will be in a strong position to enhance its ability to communicate in future years.

Summary

The ESD provides the user interface layer of the Army network. Enterprise services provide IT and information management (IM) services that are “visible” to the Army to enable and automate business processes, functions, solutions and applications. FY 15 and FY 16 activities will enable

Army collaboration with UAPs on any trusted device globally through a consistent user experience. They also will lay the groundwork for FY 17 award and implementation of a cloud-based collaboration solution; and development of a “one entry for all” user portal based on identified requirements and improved content discovery tools that utilize identified data sources.

Appendix 3 – Network Operations & Security Domain

The NSD is responsible for providing a secure, seamless and continuous network environment with protected critical data and information for the Army and UAPs. To meet this objective, the NSD will provide capabilities that improve the Army's ability to protect, detect and respond to threats to, restore and manage information and systems. The NSD will also pursue capabilities that support the management of underlying physical assets that provide end-user services for a continuous network environment. Activities also will include establishing and managing cybersecurity policies and standards, as well as preparing the workforce in the cybersecurity environment.

The overarching guidance for the NSD in the FY 15-16 timeframe is to meet the core mandated cybersecurity requirements while introducing new capabilities designed to mitigate emerging cybersecurity threats. The NSD has established the following objectives:

- Ensure networks and information are accessible, interoperable and protected against threats.
- Enable authorized users to effectively execute their mission by leveraging network capabilities.

There are nine initiatives in FY 15-16 aimed at supporting the aforementioned objectives. These efforts will enhance the network security posture and improve information sharing.

Defending the Network

The Army will conduct network defense measures that are directed, integrated and synchronized in accordance with the Unified Command Plan. Cyberspace Operations, enabled by intelligence support to cyber and the cryptologic enterprise, shall inform the operation, maintenance and security of the network, as well as shape acquisition efforts and the design of a defendable architecture. 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, including the insider threat and the advanced persistent threat (APT).

FY 15-16 Targeted Priorities

FY 15-16 NSD Activities	Joint Capability Area 6 Net-Centric						
	Net Management 6.3				Information Assurance 6.4		
	6.3.1 Optimized Network Functions and Resources	6.3.2 Deployable Scalable and Modular Networks	6.3.3 Spectrum Management	6.3.4 Cyber Management	6.4.1 Secure Information Exchange	6.4.2 Protect Data and Network	6.4.3 Respond to Attack/Event
1. Joint Regional Security Stacks						●	
2. Identity and Access Management					●		
3. Cryptographic Modernization Initiative					●		
4. Key Management Infrastructure					●		
5. Mobility					●		
6. Information Security Continuous Monitoring				●			
7. IT Asset Management	●						
8. Enterprise Service Management System	●						
9. Standardization of Network Operations across the Network	●						
10. Joint Management System				●			
11. Enhance Cyber Situational Awareness by Leveraging Big Data Analytics				●		●	●
12. Refining the Cyber Workforce	●						

Joint Regional Security Stacks

There are more than 1000 unclassified and classified external access points (known as top level architecture, or TLA stacks) that retain varying degrees of information and network management capabilities. Each TLA Stack requires a wide range of network defense tools and personnel. The Army, DISA and the U.S. Air Force are working to re-engineer and implement a JRSS approach. The joint architecture will consist of 15 security stack sites: 11 located in CONUS DISA facilities, two in SWA and two in Europe. This approach will simplify the network architecture, reduce the network attack surface and standardize network security.

FY 15 JRSS activities include:

- Successfully complete implementation at 11 sites in CONUS (seven DISA Defense Enterprise Computing Centers (DECCs), three Army sites and one Navy). CONUS physical install (NIPR JRSS) is scheduled to be completed by the end of FY 15.
- Implementation at two sites in SWA and two sites in Europe.

To execute the move from current TLA stacks to JRSS, the Army, Air Force and DISA will establish a Joint Migration Team (JMT) responsible for scheduling and coordinating transition activities. The transition guidance for JRSS will consist of both service-specific transition actions and joint transition actions. These actions will be carried out with existing resources in conjunction with DISA. All roles and responsibilities are outlined in the JMT CONOPS. The JMT lead will serve as a coordinating element between DISA and all associated Service Transition Teams. The end state is reached when all network traffic from installations is routed through JRSS (versus TLA stacks).

The consolidation of the current TLA stacks to unclassified and classified JRSS will improve network security by decreasing the cyber attack surface, standardizing firewall rule sets and clearly defining and centrally managing enclaves. JRSS is part of a Single Security Architecture (SSA) for CONUS and OCONUS installations, and will create a streamlined network with security based on logical communities of interest rather than location.

The transition of TLA stacks into JRSS significantly reduces equipment and personnel, resulting in a network that is more defensible and efficient. The transition will tremendously increase the network security posture and lower cost. JRSS augments the SSA portion of the JIE and provides the logical starting point for the network security stacks that will protect the enterprise network as part of the JIE and Intelligence Community Information Technology Enterprise (IC-ITE) SSA.

JRSS improves security for Army locations through:

- Enhanced network protection.
- Attack detection/malware management.
- Network data loss prevention.

JRSS provides a standard perimeter that empowers the cyber community to execute a high level of defense through:

- Improved situational awareness of focused and regional cyber events.
- Known, standard defense mechanisms for response actions.
- Reduced cost of current security functions by eliminating local base security systems with a focus on cyber labor at the regional level.
- Support of architecture upgrades to the network transport infrastructure, which is a precursor to JIE and IC-ITE alignment.

Identity and Access Management

The Army is establishing an enterprise IdAM framework, which will provide lifecycle management of 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 IdAM framework will support the full range of institutional and operational missions, and will align with DoD, JIE, IC-ITE and Federal Identity, Credential and Access Management (FICAM) requirements and regulations.

In FY 15-16, IdAM activities include:

- Implementation of 20 identified NIPRNet directories to fully leverage a single digital identity across the institutional force in accordance with the DoD Enterprise Directory Services mandate. This capability enables electronic policy enforcement for lifecycle management of digital identities and raises visibility of users and systems that access enterprise resources.
- Army application owners beginning to transition current systems from using Army single sign-on (SSO) to direct public key infrastructure (PKI) or a DoD-provided common authentication service.
- Enabling applications to utilize Common Access Card metadata for authentication and access control.
- Decoupling of applications from directories to eliminate organization and security boundaries.
- Creating logical access control functionality, which utilizes DoD authoritative data sources to reduce the Army's dependency on domain-based security enclaves and provide a data-centric approach to access control.

Through the enterprise IdAM framework, the Army will be able to centrally manage each user's digital identity, which is required to access network resources. In addition, IdAM will decrease the time Soldiers are disconnected from the network when transitioning between installations as they will no longer have to wait for an updated identity associated with their new location. IdAM will also improve access to required information and services across organizational and security boundaries.

This capability will enhance security, increase IT efficiencies and improve IT effectiveness across the Army by eliminating the imbedded stovepipe solutions across the Army and DoD IdAM framework. When fully implemented, enterprise IdAM framework will enable the Army to centrally manage user access to the point of need, which will ensure that the right individuals obtain the right information, at the right time, for the right reasons.

Cryptographic Modernization Initiative (CMI)

The CMI is the framework for modernizing the Army's imbedded and standalone communications security (COMSEC) capabilities that protect our National Security Systems (NSS) and National Security Information (NSI) and are reaching the end of their life cycle. This effort is aligned and coordinated with the DoD, National Security Agency (NSA), JIE, IC-ITE and COE requirements, security standards and regulations.

Once implemented, CMI will enable the Army to maintain and improve integrity, availability, authenticity, confidentiality and non-repudiation of information exchanged by the Army and UAPs. CMI will also ensure that national information is protected with modern NSS and that the Army's infrastructure is completely integrated, secure, accessible, interoperable and affordable.

In FY 15-16, cryptographic modernization activities include:

- Setting the encryption standards to secure the network by using cryptographic capabilities (imbedded and standalone) to modernize and replace legacy technology, waveforms and algorithms that are logistically unsupportable, financially unsustainable and technologically unmanageable.
- Modernizing nuclear command, control and communication (NC3) cryptographic capabilities by replacing legacy algorithms in accordance with Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6510.
- Providing a Key Management Infrastructure (KMI)-aware cryptographic device for the net-centric delivery of cryptographic keys, which will significantly reduce the logistical burden of manual key distribution while enhancing flexibility and interoperability through programmable technology.
- Providing modern cryptographic capability that will meet the Army requirement to enhance network capacity and improve network performance, while maintaining required functionality to secure data in transit.

The Army must continue to modernize and leverage new, innovative technological capabilities that provide security, robustness, interoperability and reliability. These capabilities will ensure the exchange of authentic voice, video and data between authorized individuals, groups and entities across the Army and mission operations. The Army will account for all legacy crypto devices and track the transition to a modernized capability. CMI will divest legacy imbedded and standalone components from Army inventory to reduce lifecycle and sustainment costs.

Key Management Infrastructure

Key management is a critical cybersecurity enabler of the Army network and the DoDIN. The Army is currently migrating from the legacy Electronic Key Management System (EKMS) to the KMI. The DoD KMI is synchronized with the Army's CMI to protect NSS and NSI. KMI will be a paradigm shift in the way keys are managed and distributed to the warfighter.

In FY 15-16, EKMS activities include:

- Transitioning 123 EKMS COMSEC accounts to KMI Management Clients (MCGs) in FY 15 and 186 in FY 16, in accordance with the Army fielding schedule.
- Approving a conditional material release in order for the Army to begin fielding Management Clients (MGCs). The MGC is a specific configuration/equipment for the KMI business process.
- Developing a transition plan that will be implemented following the successful completion of the limited user test (LUT).

KMI will enable net-centric capabilities (NIPR and SIPR) to deliver OTNK via the network rather than by manual means, which will minimize the number of Soldiers placed in harm's way. This modernized technology will put the Army in a position, both technologically and doctrinally, to provision "traditional" and "non-traditional" communications security products and services. It will also enable the Army to maintain integrity, authenticity, confidentiality and non-repudiation of information exchanged by the warfighter and UAPs by ensuring that data are not intercepted by our adversaries.

Mobility

The mobility initiative focuses on enabling Army users to perform work functions over a secure network at any time, from anywhere. Mobile EUDs will replace or augment the traditional desktop infrastructure; they will replicate or utilize many of the same technologies necessary to operate the current workplace.

In FY 15, Mobility will:

- Participate in the DoD Mobility Unclassified Capability Service.
- Enable government-furnished equipment (GFE) mobile communication devices to access classified knowledge centers and collaboration websites.
- Participate in the DoD Mobility Classified Capability Pilot (DMCC), with IOC achieved by end of FY 15 for DMCC (Secret and Top Secret).
- Provide an online unclassified mobile device manager.

In FY 16, Mobility activities include:

- 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 GFE mobile communication devices to access classified knowledge centers and collaboration websites through multiple classification levels.
- Providing classified Mobile Device Management online.

The Army will satisfy tactical and non-tactical 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 provides users the ability to perform work-related activities regardless of physical location. This will be accomplished over secure connections by an authenticated user at a classification level (public, unclassified and classified) appropriate to the mission and the data content. The Army will deliver mobile capabilities to both the generating force and the operating force. Generating force users will continue to employ GFE computing and mobile devices to ensure that operational assessments are conducted and evaluated. The validation and widespread adoption of mobility across the institutional Army 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 (CMDs) that meet affordability, technical and security requirements. DISA and NSA have published a plan outlining commercial mobile solutions for a classified capability.

Information Security Continuous Monitoring

Continuous monitoring is defined by DoD as the “ongoing observation, assessment, analysis and diagnosis of an organization’s cybersecurity posture, hygiene and operational readiness.” The Army is establishing the Information Security Continuous Monitoring (ISCM) Framework,

which will be achieved in a multi-year, iterative effort, leveraging current investments in enterprise and non-enterprise cybersecurity tools and capabilities.

The Army ISCM program will integrate and transition into the DoD-wide ISCM program. The Army ISCM program 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.

In FY 15-16, ISCM activities include:

- Optimizing Host-Based Security System implementation.
- Reporting asset information.
- Operationalizing Continuous Monitoring Risk Scoring (CMRS).
- Operationalizing the Assured Compliance Assessment Solution (ACAS).
- Reducing self-reporting.
- Correlating operational attributes.
- Initial correlation of vulnerability configuration data.
- Program of record reporting.
- Converging compliance scoring.

A robust ISCM will give the Army the ability to make near-real-time risk management and ongoing authorization decisions.

IT Asset Management

IT Asset Management (ITAM) comprises a strategy, process and repository to provide visibility of IT assets across the network. ITAM leverages standard network operations capabilities to automatically capture data regarding systems and applications on the network, down to individual printers and workstations, using extractors. ITAM provides the aggregation of specified data from NIPRNet- and SIPRNet-designated network management sensor grid data sources, which, when combined, provide an enterprise-wide asset view. The ITAM repository will aggregate and publish select network asset inventory information automatically collected by NIPRNet and SIPRNet instances of specific network operations. It serves as an authoritative source for consolidated asset data, making these data available to end users via web services.

In FY 15, ITAM activities include:

- Establishing role-based access controls, removing data duplications from ITAM sensors and normalizing data.
- Consolidating SIPR Host-Based Security System (HBSS) extractors.

- Updating sensors for HBSS and System Center Configuration Manager in the O&M phase.
- Updating sensors for Solar Winds to enable tactical visibility and enter development, testing and O&M phases.
- Developing and executing strategic communications documents.
- Conducting sensor revalidations of existing extractors.
- Determining Remedy Enterprise Manager (REM) validity to ITAM.
- Decommissioning IT Client Manager.
- Overseeing the maintenance of version 3.1 in O&M phases and version 3.2 research, development, testing and implementation phases.

In FY 16, ITAM activities include:

- Achieving an enterprise-wide asset view.
- Full sustainment mode (in FOC).

The overall goal and benefit of ITAM is to maximize IT asset visibility and data fidelity across the NIPRNet and SIPRNet. By establishing ITAM at the enterprise level, it will significantly improve the Army's ability to make IT investment decisions through the automatic and routine collection of information on network capabilities (e.g., systems, applications, software and devices). ITAM will also provide the Army knowledge of the IT security perimeter.

After ITAM reaches full sustainment mode, many disparate automated and manual asset management systems can and should be divested. This will enable the Army to pursue enterprise licenses, license tune-ups and coarse grain compliance status.

Enterprise Service Management System

ESMSaaS is a globally distributed network operations capability that provides a standard information technology service management (ITSM) platform for network operations staff and end users. ESMSaaS leverages industry best business practices and is received as a managed service (versus hardware/software hosted on site). Situational awareness dashboards are configured for the installation, RCC, ACOIC, functional commands and other designated Commands.

The Army's ultimate goal is to globally execute ESMSaaS across the network and to integrate ESMSaaS with tactical and Joint ITSM services/platforms. Migrating to an ESMSaaS-based delivery model will enable organizations 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.

In FY 15-16, ESMSaaS activities include:

- Awarding ESMSaaS contract and releasing CONUS-Southwest proof of concept prior to the FY 16 planning and development decision point for ESMSaaS global fielding.

- Spectrum integration development and accreditation.
- System center integration development and accreditation.
- HBSS integration development and accreditation.
- Arcsight Integration development and accreditation.
- Assured Compliance Assessment Solution (ACAS) integration development and accreditation and limited integration deployment.
- IT Client Manager integration, development and accreditation.
- Synchronizing requirements and capabilities with data center consolidation and standardization efforts.

ESMSaaS will simplify the business processes for network management and other support personnel. Training costs will be reduced over time as staff move from one organization to another on the network. A global system will improve situational awareness of hardware and software issues on the enterprise network. Licensing costs should significantly decrease, as other software is retired and decommissioned from networks.

Standardization of Network Operations across the Network

Network operations is a component of Signal support to warfighters and provides the business operations that establish, operate, manage, protect and defend the network. Network operations encompasses 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 and configuration control; detecting, reporting and resolving security issues; and facilitating the visibility and accessibility of information across the network.

In FY 15, network operations activities include:

- Publishing the CONOPs that lays out how the Army will operate and defend the network.
- Releasing prescribed information exchange specifications and network operations metadata.
- Implementing an initial WIN-T network operations standardized fielding.
- Supporting initial CP CE version 2.
- Improving WIN-T cyber alert monitoring.
- Instituting changes to improve service management and application monitoring.

In FY 16, network operations activities include:

- Continuing standardization of the network operations toolset across the network.
- Integrating emerging capabilities in network monitoring and continuous monitoring to increase situational awareness and improve the overall health of the network.

The aforementioned network operations activities in the FY 15-16 timeframe will help shape the development of emerging capabilities. The CONOPs, network operations information exchange

specifications and network operations metadata establish the framework to improve interoperability and information sharing. The network operations convergence effort continues to be a major priority. The Army will identify the tactical network operations toolset. By reducing the number of network operations tools, applications and separate networks across the Army, the Army will assure seamless network operations functions from the enterprise to the tactical edge. The overall goal, and benefit to the Army, is to standardize, unify and merge operations and security of tactical- and enterprise-level networks. NSD will continue to focus on the convergence of enterprise and tactical network operations tools, to include applications, in order to reduce redundancy and achieve efficiency and cost savings.

Joint Management System

The Joint Management System (JMS) encompasses managing the entire spectrum of network operations activities within the context of the DISA Enterprise Service Management Framework (DESMF). JMS will be used for managing, operating and defending the network. It consists of systems, tools and information management capabilities required for DoD Information Network operations and defensive cyberspace operations internal defensive measures (DCO-IDM). These capabilities permit security contexts and policy management of JRSS elements by the Services and DISA. The Services are responsible for managing security contexts and policies under their operational command and DISA is responsible for operations and maintenance of the JRSS itself.

In FY 15-16 JMS activities by version include:

- JMS 1.0: The U.S. Army TLA and the U.S. Air Force Gateways are removed and U.S. Marine Corps and U.S. Navy boundaries are peered, with traffic passing through JRSS in FY 16. Activities consist of the following:
    - Continue Army migration.
    - Begin Air Force migration.
    - Robust, scalable management capability.
    - Two activated CONUS JMS sites.
    - One activated Europe JMS site.
    - Two activated Southwest Asia JMS sites.
    - Two activated Pacific JMS sites.
- JMS 1.5: Represents minimum acceptable capability and capacity required to meet these objectives and the planning assumptions; as the demand for capacity grows, will require the programming of funds to reach the JRSS baseline, as originally defined, in order to address the capacity risks inherent in this plan. The reduced cost JRSS 1.5 capability suite consists of the JRSS capabilities currently being deployed, plus the addition of full packet capture. JMS 1.5 development and fielding will comprise the following:
    - Managing full suite of JRSs capabilities and full JRSS deployment.
    - Updating management capability.
    - DISA providing JMS operation and maintenance.

The JMS will provide a remote access capability, enabling DoDIN operations and DCO-IDM analysts to execute their missions without being co-located with the JMS. All users will be able to monitor JMS information but will only be provided the capability to change configurations in concert with the requirements of their positions and organizations.

Enhance Cyber Situational Awareness by Leveraging Big Data Analytics

Big Data 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 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 a range of threats and our people, training, materiel, finances and operations, we have an opportunity to enable better and quicker decisions and be more focused in our operations. Data as used in Big Data are defined as the 3xVs: **Volume** (amount of data), **Velocity** (speed of data) and **Variety** (types of data, structured and unstructured). Advanced analytics are defined by three attributes: **Descriptive** (aka business intelligence, which describes what you know and where you are); **Predictive** (describing where you think you are headed) and **Prescriptive** (described as the best path to the organization's goals and objectives).

In FY 15-16, enhance cyber situational awareness by leveraging Big Data analytics activities include:

- Developing the Army's Big Data Strategy.
- Conducting Big Data pilots.

Refining the Cyber 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. It is comprised 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.

In FY 15-16, refining cyber workforce activities include:

- Identifying, shaping and tracking the civilian cyberspace workforce.
- Identifying work roles.
- Aligning civilian workforce roles with the military Career Field 17 structure.

Summary

The NSD's FY 15-16 targeted priorities are intended to satisfy the security attributes of confidentiality, integrity and authentication of data, information systems and networks. NSD initiatives will support both the operational and institutional environments and set the stage for future cybersecurity enhancements. The resulting strategic effects of improved security,

information sharing and data protection lay the framework for capability gap mitigation and meeting the projected end states in the FY 17-21 timeframe.

Appendix 4 – Capability Taxonomy

Network Capacity Domain

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Enterprise Services Domain

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

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

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

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

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

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

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

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

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

Network Operations and Security Domain

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix 5 – Acronyms

Acronym	Definition
ACAS	Assured Compliance Assessment Solution
ACS	Area Core Switches
ADMP	Army Data Management Program
AEN	Army Enterprise Network
AESD	Army Enterprise Service Desk
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)
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 System
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
DCO	Defense Connect Online
DEE	Defense Enterprise Email
DEPS	Defense Enterprise Portal Service
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
ECMCS	Enterprise Content Management and Collaboration Services
EDS	Edge Distribution Switches
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

Acronym	Definition
EUD	End-User Device
EXORD	Execution Order
FOC	Full Operating Capability
FRAGO	Fragmentary Order
FY	Fiscal Year
GAL	Global Address List
Gbps	Gigabit
GFE	Government-Furnished Equipment
GOSC	General Officer Steering Committee
GVS	Global Video Service
HBSS	Host-Based Security System
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
ITAM	IT Asset Management
ITSM	Information Technology Service Management
JIE	Joint Information Environment
JMT	Joint Migration Team
JRSS	Joint Regional Security Stack
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
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

Acronym	Definition
NOSC	Network Operations and Security Center
NSA	National Security Agency
NSD	Network Operations & Security Domain
NSS	National Security System
O&M	Operations & Maintenance
OCONUS	Outside the Continental United States
OCS	Operational Capability Set
OMB	Office of Management and Budget
OTM	On-the-Move
OTNK	Over-the-Network Keying
PACOM	Pacific Command
RCC	Regional Cyber Center
SIPR	Secure Internet Protocol Router
SIPRNet	Secure Internet Protocol Router Network
SPPN	Special Purpose Processing Node
STaaS	Storage as a Service
SWA	Southwest Asia
TLA	Top Level Architecture
TRADOC	Training and Doctrine Command
UAP	Unified Action Partner
UC	Unified Capabilities
USAR	United States Army Reserve
VoIP	Voice over Internet Protocol
VTC	Video Teleconference
WAN	Wide Area Network
WGS	Wideband Global SATCOM
WIN-T	Warfighter Integrated Network – Tactical
WMA	Warfighting Mission Area