



U.S. Army Network Operations Reference Architecture

(Aligned to the DOD Enterprise)

Version 1.0 6 March 2014

Executive Summary

The Army relies on the current Network to support warfighting and business processes in changing threat, technology and mission environments. To this end, the Army faces significant challenges in achieving its vision in the Army Network Strategy and LandWarNet (LWN) 2020 and Beyond Enterprise Architecture. The strategy highlights the need to enable the Army to fight and train as well as deploy forces on little notice anytime and anywhere to prevail in unified operations in a Joint environment. To accomplish this, the Network has to be a global, single, secure, standards-based and adaptable environment that ensures access at the point of need and enables global collaboration. The Network spans all Army operations, from the administrative operations in garrison to the most forward-deployed soldier at the tactical edge.

The objectives of this Army Network Operations (NetOps) Reference Architecture (RA) are to guide the update and standardization of Network Operations to realize full capabilities envisioned in LWN 2020 and Beyond Enterprise Architecture. NetOps is envisioned as a capability with increased flexibility, simplified processes and improved network defenses. To guide NetOps development, this document provides a framework by identifying principles and rules needed to ensure focused and consistent development and refinement of Army NetOps. The principles and rules are consistent with the desired outcomes of the Department of Defense (DOD) Information Technology (IT) Enterprise Strategy and Roadmap and the Secretary of the Army's Information Technology Management Reform (ITMR) Implementation Plan to publish IT architecture guidance with enterprise level principles and rules. Also, this document provides a technical foundation for the Army NetOps (Operational and System) Architecture.

The NetOps RA is a key part of Army Chief Information Officer (CIO)/G-6 Rules-Based Architecture and ensures alignment with DOD Information Enterprise Architecture (DIEA), industry best practices, and the Joint Information Environment (JIE). The intent of this RA is to ensure integration with JIE architecture and ensure Army implementations are postured to leverage JIE capabilities. LWN NetOps Architecture (LNA) 2.0, 2010, is one of the integration implementations that enable focused application to accomplish the Army's enterprise level NetOps mission.

This document supports the implementation of an enterprise portfolio management process that integrates the Warfighter Mission Area (WMA), the Business Mission Area (BMA) and the Enterprise Information Environment Mission Area (EIEMA) at the Army Enterprise level in the Network Mission Area (NMA) portfolio.

Gary W. Blohm
Director, Army Enterprise Architecture

Executive Summary	i
1 Introduction	1
1.1 Background	1
1.2 Purpose and Scope	1
1.3 Alignment with DOD IEA and Related Strategies	3
1.4 Document Structure and Configuration Management	3
1.5 Intended Audience	4
1.6 Key Definitions	4
2 Current and Objective States	6
2.1 Current State	6
2.2 Objective State	7
2.3 Limitations and Assumptions	8
3 Army NetOps Guiding Principles and Rules	10
3.1 Principles and Rules Illustration	10
3.2 Enterprise Management: Network Connect and Operate Services	11
3.3. Net Assurance: Access and Defend Services	19
3.4. Content Management: Share Services	21
3.5 Data and Service Framework	25
4 Technical Positions and Implementation Patterns	28
4.1 Technical Positions	28
4.2 Implementation Patterns	28
5 Summary.....	29
Appendix – A: References	30
Appendix – B: Acronyms	35
Appendix – C: NetOps Standards List (StdV-1)	38
Appendix – D: U.S. Army Telecommunications Management Network Model.....	39
Annex – A: U.S. Army Network Operations Services Integrated Dictionary (AV-2)	A-1
Introduction	A-4
Purpose	A-4
Background	A-4

Common Terms used in the Army NetOps Architecture:	A-7
Summary Information	A-8
Section 1: NetOps IT Service Descriptions	A-9
Section 2: NetOps Service Alignments	A-35
Glossary of Acronyms	A-63
References to other architectures and frameworks	A-63

TABLE OF TABLES

Table 1 – Principle Rule Illustration.....	10
Table 2 – Distributed NetOps Command and Control	11
Table 3 – Resilience and Continuity of Operations	12
Table 4 – Data Diversity and Duplication	13
Table 5 – Integrated Configuration Management (CM) and Policy Based Network Management (PBNM) Capabilities.....	14
Table 6 – Integrated IT Asset Management.....	15
Table 7 – NM Interfaces to Joint Mission Partner Environment (MPE)	16
Table 8 – NM Interfaces to Mobile Partners	17
Table 9 – Enterprise Service Desk (ESD) Objectives	18
Table 10 – Defend, Understand, Secure	19
Table 11 – Information Assurance and Cryptography Management	20
Table 12 – Integrated Systems Management	21
Table 13 – Information Dissemination Management	22
Table 14 – Information Exchange Access.....	23
Table 15 – Collaboration Share Services.....	24
Table 16 – Presentation of Data	25
Table 17 – Services Structure	26
Table 18 – Service Framework	27
Table A-1 – NetOps Service Descriptions	A-9
Table A-2 – NetOps Services Alignments.....	A-35
Table A-3 - Content Management Share Services Alignments.....	A-36
Table A-4 - Directory Management Services Alignments.....	A-37
Table A-5 - Content Management Services Alignments.....	A-37
Table A-6 - Content Collection Service Alignments.....	A-38
Table A-7 - Enterprise Management Connect & Operate Services Alignments	A-39
Table A-8 - Connect Services Alignments	A-40
Table A-9 - Satellite Communication Management Services Alignments.....	A-41
Table A-10 - Wired Networking Services Alignments	A-42
Table A-11 - Wireless Communication Services Alignments	A-43
Table A-12 - Operate Services Alignments	A-44
Table A-13 - Spectrum Management Operations Services Alignments	A-45
Table A-14 - Change Management Services Alignments.....	A-46

Table A-15 - Configuration Management Services Alignments	A-47
Table A-16 - Incident Response Services Alignments	A-48
Table A-17 - Performance Management Services Alignments	A-49
Table A-18 - Computing Infrastructure Management Services Alignments	A-50
Table A-19 - NetOps Situation Awareness Services Alignment	A-51
Table A-20 - Audit Services Alignments	A-52
Table A-21 - Information Resource Planning Services Alignments	A-53
Table A-22 - Net Assurance Access & Defend Services Alignments	A-54
Table A-23 - Access Services Alignments	A-55
Table A-24 - Access Control Services Alignments	A-56
Table A-25 - Identity and Authentication Services Alignments	A-57
Table A-26 - Defend Services Alignments	A-58
Table A-27 - Security Metadata Management Services Alignments	A-59
Table A-28 - Cryptographic Management Services Alignments	A-60
Table A-29 - Secure Transfer Services Alignments	A-61
Table A-30 - Information Assurance Management Services Alignments	A-62

TABLE OF FIGURES

Figure 1: The Current Network	6
Figure 2: The Objective Network	7
Figure 3: Army NetOps Services (SvcV-1)	28
Figure 4: Army Telecommunications Management Network Model	39
Figure A-1: NetOps Services Organization	A-6

1 Introduction

1.1 Background

Historically, the Army has developed and deployed a variety of Network Operation capabilities for diverse warfighting and business communities. Often, the differences between the capabilities are due in part to a lack of commonality in the selection or implementation of standards or functional descriptions. Within the LWN (as well as the wider DOD Information Networks [DODIN]), the dissimilar capabilities are also manifested in the number of tools, technologies and processes that are deployed across these networks. In lieu of appropriate standards and controls, this practice will continue to degrade our ability to conduct the fight even as new cyber security risks arise and increase.

DOD guidance is to move toward a DOD enterprise-level consolidation of IT capabilities with multiple providers of services and data. The DOD Joint Information Environment (JIE) is envisioned to be a secure environment comprised of shared IT enterprise services and data and single security architecture to achieve full spectrum superiority, improved mission effectiveness, increased security and greater IT efficiencies. JIE will use enforceable standards, specifications, and common tactics, techniques and procedures (TTPs).

The LWN 2020 and Beyond Enterprise Architecture defines the baseline guidance and structure upon which IT will be developed, deployed and operate. Using this guidance, Army CIO/G-6 uses a Rules-Based Architecture (RBA) approach as a primary method to inform, guide and constrain design and development of required solutions and services. An implementation of RBA is the RA. RAs are being developed for specific functional areas needing baseline rules, principles and desired outcomes. This NetOps RA is one of those specific functional areas and is aligned with currently published RAs at the Army and DOD level.

1.2 Purpose and Scope

The purpose of this NetOps RA is to provide a framework for improving the Army's NetOps functions in support of Army Network Strategy and LWN 2020 and Beyond Enterprise Architecture. The contents of this document serve three general functions:

- Inform internal and external stakeholders of the CIO/G6's intent to improve Army NetOps
- Guide the delivery of NetOps services and capabilities
- Constrain the development and optimization of NetOps to enable full operational capabilities.

The increasing need for Defense to seamlessly coordinate its activities in the physical and cyberspace worlds within Joint and multi-national coalition environments requires a

new emphasis on standardization of services and capabilities. This must be achieved through clearly articulated principles, rules and standards that will form a framework for a range of activities, functions and tasks involving further NetOps development and optimization with due consideration to Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF).

The operation of our networks must be considered from a user perspective and architected from an enterprise perspective to enable end-to-end service-oriented network operations ensuring the continued success of our current and future operations. The Army's warfighting capabilities will rely on a federation of advanced technology, and NetOps must effectively integrate with and use technology to support the mission. This RA is intended to establish architectural principles and rules the Army must adhere to now to improve network operations, and ensure the Army is postured to leverage emerging JIE and industry capabilities and efficiencies.

The scope of this document covers the three key NetOps functions described below:

- The set of NetOps Enterprise Management functions that encompass the Global Information Grid (GIG) information technology services management that consist of the many elements and processes needed to communicate include enterprise services management, systems management, network management, satellite communications management, and electromagnetic spectrum management.
- The set of NetOps Content Management functions that ensure information is available on the GIG by enabling users to safeguard, compile, catalog, discover, cache, distribute, retrieve and share data in a collaborative environment.
- The set of NetOps Net Assurance functions that include the operational responsibilities for information assurance, computer network defense (CND) to include computer network defense response actions and critical infrastructure protection.

The above functions guide the installation, management, and protection of communications networks/systems/services necessary to directly support both generating and operating forces. NetOps provides the commander/users, at all levels, with end-to-end network and information system visibility, protection and priority of timely information delivery. It does not define NetOps in the context of Offensive Cyber Operations (OCO) except where these tasks fall within the purview of NetOps functional tasks described in the Annex. The three key functions will be derived and developed, and associated principles and rules will be established for their implementation and governance. The next version of the Network Operations Reference Architecture will take into account tactical equities that will include Unit Task Reorganization (UTR), dynamic reconfiguration, and network common operating picture.

The Common Operating Environment (COE) is an approved set of computing technologies and standards that enable secure and interoperable applications to be

developed rapidly. It also specifies principles as well as describes computing environment architecture and services. The COE principles, architecture, and services are not addressed in this NetOps RA, but the RA works in concert with COE.

1.3 Alignment with DOD IEA and Related Strategies

This document aligns with the DOD Information Enterprise Architecture (DIEA) v2.0, which is the authoritative source for DOD architecture governance and the Army's ITMR that establishes enterprise oversight and governance for Army's IT resources. It also acknowledges the collective strategic guidance of many stakeholders, particularly guidance and policy defined by the following:

- DOD IT Consolidation Strategy and Roadmap
- DOD Interoperability standards and GTG-P
- DOD NetOps Strategic Vision
- JIE Operations Concept of Operations (CONOPS)
- TRADOC Pamphlet 525-5-600, LWN 2015 CONOPS
- Army LandWarNet 2020 and Beyond Enterprise Architecture.

1.4 Document Structure and Configuration Management

Section 1 is self explanatory.

Section 2 discusses current and objective states of the Network as it pertains to Army NetOps. It also includes limitations of RA document coverage as well as assumptions regarding the transition to the objective network.

Section 3 addresses the guiding principles, rules, capability gaps, desired outcomes and risks under each of the three key NetOps Services (Enterprise Management: Network Connect and Operate Services, Net Assurance: Access and Defend Services and Content Management: Share Services) as well as under Data and Services Framework.

Section 4 addresses NetOps technical positions and patterns in the form of a Services Interface Description (hierarchy tree) and Standards Profile. This represents a key part of NetOps technical architecture.

The Appendices include supporting information (References, Acronyms, Standards List and Army Telecommunications Management Network Model).

The Annex includes a standalone document, the AV-2, Army NetOps Services Integrated Dictionary.

Upon publication, this RA will be placed under configuration control of the Army CIO/G-6 Enterprise Information Environment Mission Area (EIEMA) Architecture Configuration

Control Team (ACCT). The ACCT is responsible for review, approval, and processing of change requests for EIEMA technical architecture standards and guidance documents. The ACCT is chaired by the Civilian Director of the Army Architecture Integration Center with senior direction from the Army CIO Enterprise Guidance Board. RAs are made available to organizations through Training and Doctrine Command's (TRADOC) Army Capability Architecture Development and Integration Environment (ArCADIE) at the <https://cadie.army.mil> site.

1.5 Intended Audience

The intended audience for this document includes IT investment decision makers, WMA, BMA and NMA architects, program managers, solution architecture developers, Army NetOps service providers and NetOps mission support. A key objective is for the Army NetOps community to seamlessly coordinate network operation activities in cyberspace with joint and multinational coalitions. This document should be referenced when developing operational and solution architectures to ensure alignment with DOD guidance/architectures/strategies and joint initiatives. IT investment review boards and portfolio review groups use it to validate procurement solutions and to support the Network Mission Area.

1.6 Key Definitions

The three NetOps core functions identified in Army NetOps include Enterprise Management, Net Assurance and Content Management. To extend definitions in context with the "Services" term used in IT architecture development, these "function" terms will be referred to as "Services." The definitions for these services are defined below, and they are aligned with the function definition with no conflict.

Enterprise Management: Network Connect and Operate Services - These services provide the functionality required to support near-real-time operational management of the LWN to include situational awareness, computing infrastructure management, change and configuration control and end user support (incident and problem resolution.) It also includes services (acquires, improves, maintains) that provide the ability for any user or service to reach another entity or to identify and use any other service.

Net Assurance: Access and Defend Services - These include the set of services that provide the ability and means to communicate (to both human and machine users) with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions (derived from Committee on National Security Systems Instruction [CNSSI] 4009). It also provides the functionality to ensure data and services are secure and trusted across the DOD.

Content Management: Share Services - These include the set of services that provide the functionality required to enable information and information assets to be

used within and across mission areas per Defense Information Enterprise Architecture (DIEA). Functions include monitoring, managing, and facilitating the visibility and accessibility of information within and across the LWN. It includes information management planning services that support budget planning, manipulating and controlling of information throughout its life-cycle through the creation, modification and monitoring of service level agreements, organizational level agreements, Information Dissemination Management (IDM) and other contract-related documents.

2 Current and Objective States

2.1 Current State

The Army universally leverages the Network (See Figure 1) to improve warfighting and business processes as well as reduce operational and maintenance costs. However, the Army faces significant challenges in achieving its vision. As an example, the current state involves deployed tactical forces relying on limited reach back capabilities to access and use services and stored data, and this also lends itself to security vulnerabilities that need to be mitigated. We must dramatically improve our ability to protect our network, information and data against increasingly sophisticated cyber-attacks. This will require standardized top level security architecture and the integration of all Army networks into a global, single, secure, standards-based Army Network.

The Network Today

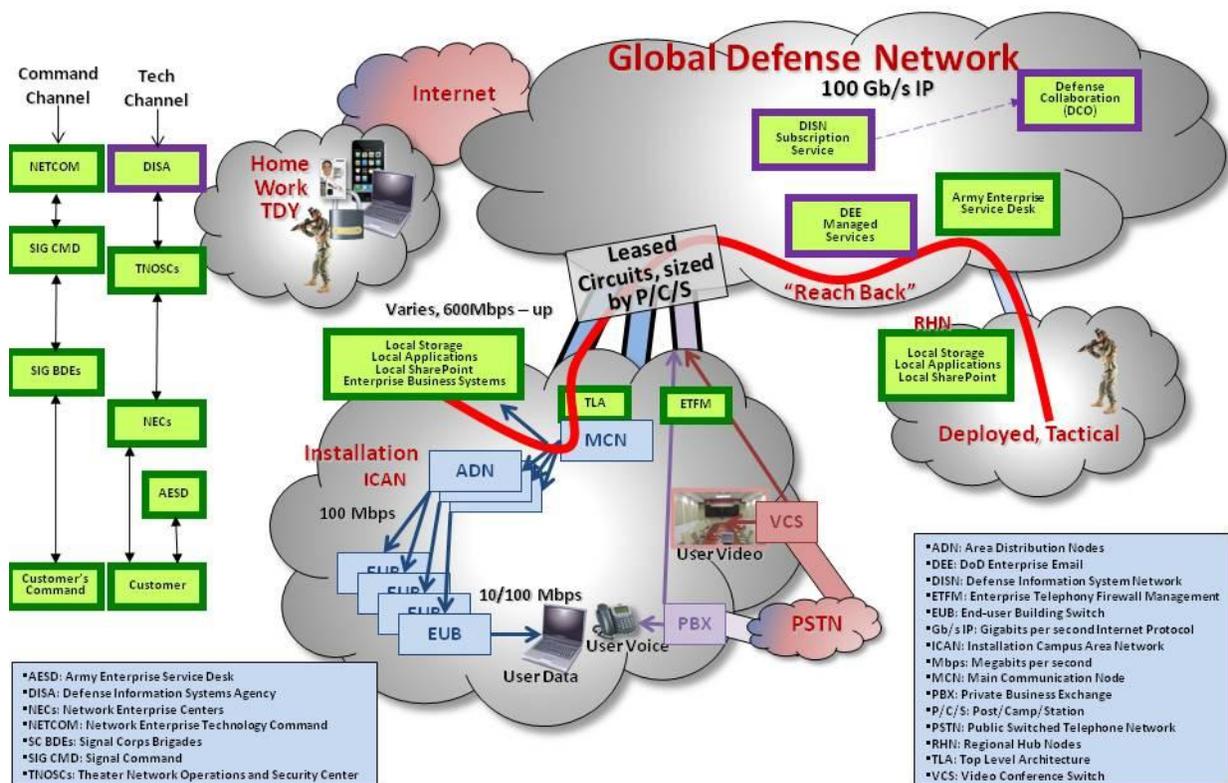


Figure 1: The Current Network

- Proactive defense of networks and data.
- Support of cross domain security.
- More effective management of network performance and dynamic allocation of enterprise resources.
- Increased capability for physical and virtual processing of information and data across the enterprise.
- Greater access control for all users and devices.
- Common policies, standards, and management processes.
- Effective development and use of architectures.

2.3 Limitations and Assumptions

2.3.1 Limitations

- NetOps RA basically establishes a framework for developing NetOps in support of Army Network Strategy and LWN 2020 and Beyond Enterprise Architecture. Updates to cover specific issues and areas shall be incorporated in future publications as required.
- NetOps RA is focused on enterprise level rules and Technical Architecture (e.g., Services Context Description [SvcV-1], Standards Profile [StdV-1]) and not on Operational Architecture (e.g., High-Level Operational Concept Graphic [OV-1], Operational Activity Model [OV-5b]) or Systems Architecture (e.g., Systems Interface Description [SV-1], Systems Resource Flow Description [SV-2]).
- NetOps RA does not address Solution Architecture¹ or resourcing implementation. This RA is intended to inform, guide and constrain implementation efforts; therefore, it should be used as a guide for developing Solutions Architecture.

¹ Solution Architecture - An architecture that describes a solution at the physical level of abstraction; solution is a set of DOTMLPF changes required to provide a mission or business capability; solution as a DOTMLPF-level response to achieving a capability. Ref: Army Architecture Integration Center (AAIC) Integrated Dictionary, AV-2.

2.3.2 Assumptions

- The Network is not owned and controlled by one organization – decisions must be made in the context of shared need and shared responsibilities. Clearly articulated roles must be defined between NetOps command elements whether Joint, Army, institutional or operational including Coalition Forces.
- NetOps processes will provide commonality of industry best practice processes that are integrated horizontally and vertically, and it will enable operators with experience that is consistent across the Network.
- Wherever possible, capabilities are to be universal throughout the enterprise to benefit from efficiencies and economies of scale.
- The Network Mission Area (NMA) portfolio managers will work closely with Warfighter and Business Mission Areas (BMAs) to synchronize IT requirements guidance for the Program Executive Groups to assist in modernizing the Network, and realize significant efficiencies through effective and affordable solutions.
- Human capital capabilities (soldiers, civilians, contractors) are sufficiently agile to enable a single, secure, standards based end-state.
- NetOps RA should enable and support accountability.
- Solution Architectures will move toward a simplified and more secure network.

3 Army NetOps Guiding Principles and Rules

3.1 Principles and Rules Illustration

Table 1 illustrates how these rules will be presented within this document. The table is organized as follows:

- An enterprise guiding principle (derived from the DIEA) is associated with a required DIEA/JIE capability.
- Associated with each guiding principle is a reference to applicable Joint Capabilities Areas (JCA) to show how rules support the JCA.
- Gaps within the current network (desired capabilities Army wishes to achieve) are then identified.
- From the identified gaps, a set of rules are listed that will produce the desired outcomes.
- If implementation of a rule warrants additional consideration (or if a known risk exists), this information will be provided to facilitate future risk mitigation and serve as documentation of the current challenges associated with the Army’s NetOps architecture.

Guiding Principle	
<i>Guiding Principle that is derived From the Defense Information Enterprise Architecture (DIEA)</i>	
Capability Gap(s)	
<i>Identified Gaps in a specific capability area.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>Architectural rules (constraints /guidance) that need to be adhered to in order to satisfy the capability gap & standards to follow.</i>	<i>Specific outcomes that will be achieved with successful implementation of the rules.</i>
Considerations and Known Risk(s) (Continued)	
<i>Identified considerations, risk, and challenges associated with implementing the identified rules.</i>	

Table 1 – Principle Rule Illustration

3.2 Enterprise Management: Network Connect and Operate Services

The principles applicable to this Service category are shown in Tables 2 through 9.

<i>Principle: Army Network Management (NM) capabilities shall be capable of distributed network control and facilitated net-centric sharing of network configuration, status, security, performance, utilization, and mission impact data with authorized users. It supports Joint Capability Area (JCA) 6.0 Net Centric</i>	
Capability Gap	
<i>Network Management and/or Enterprise Service Management capabilities are not fully interoperable and integrated vertically and horizontally across the force.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>1) Ensure vertical and horizontal integration of applicable information exchanges pertaining to network management and enterprise service management capabilities.</i>	<i>Army network management and enterprise service management will have a common operational picture of the network and improved network situational awareness for the commanders.</i>
<i>2) Ensure common and standardized training, use of common processes providing required functionality, and integrated management procedures that support operational continuity, responsiveness and Quality of Service (QoS) requirements.</i>	<i>Personnel with transferable skills that can operate within different network environments with minimal additional training, use of common processes will ensure quicker usage and lower maintenance costs, and integrated procedures that improve continuity, responsiveness and QoS.</i>
<i>3) Utilize standards- based interfaces between management systems; service oriented information exchange of element to network to service to business management layers (See Appendix D, Figure 4) will follow commercial best practices.</i>	<i>Network management and enterprise service management will operate with greater efficiency and interoperability ensuring improved mission effectiveness in operating, maintaining and protecting the network while meeting information sharing requirements.</i>
<i>4) Follow applicable standards and practices in Appendix C (Standards List, StdV-1), IT Service Management (ITSM) Forum best practices and applicable ISO/IEC 20000 standards.</i>	
Considerations and Known Risk(s)	
<i>ASA(ALT) is responsible for the consolidation and reduction of NetOps tools supported by principal Army/Joint/DOD stakeholders.</i>	

Table 2 – Distributed NetOps Command and Control

Principle: Components operating network management systems shall develop alternative and/or backup and disaster recovery SLAs. It supports JCA 6.2 Enterprise Services.

Capability Gap	
<i>NetOps Network Management SLAs are inconsistent.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>1) Establish network management SLAs that will articulate robust QoS, interoperability, and availability.</i>	<i>Consistent and standardized SLAs that address information exchanges and operations to ensure QoS, operational interoperability and network availability.</i>
<i>2) Ensure Continuity Of Operations (COOP) and associated activities for information systems and networks.</i>	<i>Common operating picture of the network, continuity of operations across the network with applicable information systems, support for Mission Essential Functions (MEF), plans for disaster recovery, and COOP services based on Mission Assurance Category (MAC).</i>
<i>3) Information Technology (IT) backup process will have ability to achieve necessary data restoration after an event and IT service continuity recovery plans will be developed and kept aligned to business continuity priorities.</i>	<i>SLAs addressing the following: a) disaster recovery and backup plans to reconstitute complex configurations to original configurations and settings, b) monitoring of backup validation processes to ensure recovery success and adherence to regulatory compliance requirements, and c) continuity in maintenance of recovery plans to ensure business continuity priorities are met by IT services.</i>
<i>4) Follow Appendix C (Standards List, StdV-1).</i>	
Considerations and Known Risk(s)	
<i>Incomplete network management data exchanges could provide limited visibility of needed critical mission infrastructure assets.</i>	

Table 3 – Resilience and Continuity of Operations

Principle: NM systems shall employ methods of data diversity and duplication to mitigate potential loss or disruption of capabilities. It supports JCA 6.3 Net Management.

Capability Gap	
<i>NM data is held in singular repositories or processed in single nodes reducing resilience and redundancy.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>1) NM systems will employ applicable methods (e.g., data diversity, duplication, replication, storage redundancy) to mitigate potential loss or disruption of their capabilities.</i>	<i>Multiple data storage and data processing sites to mitigate potential data and processing losses.</i>
<i>2) Follow Appendix C (Standards List, StdV-1).</i>	<i>Established authoritative NM data repository and services provided throughout the enterprise utilizing methods of transmission and storage ensuring resiliency and continuity of capabilities.</i>
Considerations and Known Risk(s)	
<i>Lack of availability of repository capabilities and transmission mediums must be factored when designing and incorporating systems into best practice and Tactics, Techniques, Procedures (TTPs).</i>	

Table 4 – Data Diversity and Duplication

Principle: NM systems shall use integrated and automated configuration management (CM) and policy based network management (PBNM) capabilities to improve the ability to rapidly and consistently maintain network performance and respond to information assurance (IA) events. It supports JCA 6.3 Net Management.

Capability Gap	
<i>Not all Network management capabilities exploit integrated CM and PBNM functionality to implement policies and changes on the network.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s).
<p><i>1) Ensure NM systems use integrated and automated CM and PBNM capabilities to implement network management policies to maintain network performance and to respond to IA events.</i></p> <p><i>2) Follow Appendix C (Standards List, StdV-1).</i></p>	<p><i>Effective use of CM and PBNM capabilities to implement policies (e.g., having complete visibility of configuration assets on the network) ensuring maintenance of network performance, rapid and consistent responses to IA events, and ability to scale to support additional, changing and complex operational requirements.</i></p>
Considerations and Known Risk(s)	
<i>Partially integrated configuration management efforts and unsupported automated policy based network management efforts within complex networks may require additional resources to ensure network changes support operations.</i>	

Table 5 – Integrated Configuration Management (CM) and Policy Based Network Management (PBNM) Capabilities

Principle: NM and Systems Management (SM) systems shall be integrated, as appropriate, to create IT asset management capabilities that provide the warfighter with enhanced situational awareness (SA) to support common complete network understanding, planning, and monitoring; distributed network management and spectrum control; and also to reduce life cycle costs. It supports JCA 6.3 Net Management

Capability Gap	
<i>Army IT resource management suffers due to discontinuities in the network and a lack of visibility of all network assets.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>1) NM and SM systems will be integrated to create integrated IT asset management capabilities ensuring mitigation of operational discontinuity risks, improved situational and network awareness, enhanced asset awareness and distributed network management and spectrum control.</i>	<i>Mitigation of network operational discontinuity risks, common and complete visibility of configuration assets on the Network, and integrated network management for greater situational awareness and improved network spectrum control.</i>
<i>2) Assets (e.g. radios, servers, storage and processing devices, software, firmware) must be marked appropriately for identification, tracking, monitoring, and reporting/logging during transfer and allocation.</i>	<i>IT assets appropriately labeled and marked to support NM and SM systems in IT asset management.</i>
<i>3) Follow Appendix C (Standards List, StdV-1), ITIL best practices, and DOD Information Technology Asset Management (ITAM) best practices.</i>	
Considerations and Known Risk(s)	
<i>Limited alignment through planning, acquisition, operational and decommissioning life cycle states adversely affect successful tracking of assets and financial obligations.</i>	

Table 6 – Integrated IT Asset Management

<i>Principle: NM shall be able to interface with the Mission Partner Environment (MPE). It supports JCA 6.3 Net Management.</i>	
Capability Gap	
<i>Currently, there is no single interoperable allied mission network that is available for immediate deployment.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<p>1) <i>Ensure NM, depending on coalitions of foreign military and non-military partners within the MPE, is able to interoperate with applicable networks supporting unified action and mission partner operations.</i></p> <p>2) <i>Provide guidance to partners in the MPE to ensure partner network environments are adequately differentiated between domains or national enclaves to support Army architecture interfaces.</i></p> <p>3) <i>Follow Appendix C (Standards List, StdV-1) and ITIL best practices.</i></p>	<p><i>Ability of Army NM to be interoperable and scalable (for the network to operate with increasing numbers of partners, trust relationships, users, regional commands, geographical distribution, sensors/feeds, and applications/services) with allied or coalition MPE to support unified actions of mission partners while efficiently and effectively collaborating and sharing NM information using secure networks.</i></p> <p><i>When available, MPE will be capable of interoperating with Army NM at the applicable domain or enclave levels.</i></p>
Considerations and Known Risk(s)	
<i>Future coalition networks should be designed in light of developments in End State Information Sharing framework and cloud computing. Trade-offs between interoperability and security and technologies will constrain the solution set.</i>	

Table 7 – NM Interfaces to Joint Mission Partner Environment (MPE)

Principle: Where possible, NM interfaces to mobile partners shall employ commercial standards, architectures, models, and exchange mechanisms. It supports JCA 6.3 Net Management.

Capability Gap	
<p><i>Today, the Army serves as the primary “mobile service provider” (MSP) of commercial mobile devices to numerous Army organizations and individual end users. Going forward, this MSP role will expand significantly due to the addition of various commercial mobile device user communities and complicated NM system. The gap is the lack of standardized and integrated network operations management to support the MSP role.</i></p>	
Architectural Rule(s) that mitigate Capability Gap.	Desired Outcome(s)
<p><i>1) The Army will develop standardized and integrated NetOps capabilities that can support the MSP role.</i></p> <p><i>2) Follow Appendix C (Standards List, StdV-1) and ITIL best practices.</i></p>	<p><i>Standardized NetOps management to support the MSP role will improve the ability to develop and share common management data exchanges between mobile users and service providers, efficiencies through smaller set of standards and ease of implementation, client access into LWN authoritative data and service resources, security with communications and data storage, utilization of Defense enterprise mobile support services, and utilization of common Software Development Kits (SDK) wherever possible.</i></p>
Considerations and Known Risk(s)	
<p><i>Lack of standardization, integration, and security could delay an enterprise solution that traverses the Army Mobile Handheld Computing Environment (Mobile HH CE) - for future Army mobile apps and devices.</i></p>	

Table 8 – NM Interfaces to Mobile Partners

Principle: ESD functional requirement should be based on statistical information related to current DOD-wide call center, help desk, service desk, and other IT support operations. It supports JCA 6.3 Net Management.

Capability Gap	
<i>There is a need to establish an Army-wide Enterprise Service Desk (ESD) function across a number of subordinate and federated organizations to ensure reliable IT service support to LWN service consumers.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>1) Through consolidation and/or augmentation efforts, use applicable statistical information to support establishment of Army-wide ESD capability at appropriate levels in Army organizations.</i>	<i>Use of statistical information during analysis for having established, coordinated and federated ESDs at appropriate levels throughout the Army to reliably support LWN service consumers.</i>
<i>2) As a minimum, ensure ESDs provide the following functionalities: a) be capable of processing support calls at a rate equivalent to commercial solutions, b) have a first call resolution percentage within commercial thresholds, c) be able to dispatch on-site technicians within established thresholds, d) shall refer issues to operations within assigned thresholds, e) complete and forward to the appropriate IT Service Manager requests from users to modify the functionality of a service, and f) have ability to access change request submitted by the user for enhanced IT Service functionality in order to provide the user updates on its current status.</i>	<i>ESDs have functionalities that meet or exceed commercial best practice requirements to ensure reliable IT service support associated with capacity and performance requirements (e.g., calls per hour, service requests processing time [processing time from users to ESD and back to users], status/update provided back to users on their change requests).</i>
<i>3) Follow Appendix C (Standards List, StdV-1) and ITIL best practices.</i>	
Considerations and Known Risk(s)	
<i>ASA (ALT) is responsible for the consolidation and reduction of Army-wide call centers, help desk, service desk, and other IT support operations supported by principal Army/Joint/DOD stakeholders; prior command/activity investments must be accounted for in cost benefit analysis.</i>	
<i>Capability Development Documents (CDD) or Joint Emergent Operational Needs (JEON) and in-place contracted services are incorporated in solution development.</i>	

Table 9 – Enterprise Service Desk (ESD) Objectives

3.3. Net Assurance: Access and Defend Services

The principles applicable to this Service category are shown in Tables 10 and 11.

<i>Principle: Defense will improve by increased understanding of the full Battle-space (physical and logical) and benefit from audits, sensors, forensic and incident management inputs across LWN and the JIE. It supports JCA 6.4 Information Assurance.</i>	
Capability Gap	
<i>Identifying and stopping outside/insider attackers, configured systems that cannot ensure that attacks are contained should they evade perimeter defenses, and hardened perimeters that result in reduced mission agility prevent network manager and their commanders from effectively defending LWN.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<p>1) Ensure NetOps processes include situational awareness and understanding of the full Battle-space through direct observation, monitoring and analysis as supported by the use of network sensors, service desk incidents and vulnerability reports.</p> <p>2) As a minimum, provide NetOps the ability to perform the following: a) mark data assets accurately and as required (e.g., classification, dissemination controls, releasability, declassification), b) secure file transfer, c) appropriately characterize and publicize, through situational awareness reporting to the appropriate communities, the consequences of cyber events on the Network and its supported missions within, and d) ensure endpoint security.</p> <p>3) Incorporate within the JIE Single Security Architecture (SSA) Framework.</p> <p>4) Follow Appendix C (Standards List, StdV-1) and ITIL best practices.</p>	<p>NetOps has situational awareness and understanding of the full Battle-space through direct observation, continuous monitoring, and analysis of the Army's end-to-end Network and incident event reporting.</p> <p>NetOps has abilities (e.g., marked and secured metadata, asset management, secured data at rest and in-transit within and across disparate security domains, compliance with security TTPs [e.g., scanning], centrally managed endpoint security through the use of host-based security agents, antivirus, intrusion prevention and detection, rogue system detection, system compliance and policy enforcement, threat isolation ability) to effectively mitigate risks involving network penetration and intrusions (e.g., outside and inside attacks), denial-of-service, and any other security breach that impacts network managers and commanders from effectively defending the LWN.</p> <p>NetOps is integrated with JIE SSA Framework.</p>
Considerations and Known Risk(s)	
<i>Cyber capabilities at the appropriate level of the formation may require training and/or Top Secret / Special Compartmented Information (TS/SCI) clearances.</i>	

Table 10 – Defend, Understand, Secure

Principle: Reduce the consequences of network attacks by monitoring security compliance, detecting malicious activity, and enforcing cryptographic management best practices. It supports JCA 6.4 Information Assurance.

Capability Gap	
<i>Information Assurance (IA) and cryptographic policies are not continuously updated and enforced.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<p><i>1) Implement management activities and practices to ensure the update and enforcement of IA and cryptographic policies.</i></p> <p><i>2) As a minimum, ensure activities and practices include the following: a) find malicious behavior through passive and active continuous monitoring and assess cause and effects, b) manage malware effect detection, malware software, security auditing, encryption, and information assurance (IA) policy implementation, c) alert commands/activities to vulnerability analyses and changes in information operations condition postures, and recommend corrective action to mitigate threats, d) publish malware definitions, malware software identification, and information assurance policies (including risk mitigation), e) enforce the use of protocols that provide data confidentiality, data integrity, authentication, and non-repudiation, f) manage the allocation, distribution, maintenance and use of cryptographic keying and encryption materials.</i></p> <p><i>3) Follow Appendix C (Standards List, StdV-1).</i></p>	<p><i>NetOps management activities and practices are established to continuously update and enforce IA and cryptographic policies.</i></p> <p><i>As a minimum, NetOps effectively enforces IA and cryptographic policies that result in continuous monitoring of the Army's Network end-to-end security, certification and accreditation of Information Systems through an enterprise process, implementation of corrective actions, improved automation of Communications Security (COMSEC) key management, control, and distribution functions, and enabled DOD information systems to use Public Key Infrastructure (PKI) for digital signature and encryption; with applicable efforts to mitigate the impact of IA threats (potential and actual) to network services, systems, and devices.</i></p>
Considerations and Known Risk(s)	
<i>Measures not followed to protect and defend information and Information Systems to ensure their availability, integrity, authentication, confidentiality will allow threats to degrade Command and Control of network operations.</i>	

Table 11 – Information Assurance and Cryptography Management

3.4. Content Management: Share Services

The principles applicable to this Service category are shown in Tables 12 to 15.

<p><i>Principle: Systems Management (SM) systems shall have and use integrated, automated configurations capabilities to improve the ability to rapidly and consistently maintain systems availability and performance and respond to information assurance (IA) events. It supports JCA A3.2.1 Provide Computing Infrastructure.</i></p>	
<p>Capability Gap</p>	
<p><i>Not all systems management implementations exploit integrated configuration management functionality to improve policy and change management implementation.</i></p>	
<p>Architectural Rule(s) that mitigate Capability Gap</p>	<p>Desired Outcome(s)</p>
<p><i>1) Army systems management implementations will utilize integrated configuration management to perform the following: a) improve systems management support to generating and operating forces, b) reduce systems management burdens on the operating and generating forces, c) apply Common Operating Environment (COE) architecture that normalizes the computing environment and achieves a balance between unconstrained innovation and standardization.</i></p> <p><i>2) Follow Army NetOps CONOPS, JIE Operations CONOPS, and ITIL best practices.</i></p>	<p><i>Systems management implementations, after using integrated configuration management functionality, will show abilities to improve policy and change management as well as effective and efficient operation of information systems and elements of systems (operating systems, databases, and hosts of the end-users) by having the following: a) ability to remotely configure and manage Army enterprise servers, general purpose desktops/laptops, web systems, storage systems, virtual machines, and Army applications, and b) ability to perform remote host discovery, patching, limited software self-repair, host/application event/fault management, and c) ability to manage General Purpose (GP) computing assets, GP software distribution and perform installation, patch, remote platform maintenance and configuration settings control.</i></p>
<p>Considerations and Known Risk(s)</p>	
<p><i>The current systems management design is comprised mainly of command procured solutions. There is no formal Army Program of Record resulting in inconsistent training, incompatible baselines, limited cross-systems integration, or organizational staffing to ensure the Joint Information Environment vision is met.</i></p>	

Table 12 – Integrated Systems Management

Principle: The ability to perform network-enabled Information Dissemination Management (IDM) tasks and dissemination of the right information, to the right place, at the right time, and in a usable format. It supports JCA 5.2.3 Share Knowledge and Situational Awareness.

Capability Gap	
<i>Non-homogeneous LWN prevents seamless transmission of information to any authorized user including partners and coalitions.</i>	
Architectural Rule(s) that mitigate Capability Gap.	Desired Outcome(s)
<i>1) Enable network users and systems to exchange information utilizing integrated network services (e.g., e-mail, DOD unique message formats, server domain access, web services, and alerts).</i>	<i>A homogeneous LWN ensuring seamless transmission and dissemination (development and sharing of common messaging data) of the right information to authorized users (Partners and Coalition) through the use of integrated network services.</i>
<i>2) Ensure authoritative and trusted data repositories will be exposed and made accessible by Information Dissemination Management (IDM) services.</i>	<i>Seamless transmission and dissemination also includes IDM services that ensure timely and accurate delivery of information through the maintenance of IDM policies and proper identification of information needs and requirements throughout the information lifecycle; outcomes include reduced cost of integration, reduced duplication of effort, improved situational awareness, and improved information exchanges between users and between systems.</i>
<i>3) Follow Appendix C (Standards List, StdV-1).</i>	
Considerations and Known Risk(s)	
<i>Integration of intelligent agents, web services, and traditional data sources in a service-oriented architecture to facilitate collaboration.</i>	

Table 13 – Information Dissemination Management

Principle: Capabilities designed to support users outside of their existing expected set can achieve a measure of agility as a competitive advantage over adversaries. Data, services and applications must be serviced to be visible, accessible, understandable, and trusted by “the unanticipated user”. It supports JCA 5.2.2.3 Define Knowledge Structure.

Capability Gap	
<i>Not all NetOps information is currently searchable and is currently held in isolated repositories which are not easily discoverable or easily permits maximum reuse of data and information.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<p><i>1) C2 and NetOps personnel will be able to discover information, content or services of the Network that exploit unique descriptions stored in directories, registries, and catalogs (an example of a discovery service is a search engine).</i></p> <p><i>2) Authoritative Data Sources will be the primary first location for data information to be discovered; ensure exchanges are standardized, data will be described in accordance with the enterprise standards for metadata discovery, reduction (to avoid duplication) of reporting tools to identify, create, use and re-use of existing information, and integration of available information at the Open Systems Interconnection (OSI) model levels.</i></p> <p><i>3) Follow National Information Exchange Model (NIEM), DOD and DISA adopted industry interface standards, and Appendix C (Standards List, StdV-1).</i></p>	<p><i>NetOps information is searchable and easily discoverable providing C2 and NetOps personnel the following: a) improved ability to develop and share common data between NetOps partners and service providers, and b) improved access that provides enterprise-wide granting or denying requests for obtaining and using information and related information processing.</i></p> <p><i>Minimization of isolated repositories and availability and use of Authoritative Data Sources; increased use and re-use of authoritative information will reduce data storage and data duplication.</i></p>
Considerations and Known Risk(s)	
<p><i>Data query criteria and query language should be in common structures that can be utilized by communities of interest.</i></p> <p><i>Activities must acknowledge beyond the NetOps data sharing national security interests (defense and law enforcement) the concerns of patents and intellectual property, legitimacy of the requests, contract or privacy interests and consideration of non-disclosure agreements.</i></p>	

Table 14 – Information Exchange Access

Principle: Warfighters will have access to capabilities that permit collaboration between mission partners. Examples of collaboration services are chat, online meetings, and work group applications. It supports JCA 5.2.3 Share Knowledge and Situational Awareness.

Capability Gap	
<i>Current collaboration capabilities provide local rather than enterprise services reducing efficient and collaborative efforts across the enterprise.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>1) Implement enterprise collaboration capabilities to the greatest possible number of authorized users.</i>	<i>Efficient collaboration and sharing of information across the enterprise.</i>
<i>2) Ensure business processes (e.g., TTPs) will be evaluated on efficiency and effectiveness in the context of improved use of common collaboration capabilities in consideration of available information, network limitations and mission needs.</i>	<i>Reduced reliance on local management and administration of collaboration capabilities resulting in efficient and effective business processes.</i>
<i>3) Follow Appendix C (Standards List, StdV-1).</i>	
Considerations and Known Risk(s)	
<i>Collaboration between multiple partners will have to contend with connections from service providers, available bandwidth limitations, and decisions on consideration for Need-to-know verses Need-to-share.</i>	

Table 15 – Collaboration Share Services

3.5 Data and Service Framework

The principles applicable in this section are shown in Tables 16 to 18. Note that these principles are not part of the three NetOps Service categories shown in Sections 3.2, 3.3 and 3.4. However, these principles contribute and support NetOps Services as well as move toward a JIE construct for data and services.

<i>Principle: Data, information and knowledge will be presented and delivered in an appropriate manner to the consumer whether War fighter or other system such that it is accessible, usable and reusable to the maximum number of authorized users. It supports JCA 2.5 Battlespace Awareness Data Dissemination and Relay.</i>	
Capability Gap	
<i>NetOps systems do not (by design) permit easy presentation of data due to inconsistent policies, standards, architectures and classifications.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>1) Army will ensure consistent implementation of policies, standards, architecture, classifications and industry best practices to enable NetOps systems applicable presentation of data (e.g., traditional media and new media for web-based publishing, computer based production, distribution, user interaction of text, interactive media, digital distribution platforms, online distribution, print-on-demand, subscription, self-publishing).</i>	<i>Consistent implementation of policies, standards, architecture and classification with NetOps systems to ensure data availability and easy data presentation resulting in mission success.</i>
<i>2) Use enterprise level data services and storage to increase visibility, permit effective access, use and reuse of presentable data.</i>	<i>Shared data and increased use of common enterprise services to present data, information, and knowledge for wider community distribution.</i>
<i>3) Follow Appendix C (Standards List, StdV-1).</i>	
Considerations and Known Risk(s)	
<i>Not following industry best practices will delay enterprise wide distribution and collaboration of needed information for training, mission support, and improved processes development.</i>	

Table 16 – Presentation of Data

Principle: Army will coordinate its technical, operational, and system architectures in support of DoD standards and frameworks and Army leadership guidance to ensure all necessary capabilities are accurately accommodated and fully synchronized to support tactical and institutional warfighter IT needs. It supports JCA 2.5 Battlespace Awareness Data Dissemination and Relay.

Capability Gap	
<i>Existing Army NetOps architectures have not always been developed in accordance with DOD IEA. As a result, there are gaps and inconsistencies throughout the force preventing integration and interoperability with other departments and mission partners.</i>	
Architectural Rule(s) that mitigate Capability Gap	Desired Outcome(s)
<i>1) Follow the Services model with a capability view structure that addresses Army LWN requirements. [See Figure 3, Army NetOps Services, SvcV-1]].</i>	<i>Consistent and coordinated development of NetOps services with other Military Departments and Mission Partners; the service areas provide a means of grouping similar capabilities together for analysis and planning purposes.</i>
<i>2) Integrate TRADOC and ASA(ALT) Operational NetOps Architecture and System Engineering Plans (SEP) with the Technical NetOps Department of Defense Architecture Framework (DODAF) products.</i>	<i>Integration of NetOps operational, systems and technical architectures with other parallel applicable documents and products.</i>
<i>3) Follow Appendix C (Standards List, StdV-1).</i>	
Considerations and Known Risk(s)	
<i>No major risks identified at this time.</i>	

Table 17 – Services Structure

Principle: Army will move toward an information sharing framework in line with DOD architecture vision using an open standards based layered telecommunications management network architecture and a standardized functional dictionary. It supports JCA 6.3.1 Optimized Network Functions and Resources.

Capability Gap	
<i>Existing Army systems and services have gaps and inconsistencies throughout the Network that prevents using industry best practice standards, management processes, data sharing, and situational awareness views.</i>	
Architectural Rule(s) that mitigate Capability Gap.	Desired Outcome(s)
<p><i>1) Use service terms defined in the Annex (Army NetOps Services Integrated Dictionary, AV-2, a separate standalone document).</i></p> <p><i>2) In coordination with DOD IEA (DISA and JIE), follow DoDI 8410.03, Network Management, that defines telecommunications management network (TMN) as architecture for management, including planning, provisioning, installation, maintenance, operation and administration of telecommunications equipment, networks, and services.</i></p> <p><i>3) Follow the Army Information Architecture (AIA).</i></p> <p><i>4) Follow the Global Information Grid (GIG) Technical Profiles (GTP), DoD IT Standards Registry Standard ITU-T M.3400:2000, TMN Management Functions, 2000 mandated standard architecture as depicted in Appendix D, Figure 4.</i></p> <p><i>5) Follow the International Organization for Standardization (ISO) for FCAPS (Fault, Configuration, Accounting, Performance, Security) network management tasks.</i></p> <p><i>6) Follow Appendix C (Standards List, StdV-1) and DOD CIO guidance.</i></p>	<p><i>Army network and systems postured with a framework (e.g., standards, models, processes, data and information, architecture) to improve NetOps through the following :</i></p> <p><i>Adherence to the Army NetOps Services Integrated Dictionary (AV-2) to enable improved NetOps services across the Army force structure.</i></p> <p><i>Improved interoperability with Defense Information Systems Network (DISN) services and TMN to provide commanders with more complete situational awareness.</i></p> <p><i>Compliance with Army Information Architecture (AIA) vision will assist generating forces and operating forces ability to provide, share, and use network operations information sharing to enhance mission effectiveness.</i></p> <p><i>Interoperability with DISA’s Operational Support System Architecture which the JIE Enterprise Operations Center (EOC) Operations Support System (OSS) framework is based.</i></p>
Considerations and Known Risk(s)	
<i>Full situational awareness, total asset/resource management and complete defense will not be achieved without efficient data sharing.</i>	

Table 18 – Service Framework

4 Technical Positions and Implementation Patterns

4.1 Technical Positions

Technical positions are identified in the DoDAF StdV-1 (Standards Profile) and StdV-2 (Standards Forecast). The NetOps StdV-1 is discussed in Appendix C. StdV-2 is currently being developed and planned for inclusion in updated versions of this NetOps RA document.

4.2 Implementation Patterns

Figure 3 illustrates Army NetOps Services (SvcV-1, Service Context Description). This pattern shows the overall structure and organization of NetOps Services. This view shows first (e.g., Operate Services, Defend Services, Share Services) and second (e.g., Change Management Services, Secure Transfer Services, Content Management Services) level services. The first level of the SvcV-1 serves as a single source for Army program managers to align and assist the NetOps community in indentifying IT solutions. The second level is for general NetOps service and interface development. Additional services under the second level of services are currently being defined and will be available on the next update of this NetOps RA document.

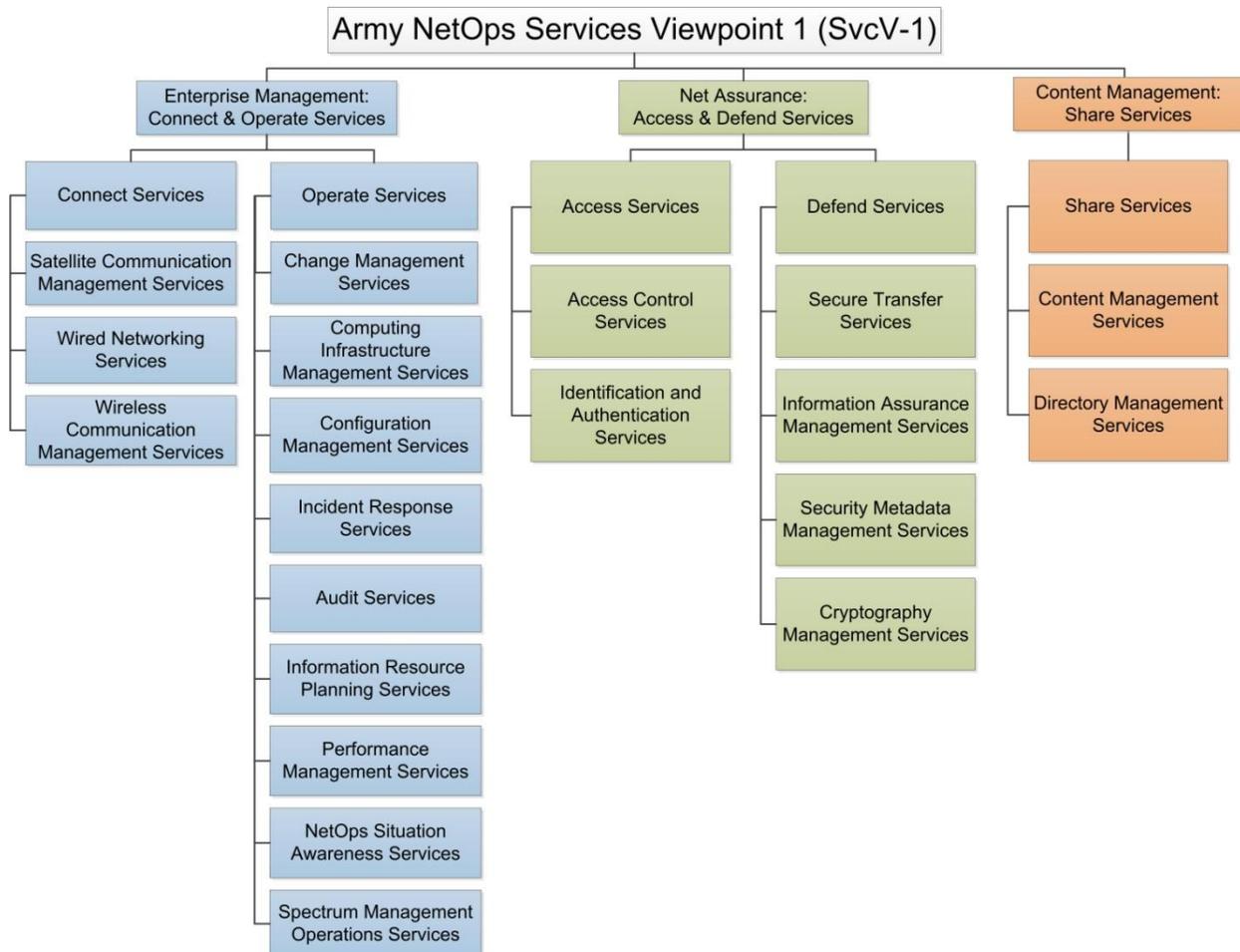


Figure 3: Army NetOps Services (SvcV-1)

5 Summary

The objectives of this Army NetOps RA are to guide the update and standardization of NetOps to realize full capabilities envisioned in LWN 2020 and Beyond Enterprise Architecture. NetOps is envisioned as a capability with increased flexibility, simplified processes and improved network defenses. To guide NetOps development, this RA document provides a framework by identifying principles and rules needed to ensure focused and consistent development and refinement of Army Network Operations. The RA is a key part of Army CIO/G-6 Rules-Based Architecture and ensures alignment with DIEA, industry best practices, and the JIE.

In addition, the principles and rules within this RA are consistent with the desired outcomes of the DOD and the Army's LWN 2020 and Beyond Enterprise Architecture. This NetOps framework will improve network operations by establishing a global, single, secure, standards-based Army Network. This will make the best use of available Army resources for the Network and eliminate unnecessary redundancies and inefficient IT infrastructure by providing a common reference for portfolio and weapons systems reviews. This document is intended to ensure network operations effectively use the LWN, enable the latest information technology to support warfighting and business missions, and ensure Army NetOps can best support the warfighter in dynamic network environments. It also will ensure the Army is postured to leverage JIE capabilities as they emerge.

Appendix – A: References

Department of Defense Global Information Grid Architectural Vision, June 2007;
http://www.msco.mil/documents/7_GIG%20Architectural%20Vision%20-%20200706%20v1.0.pdf

DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 23 April 2007;
<http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf>

DoDD Information Assurance, 21 November 2003;
http://www.prim.osd.mil/Documents/DoDD_8500_1_IA.pdf

DODD Department of Defense Continuity Programs 3020.26, 09 January 2009:
<http://www.dtic.mil/whs/directives/corres/pdf/302026p.pdf>

DOD NetOps Strategic Vision memo, 11 Dec 2008;
http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD_NetOps_Strategic_Vision.pdf

DOD Reference Architecture Description, June 2010.

http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf

DODI 8320.02, Sharing Data, Information, and IT Services in the DoD, 05 August 2013;
<http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf>

DODI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007,
<http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf>

DoDI 8410.02, NetOps for the Global Information Grid (GIG), 19 December 2008;
<http://www.dtic.mil/whs/directives/corres/pdf/841002p.pdf>

DoDI 8410.03, Network Management, 29 August 2012;
<http://www.dtic.mil/whs/directives/corres/pdf/841003p.pdf>

DODI 8320.05, Electromagnetic Spectrum Data Sharing, 18 August 2011,
<http://www.dtic.mil/whs/directives/corres/pdf/832005p.pdf>

DOD IEA, 10 August 2012; <http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx>

DOD IT Standards Registry, under GTG-P Global Information Grid (GIG) Technical Profiles (GTP), <https://gtg.csd.disa.mil/disr/dashboard.html>

DOD Global Information Grid (GIG) Architecture Federation Strategy Version 1.2,
August 2007

DOD Information Assurance policy chart http://iac.dtic.mil/csiac/ia_policychart.html site

DOD ITAM Integrated Process Team;
<http://acc.dau.mil/CommunityBrowser.aspx?id=445971&lang=en-US>)

CJCSI 6510.01F, INFORMATION ASSURANCE (IA) AND SUPPORT TO COMPUTER NETWORK DEFENSE (CND), 09 February 2011;
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

CNSS; Committee on National Security Systems; <http://www.cnss.gov/>

CYBERCOM: <https://www.jtfgno.mil/default.aspx>

Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy, August 2009;
http://dodcio.defense.gov/Portals/0/Documents/DoD_IA_Strategic_Plan.pdf

Joint Capability Areas (JCA): <https://jdeis.js.mil/jdeis/index.jsp?pindex=43>

Joint Information Environment (JIE) Operations CONOPS, 25 January 2013

Joint Publication 6-0 Joint Communications System, 10 June 2010;
<https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=235>

National Information Exchange Model (NIEM) <http://www.ise.gov/national-information-exchange-model-niem>

Net-Centric Enterprise Information Assurance (IA) Strategy Annex to the DoD IA Strategic Plan

DISA (Defense Information Systems Agency) service catalog:
<http://www.disa.mil/Services> [current]

DISN (Defense Information Systems Network) Architecture, September 2012;
https://intellipedia.intelink.gov/wiki/DISA_Global_Information_Grid_Convergence_Master_Plan_Outline/OSS_Architecture

Glossary of Key Information Security Terms, May 2013;
<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

AR 25-1, Army Information Technology, 25 June 2013;
http://www.apd.army.mil/pdf/r25_1.pdf

AR 25-2, Information Assurance, March 2009:
http://armypubs.army.mil/epubs/pdf/r25_2.pdf

DA PAM 25-1-1, Army Information Technology Implementation Instructions, 25 June 2013; http://www.apd.army.mil/pdf/files/p25_1_1.pdf

Army Appendix C: Common Operating Environment (Oct. 2010) to LandWarNet 2020 and Beyond Enterprise Architecture.
<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>

Army Directive 2009-03, Army Data Management, 30 October 2009;
http://armypubs.army.mil/epubs/pdf/ad2009_03.pdf

Army Information Technology Management Reform (ITMR) Implementation Plan.
February 2013
<http://ciog6.army.mil/LinkClick.aspx?fileticket=l4XCj2m6A6l%3d&tabid=64>

Army Mobility Strategy (CAC required);
https://intellipedia.intelink.gov/wiki/User:Demetrius.I.davis/Army_Mobility_Strategy

Army Coalition Contingency Mission Network: G-6 Studies Day, Presenters: Dr. Isaac Porche and Dr. Joel Predd, RAND ARROYO Center, May 2012

Army Common Operating Environment Architecture Guidance, DA, Memorandum, 20 October 2010;
<http://ciog6.army.mil/LinkClick.aspx?fileticket=wFb9UKmAEGo%3d&tabid=146>

Army Identity and Access Management Reference Architecture V3.0 (DRAFT), January 2014, (To be published)

Army Information Architecture (AIA) June 2013
<http://ciog6.army.mil/LinkClick.aspx?fileticket=bsn-3crGLKE%3d&tabid=146&portalid=1&mid=817>

Army LandWarNet 2020 and Beyond Enterprise Architecture (Aug. 2013)

<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>

[http://ciog6.army.mil/Portals/1/Architecture/LWN%202020%20EA%207%20August%202013%20Version%201.0%20\(FINAL\).pdf](http://ciog6.army.mil/Portals/1/Architecture/LWN%202020%20EA%207%20August%202013%20Version%201.0%20(FINAL).pdf)

Army Network Security Reference Architecture, V1.0, 01 August 2013;

<http://ciog6.army.mil/Architecture/tabid/146/Default.aspx>

Industry sites:

IT Service Management Forum (ITSM); <http://www.itsmfusa.org/>

DOD participation in the TeleManagement Forum (TMF);

<http://www.tmforum.org/defense>

Appendix – B: Acronyms

Abbreviation	Definition
AAA	Authentication - Authorization - Accounting
ADN	Area Distribution Nodes
AESD	Army Enterprise Service Desk
AIA	Army Information Architecture
API	Application Programming Interface
ARCADIE	Army Capability Architecture Development and Integration Environment
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics, and Technology
ATM	Asynchronous Transfer Modem
BMA	Business Mission Area
CNSSI	Committee on National Security Systems Instruction
COE	Common Operating Environment
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
DEE	DOD Enterprise Email
DDMS	DOD Discovery Metadata Specification
DIACAP	DOD Information Assurance Certification and Accreditation Process
DIEA	Defense Information Enterprise Architecture
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DOD IT Standards Registry
DNS	Domain Name System
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODIN	Department of Defense Information Network
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
EIEMA	Enterprise Information Environment Mission Area
EMS	Element Management System
ERP	Enterprise Resource Planning
ES	Enterprise Services
ETFM	Enterprise Telephony Firewall Management
EUB	End-User Building Switch
FCAPS	Fault, Configuration, Accounting, Performance, Security
FedRAMP	Federal Risk and Authorization Management Program
FR	Frame Relay
Gb/s IP	Gigabits per second Internet Protocol
GOTS	Government Off the Shelf
GIG TP	Global Information Grid Technical Profiles
ICAN	Installation Campus Area Network
IDM	Information Dissemination Management
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission

Abbreviation	Definition
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITAM	Information Technology Asset Management
ITIL	Information Technology Infrastructure Library
ITMR	Information Technology Management Reform
ITSMF	IT Service Management Forum
ITU-T	International Telecommunication Union for Telecommunications
JCA	Joint Capability Area
JIE	Joint Information Environment
JMS	Java Message Service
LSC	Local Session Controller
LNA	LWN Network Architecture
LWN	LandWarNet
MAC	Mission Assurance Categories
Mbps	Megabits Per Second
MCN	Main Communication Node
MPLS	Multiprotocol Label Switching
MSP	Multiservice Provisioning Platform
MTOSI	Multi-Technology Operations System Interface
NIEM	National Information Exchange Model
NECs	Network Enterprise Centers
NETCOM	Network Enterprise Technology Command
NMA	Network Mission Area
OCO	Offensive Cyber Operations
ODXC	Optical Digital Cross Connect
OTS	Optical Transport System
P/C/S	Post/Camp/Station
PBNM	Policy-Based Network Management
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RA	Reference Architecture
RBA	Rules-Based Architecture
RHN	Regional Hub Nodes
RSS	Regional Security Stack
SC BDEs	Signal Corps Brigades
SDK	Software Development Kits
SIG CMD	Signal Command
SLA	Service Level Agreement
SM	Systems Management
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SP	Service Provider
TDM	Time Division Multiplexing
TLA	Top Level Architecture
TMN	Telecommunications Management Network
TNOSCs	Theater Network Operations and Security Center

Abbreviation	Definition
TRADOC	Training and Doctrine Command
UC	Unified Capabilities
VCS	Video Conference Switch
UTR	Unit Task Reorganization
VOIP	Voice Over Internet Protocol
VOX	Voice-Operated Switch
VPN	Virtual Private Network
WMA	Warfighter Mission Area
XML	Extensible Markup Language

Appendix – C: NetOps Standards List (StdV-1)

The NetOps standards (StdV-1) are grouped by the three core services:

Enterprise Management: Operate and Connect Services
Net Assurance: Access and Defend Services
Content Management: Share Services

Details of the StdV-1 will be available on the ArCADIE web site: <https://cadie.army.mil>

The DOD standards, where the StdV-1 was derived from, can be found by searching the Global Information Grid Technical Profiles (GTP) DOD Information Technology Standards Registry (DISR): <https://gtg.csd.disa.mil/disr/standards/search> site

Note: The Tables (Tables 2 to 18) in this RA document consist of rules for following DISR and industry standards. As the standards mature overtime, CIO/G6 will submit Change Requests to the DISR for the applicable non-DISR/non-mandated standards. Program Managers will ensure that they comply with StdV-1, which include standards selected from the DISR.

Appendix – D: U.S. Army Telecommunications Management Network Model

The DoD’s network management environment of the Defense Information Systems Network (DISN) is transforming toward a single, comprehensive system of integrated components using a service-oriented integration architecture to achieve DoD’s NetOps strategic vision. Known as Network Services DISN Operational Support Systems (OSS), this architecture facilitates and automates many activities by using commercial best practices, industry technologies/standards, and international frameworks.

The DISN OSS is critical to the development and rapid delivery of services to the warfighter as well as offering significant reduction in operational expenses. It also will be key in the JIE in compliance with DISR for Telecommunications Management Network (TMN). To keep pace with the DISN and ensure the Army can best leverage the JIE, the Army TMN model includes Army functionality as well as reflect key attributes of and be in compliance with the DISR. This is presented in Figure 4 and provides a hierarchical visualization providing a basis for NetOps service management and service oriented information sharing.

U.S. Army Telecommunications Management Network Model

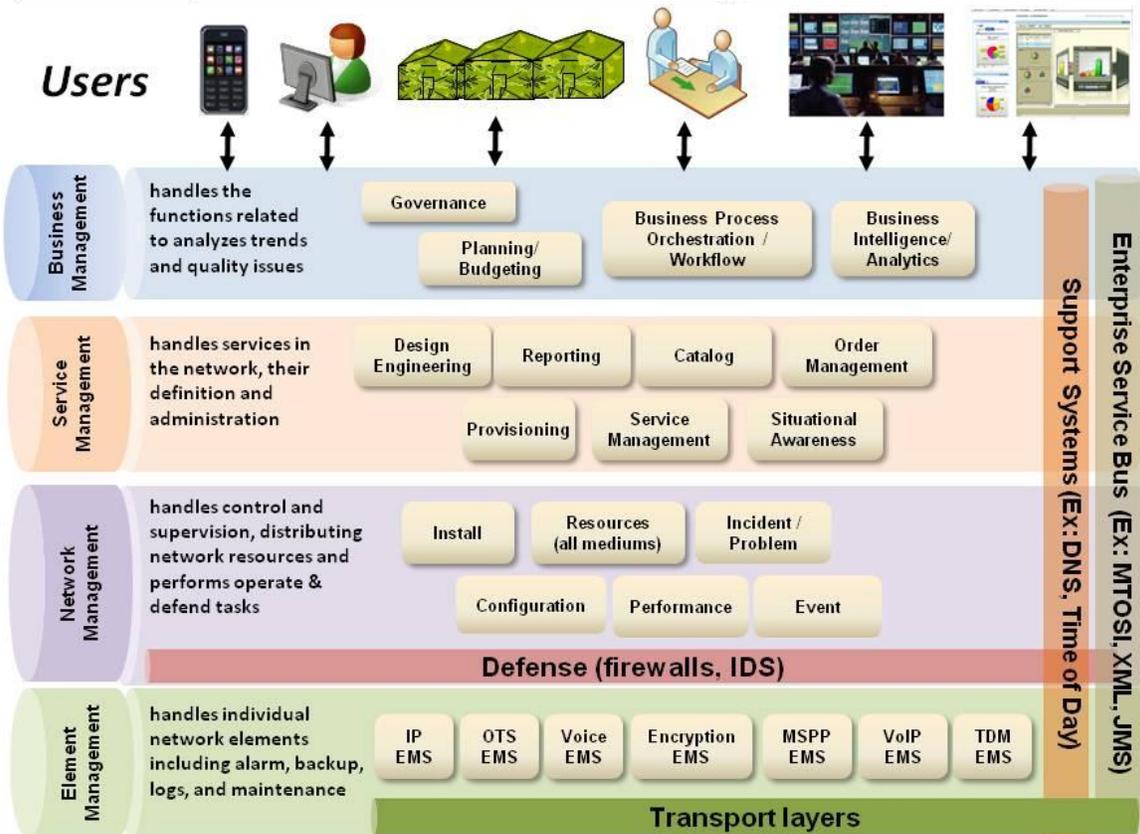


Figure 4: Army Telecommunications Management Network Model

The Army TMN model shows four layers. Each layer comprises a variety of services that interface with other layers through enterprise service bus and/or support systems. All layers and interfaces represent an infrastructure that supports users in different warfighting and business environments.

Business Management layer handles the functions related to trend analysis and quality issues; directs processes, sets policies, and translates the commander's intent into specific course of action plans for preparation and execution.

Service Management layer handles network services and their definition, administration, engineering missions into specific work plans, technical orders or communications tasks, acquiring, sustaining, decommissioning, and disposal of equipment, services and information.

Network Management layer handles installing and distributing network resources, performs operate and defend tasks, performs control tasks, synchronizes resources with Commander's prioritization, maintains agreed service levels, manages incidents/problems, performance and change management, and assures network and information availability by anticipating, preventing, detecting and responding to malicious and non-malicious threats; includes defense entities (e.g., firewall, intrusion detection system [IDS]).

Element Management layer handles individual Network Elements Management alarms, information backup, logging, and maintenance; manages functions and capabilities within each network Element Management System (EMS) (e.g., Internet Protocol EMS [IP EMS], Optical Transport System EMS [OTS EMS]); however, does not manage the traffic between them, and can include automated delivery of updates and patches to deployed server appliances, operating systems and all related applications.

Support Systems provides applications that are shared among all layers; examples are access control, time-of-day synchronization, storage, Domain Name System (DNS) and auditing following the service-oriented Army Information Architecture (AIA) vision.

Enterprise Service Bus provides interaction between software applications based on discrete pieces of software providing functionality to other applications following the service-oriented AIA vision.

Defense provides end point security (with host based agents) vulnerability management, intrusion detection and prevention, data protection at rest, threat assessment, anti-virus services and firewall monitoring.

Transport Layers define the electrical and physical specifications and the relationship between a device and a physical transmission medium (e.g., copper wire, fiber optical cable, wireless radio frequency, or satellite).

Annex – A: U.S. Army Network Operations Services Integrated Dictionary (AV-2)

ANNEX to U.S. Army Network Operations Reference Architecture (RA)



U.S. Army CIO/G-6

Version 1.0

Table of Contents

Introduction.....	A-4
Purpose	A-4
Background.....	A-4
Common Terms used in the Army NetOps Architecture:.....	A-7
Summary Information.....	A-8
Section 1: NetOps IT Service Descriptions	A-9
Section 2: NetOps Service Alignments	A-35
Glossary of Acronyms	A-63
References to other architectures and frameworks	A-63

TABLE OF TABLES

Table A-1 – NetOps Service Descriptions	A-9
Table A-2 – NetOps Services Alignments.....	A-35
Table A-3 - Content Management Share Services Alignments.....	A-36
Table A-4 - Directory Management Services Alignments.....	A-37
Table A-5 - Content Management Services Alignments.....	A-37
Table A-6 - Content Collection Service Alignments.....	A-38
Table A-7 - Enterprise Management Connect & Operate Services Alignments	A-39
Table A-8 - Connect Services Alignments	A-40
Table A-9 - Satellite Communication Management Services Alignments.....	A-41
Table A-10 - Wired Networking Services Alignments	A-42
Table A-11 - Wireless Communication Services Alignments	A-43
Table A-12 - Operate Services Alignments	A-44
Table A-13 - Spectrum Management Operations Services Alignments	A-45
Table A-14 - Change Management Services Alignments.....	A-46
Table A-15 - Configuration Management Services Alignments.....	A-47
Table A-16 - Incident Response Services Alignments.....	A-48
Table A-17 - Performance Management Services Alignments	A-49
Table A-18 - Computing Infrastructure Management Services Alignments	A-50
Table A-19 - NetOps Situation Awareness Services Alignment	A-51
Table A-20 - Audit Services Alignments.....	A-52
Table A-21 - Information Resource Planning Services Alignments.....	A-53
Table A-22 - Net Assurance Access & Defend Services Alignments.....	A-54
Table A-23 - Access Services Alignments	A-55
Table A-24 - Access Control Services Alignments	A-56

Table A-25 - Identity and Authentication Services Alignments.....	A-57
Table A-26 - Defend Services Alignments.....	A-58
Table A-27 - Security Metadata Management Services Alignments	A-59
Table A-28 - Cryptographic Management Services Alignments	A-60
Table A-29 - Secure Transfer Services Alignments.....	A-61
Table A-30 - Information Assurance Management Services Alignments.....	A-62

TABLE OF FIGURES

Figure A-1: NetOps Services Organization	A-6
-------------------------------------------------------	------------

Introduction

In support of the NetOps Trail Boss (PEO C3T) and aligning to her priorities, CIO/G-6 produced this comprehensive NetOps Services Integrated Dictionary (DODAF AV-2). This AV-2 documents an agreement resulting in a single source of standardized NetOps services and their corresponding definitions which have been reviewed and coordinated by the NetOps stakeholders (CIO/G-6, ASA(ALT), TCM GNE (TRADOC lead), ARCYBER and NETCOM).

Purpose

The purpose of this AV-2 is to define the sets of information technology services that enable Army Network Operations, and provide the NetOps community an Integrated Dictionary of IT Services supporting NetOps activities. It comprises an AV-2 for Army NetOps Architecture Technical (ANA-T) services and is a companion document to the Army NetOps Architecture Operational (ANA-O) AV-2 that describes the operational viewpoint (produced by TRADOC and available on ArCADIE) and the Army NetOps Architecture System (ANA-S) that describes the system viewpoint (produced by ASA (ALT) and available on ArCADIE). The result of this effort is a single source AV-2 that Army program managers can use to align their programs, and assist the NetOps community in identifying information technology solutions that may be duplicative. The objective is to reduce IT costs by eliminating duplicative services from the Army inventory.

Background

The Army CIO/G-6, in concert with the NetOps Trail Boss (PEO C3T), has led a team of subject matter experts in developing a single source that describes NetOps services in order to reduce confusion over competing terms related to the set of information technology services that support NetOps. The intent of this effort was not to define all terms that relate to NetOps, but only the definitions of IT services supporting NetOps activities.

The team also focused its efforts on defining services relating to four priority areas for the NetOps Trail Boss: Security Supporting Infrastructure Defense, Information Technology Asset Management (ITAM), Service Management, and Spectrum Management Operations.

The list of IT services is closely aligned to the DoD Information Enterprise Architecture (DIEA) service descriptions, with some modifications. In some areas the Army added services to support Global Information Grid (GIG) 2.0 and Army NetOps Architecture Operational Viewpoint that were not covered within DIEA. Some of the definitions were also modified for clarity, or specialized to meet Army requirements.

DIEA also addresses services that are assigned to the Common Operating Environment (COE) community of interest. Those services are not addressed in this NetOps AV-2. Readers should refer to the COE Services AV-2 for descriptions of what DIEA describes as "Share" services. The criteria for inclusion as a NetOps service was that the service must be primarily used by network operators (signals professionals assigned duties to operate, defend, control, manage, etc., network assets), and not those used across the

Army. For example, since all Army personnel use Enterprise Collaboration Services, those services would be described in the COE architecture. Likewise, since NetOps personnel are solely responsible for updating, coordinating, and approving network directory services (described in DIEA as a Share Service), Directory Management Services are described in the NetOps AV-2. Therefore, the Share services considered a part of NetOps services are Content Management and Directory Management. Doctrinally some Spectrum Management Operations reside outside traditional NetOps activities; however, spectrum management is a key enabler of successful network operations. In the tactical arena especially NetOps cannot function without spectrum management. Therefore, the Spectrum Management Operations services are placed within the NetOps service area.

The NetOps IT services are grouped to align to both the GIG 2.0 and DIEA categories, since most Army organizations have traditionally grouped NetOps services according to the GIG 2.0 construct. Figure 1 is a high level Services Context Model, or SvcV-1, that describes the logical groupings of NetOps IT services.

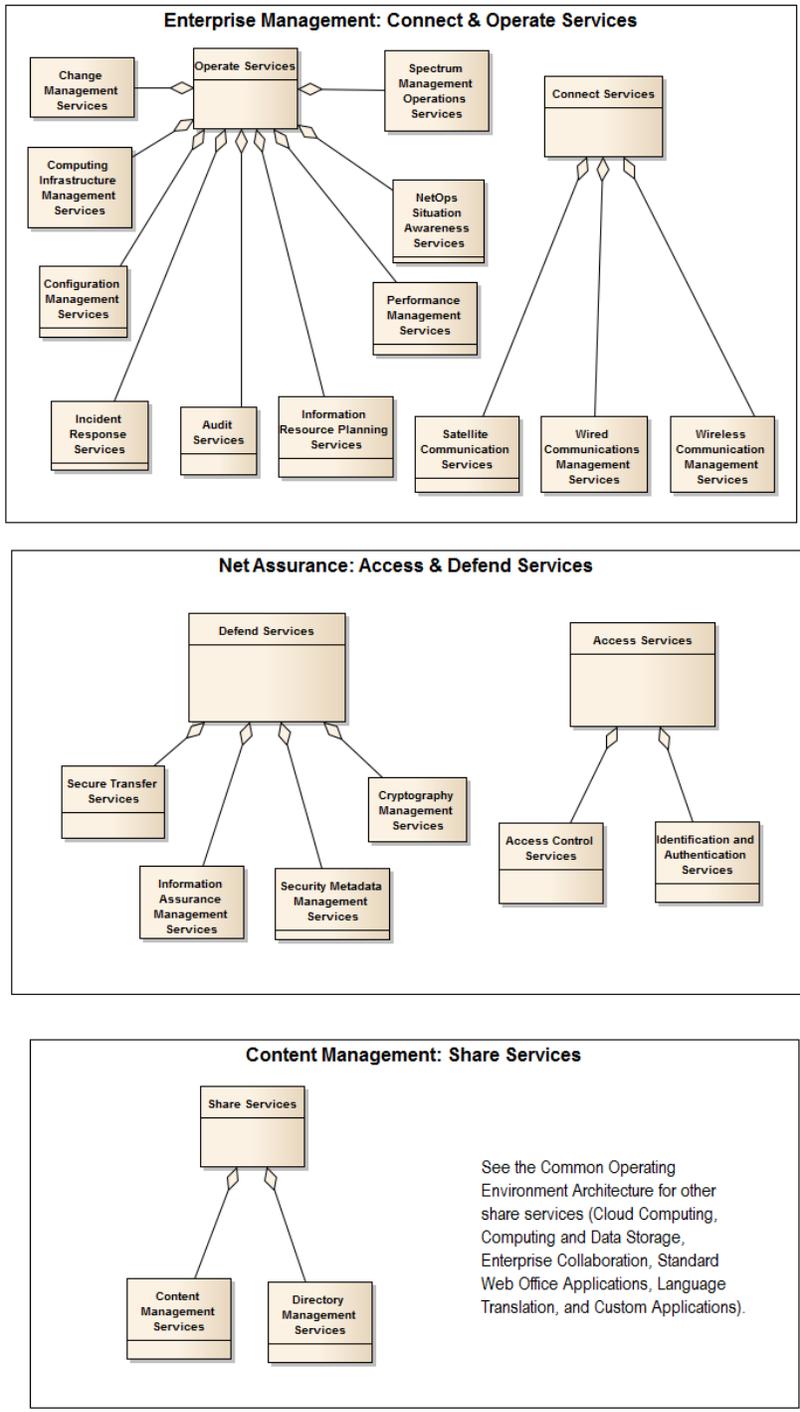


Figure A-1: NetOps Services Organization

Common Terms used in the Army NetOps Architecture:

Service: a mechanism which enables users to request IT capabilities, which are then provided in a manner transparent to the user.

Crucial Services: those Services that must be available to enable or enhance effective mission accomplishment when the warfighter is operating in a disconnected, intermittent, low bandwidth (DIL)/austere environment. (TRADOC Mission Command Information Systems Concept of Operations (CONOPS))

Operationally Accessible Services: those services that are accessible by the warfighter from forward locations within the deployed formations via the Tactical Installation Processing Node (IPN) at each echelon on the deployed tactical network. (TRADOC Mission Command Information Systems CONOPS)

Enterprise Accessible Service: those services that are accessible by the warfighter from the Area Processing Center (APC), Network Service Center (NSC) or from the Generating Force / Home Station. (TRADOC Mission Command Information Systems CONOPS)

Summary Information

<p style="text-align: center;">Primary Audience</p> <ul style="list-style-type: none">• CIO/G-6 SAIS-AOB• ASA(ALT)• PEOs (PEO-C3T, PEO-IEW&S and PEO-EIS)• TRADOC AIMD• Developers and managers of the Army Enterprise Network - which is comprised of the Institutional (enterprise and installation) and Operational components
<p style="text-align: center;">Architecture Perspective</p> <ul style="list-style-type: none">• Enterprise level descriptions of Army NetOps Technical Services
<p style="text-align: center;">Questions this DoDAF Product Addresses:</p> <ul style="list-style-type: none">• What are the sets of information technology services required to support Army NetOps activities?• How are those services organized?• How are those services aligned to Joint, Army, and industry concepts, requirements, and capabilities?
<p style="text-align: center;">Enterprise Level Issues this DoDAF Product Identifies that Require Action</p> <ul style="list-style-type: none">• CIO/G-6 needs to review, modify, and validate the proposed list of NetOps information technology services• The NetOps community of interest needs to coordinate and approve the service definitions• The NetOps community of interest needs to use the final service descriptions as a baseline for identifying and eliminating duplicative NetOps IT services currently in the inventory• ASA(ALT) needs to procure IT services that align to the final list of CIO/G-6 approved service

The AV-2 consists of two sections.

- NetOps IT Service Descriptions aligned to the four development priority areas identified by the NetOps Trail Boss (Security Supporting Infrastructure Defense, ITAM, Service Management, and Spectrum Management Operations). Sections marked “N/A” are outside the current FY14 Trail Boss priority areas. This version of the AV-2 only contains service descriptions that have been reviewed by the AV-2 review team.
- NetOps IT Service Alignment to Joint, Army, and Industry capabilities, activities, and services to provide program managers and others with a quick reference guide of requirements traceability.

Section 1: NetOps IT Service Descriptions

Table A-1 – NetOps Service Descriptions

Number	Service	Description	AV-2 Team Reviewed
0	NetOps Services	Technical capabilities for managing, operating and defending the Army's portion of the GIG.	15-Mar-13
1.	Content Management: Share Services	The set of NetOps services that provide the functionality required to enable information and information assets to be used within and across mission areas (DIEA), through monitoring, managing, and facilitating the visibility and accessibility of information within and across the LandWarNet (derived from GIG 2.0).	15-Mar-13
1.1	Directory Management Services	The set of Share Services that provide (acquire, improve, maintain) a shared information infrastructure for locating, managing, administering, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects.	21-Mar-13
1.1.1	Directory Configuration Service	The Directory Management service that enables updates from the change and configuration management services, including releases (patches).	20-Jun-13
1.1.2	Directory Database Administration Service	The Directory Management service that provides the ability to create and maintain directory management databases.	20-Jun-13
1.1.3	Directory Data Structure Service	The Directory Management service that provides an organizational infrastructure for common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects.	20-Jun-13
1.1.4	Directory Search Service	The Directory Management service that locates common items and network resources, which can include volumes, folders,	20-Jun-13

Number	Service	Description	AV-2 Team Reviewed
		files, printers, users, groups, devices, telephone numbers and other objects.	
1.1.5	Directory Archival Service	The Directory Management service that coordinates file storage (archival/retention) for supported network services and systems.	30-May-13
1.1.6	Directory Performance Reporting Service	The Directory Management service that coordinates with Performance Management services to provide details on Directory Management service and system capacity audits and key performance indicators.	30-May-13
1.1.7	Directory Security Control Service	The Directory Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	30-May-13
1.2	Content Management Services	The set of Share Services that collect, manage, discover, cache, distribute, retrieve, subscribe, share and publish information in any form or medium. (Derived from DIEA and GIG 2.0)	21-Mar-13
1.2.1	Content Discovery Service	The Content Management service that provides a means by which users and applications can find data and services on the GIG, such as through catalogs, registries, and other search services to allow users and applications to more effectively find data. (Derived from DIEA S1.3.1.1, Content Discovery)	20-Jun-13
1.2.2	Content Publication Service	The Content Management service that supports the efficient delivery of mission critical information and products to the warfighter. (DIEA S.1.3.1.0, Content Delivery)	20-Jun-13
1.2.3	Content Collection Service	The Content Management service that collects (pulls) data from other NetOps services for discovery and publication purposes.	21-Mar-13
1.2.4	Content Translation Service	The Content Management service that processes source text for translation from one language and produces a translated text in a target language without human intervention.	20-Jun-13

Number	Service	Description	AV-2 Team Reviewed
1.2.5	Information Dissemination Management Service	The Content Management service that ensures the timely and accurate delivery of information through the maintenance of IDM policies, and the identification of information needs/requirements throughout the lifecycle of information.	27-Jun-13
1.2.6	Content Archival Service	The Content Management service that coordinates file storage (archival/retention) for supported network services and systems.	20-Jun-13
1.2.7	Content Performance Reporting Service	The Content Management service that coordinates with Performance Management services to provide details on Content Management service and system capacity audits and key performance indicators.	30-May-13
1.2.8	Content Security Control Service	The Content Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	30-May-13
2	Enterprise Management: Connect & Operate Services	The set of NetOps services that provide the functionality required to support near-real-time operational management of the LandWarNet to include situational awareness, computing infrastructure management, change and configuration control, and end user support (incident and problem resolution)	27-Jun-13
2.1.	Connect Services	The set of services that provides (acquires, improves, maintains) the ability for any user or service to reach any other or identify and use any other service.	30-May-13
2.1.1	Satellite Communication Management Services	The set of Connect Services that provide (acquire, improve, maintain) telecommunications through the use of communications satellites.	27-Jun-13
2.1.1.1	Satellite Authorization Service	The Satellite Communications Management service that coordinates satellite access requests and authorizations.	21-Mar-13

Number	Service	Description	AV-2 Team Reviewed
2.1.1.2	Satellite Change Management Service	The Satellite Communications Management service that disseminates, coordinates, and implements change schedules affecting satellite networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes.	21-Mar-13
2.1.1.3	Satellite Management Service	The Satellite Communications Management service that enables network managers to establish and modify satellite links/networks, adjust devices, and receive and analyze performance data on satellites and devices.	21-Mar-13
2.1.1.4	Satellite Spectrum Coordination Service	The Satellite Communications Management service that processes allocation requests between spectrum managers in the joint and non-DoD environments. This includes all unified partners.	21-Mar-13
2.1.1.5	Satellite Search Service	The Satellite Communications Management service that coordinates with Discovery services to provide the ability to search information related to satellite service on the network.	24-Mar-13
2.1.1.6	Satellite Archival Service	The Satellite Communications Management service that coordinates file storage (archival/retention) for supported network services and systems.	22-Mar-13
2.1.1.7	Satellite Performance Reporting Service	The Satellite Communications Management service that coordinates with Performance Management services to provide details on satellite service and system capacity audits and key performance indicators.	23-Mar-13
2.1.1.8	Satellite Security Control Service	The Satellite Communications Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	25-Mar-13
2.1.2	Wired Networking Services	The set of Connect Services that provide (acquire, improve, maintain) the seamless transmission of information (voice, video, or data) (through a physical connection) by using the set of communication protocols, including IP and non-IP protocols.	21-Mar-13

Number	Service	Description	AV-2 Team Reviewed
2.1.2.1	Internet Protocol (IP) Based Networking Service	The Wired Networking service that provides (acquire, improve, maintain) the seamless transmission of information (voice, video, or data) by using the set of communication protocols used for the Internet and other similar networks.	27-Jun-13
2.1.2.2	Non-IP (legacy) Based Networking Service	The Wired Networking service that provides (maintain) the seamless transmission of information (voice, video, or data) by using the set of communication protocols excluding IP.	27-Jun-13
2.1.2.3	Wired Management Service	The Wired Communications Management service that enables network managers to establish and modify wired networks, and adjust wired devices, and receive and analyze performance data on wired networks and devices.	27-Jun-13
2.1.2.4	Wired Change Management Service	The Wired Communications Management service that disseminates, coordinates, and implements change schedules affecting wired networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes.	27-Jun-13
2.1.2.5	Wired Search Service	The Wired Networking service that coordinates with Discovery services to provide the ability to search information related to wired service on the network.	27-Jun-13
2.1.2.6	Wired Archival Service	The Wired Networking service that provides file storage (archival/retention) for wired connections (Previous configuration files, log files, etc.).	27-Jun-13
2.1.2.7	Wired Performance Reporting Service	The Wired Networking service that coordinates with Performance Management services to provide details on wired service and system capacity audits and key performance indicators.	27-Jun-13
2.1.2.8	Wired Security Control Service	The Wired Networking service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	27-Jun-13

Number	Service	Description	AV-2 Team Reviewed
2.1.3	Wireless Communication Management Services	The set of Connect Services that provide (acquire, improve, maintain) communications through means such as radio frequency, microwave, or infrared (IR) that transfer information (voice, video, data) via emanations within the electromagnetic spectrum supporting IP and Non-IP (e.g. tactical) networks.	21-Mar-13
2.1.3.1	Wireless Authorization Service	The Wireless Communications Management service that coordinates wireless support requests and authorizations.	27-Jun-13
2.1.3.2	Wireless Change Management Service	The Wireless Communications Management service that disseminates, coordinates, and implements change schedules affecting satellite networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes.	27-Jun-13
2.1.3.3	Wireless Management Service	The Wireless Communications Management service that enables network managers to establish and modify wireless networks, and adjust wireless devices, and receive and analyze performance data on wireless networks and devices.	27-Jun-13
2.1.3.4	Wireless Search Service	The Wireless Communications Management service that coordinates with Discovery services to provide the ability to search information related to wireless service on the network.	27-Jun-13
2.1.3.5	Wireless Archival Service	The Wireless Communications Management service that coordinates file storage (archival/retention) for supported network services and systems.	27-Jun-13
2.1.3.6	Wireless Performance Reporting Service	The Wireless Communications Management service that coordinates with Performance Management services to provide details on wireless service and system capacity audits and key performance indicators.	27-Jun-13
2.1.3.7	Wireless Security Control Service	The Wireless Communications Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	1-Jul-13

Number	Service	Description	AV-2 Team Reviewed
2.2.	Operate Services	The set of services that enable the ability to dynamically allocate and configure networks, services and the underlying physical assets to enable situational awareness, protection and operational management of the IE. (DIEA)	21-Mar-13
2.2.1.	Spectrum Management Operations Services	The set of Operate Services that include the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations.	26-Apr-13
2.2.1.1	Spectrum Coordination Service	The Spectrum Management Operations service that processes allocation requests between spectrum managers in the joint and non-DoD environments. This includes all unified partners.	26-Apr-13
2.2.1.2	Spectrum Planning Service	The Spectrum Management Operations service that enables the production of the spectrum management plan, which provides guidance for all spectrum management functions, including information exchange, expected coordination channels, format for deliverable products, interference and reporting resolution procedures, and suggested resolution steps.	26-Apr-13
2.2.1.3	Spectrum Situation Awareness Service	The Spectrum Management Operations service that provides information pertinent to managing spectrum use, and impacts on Army operations. Displays the background electromagnetic environment and the friendly, neutral, and adversarial electromagnetic order of battle within the electromagnetic area of influence associated with a given operational area.	26-Apr-13
2.2.1.4	Spectrum Assessment Service	The Spectrum Management Operations service that provides analysis of spectrum use and the associated risks and impacts to mission capabilities.	26-Apr-13
2.2.1.5	Spectrum Allotment Service	The Spectrum Management Operations service that provides the allotment of spectrum assignments for supported wireless systems (radios, modems, sensors, etc.)	27-Apr-13

Number	Service	Description	AV-2 Team Reviewed
2.2.1.6	Spectrum Request Service	The Spectrum Management Operations service that processes requests for frequencies enabling the use of spectrum dependent devices.	28-Apr-13
2.2.1.7	Spectrum Subscription Service	The Spectrum Management Operations service that requests and receives spectrum related data from authoritative data sources. Spectrum managers require access to multiple accounts in order to request and receive spectrum related data.	29-Apr-13
2.2.1.8	Frequency Assignment Service	The Spectrum Management Operations service that assigns frequencies as authorized for a specific frequency, group of frequencies, or frequency band to be used at a certain location under specified conditions such as bandwidth, power, azimuth, duty cycle, and modulation.	30-Apr-13
2.2.1.9	Spectrum Deconfliction Service	The Spectrum Management Operations service that optimizes the usage of the electromagnetic spectrum through the investigation, avoidance, and resolution of interference hazards preventing fratricide of emitters between friendly forces.	21-Mar-13
2.2.1.10	Spectrum Configuration Control Service	The Spectrum Management Operations service that enables updates from the change and configuration management services, including releases (patches).	21-Mar-13
2.2.1.11	Spectrum Search Service	The Spectrum Management Operations service that coordinates with Discovery services to provide the ability to search information on the network relevant to spectrum management affecting networks, data assets, services, applications, and device settings.	21-Mar-13
2.2.1.12	Spectrum Archival Service	The Spectrum Management Operations service that coordinates file storage (archival/retention) for supported network services and systems.	21-Mar-13
2.2.1.13	Spectrum Performance Reporting Service	The Spectrum Management Operations service that coordinates with Performance Management services to provide details on Spectrum Management service and system capacity audits and key performance indicators.	21-Mar-13

Number	Service	Description	AV-2 Team Reviewed
2.2.1.14	Spectrum Security Control Service	The Spectrum Management Operations service that that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	21-Mar-13
2.2.2.	Change Management Services	The set of Operate Services that coordinate and disseminate configuration change schedules for networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes. (Derived from DIEA)	23-May-13
2.2.2.1	Change Schedule Service	The Change Management service that disseminates, coordinates, and implements change schedules affecting networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes.	23-May-13
2.2.2.2	Change Processing Service	The Change Management service that processes requests for change, change records, and change schedules affecting networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes.	23-May-13
2.2.2.3	Change Search Service	The Change Management service that coordinates with Discovery services to provide the ability to search information on the network relevant to change management affecting networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes.	23-May-13
2.2.2.4	Change Archival Service	The Change Management service that coordinates file storage (archival/retention) for supported network services and systems.	2-May-13
2.2.2.5	Change Management Performance Reporting	The Change Management service that coordinates with Performance Management services to provide details on Change Management service and system capacity audits and key performance indicators.	22-Mar-13

Number	Service	Description	AV-2 Team Reviewed
	Service		
2.2.2.6	Change Security Control Service	The Change Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings affecting networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes.	21-Mar-13
2.2.3	Configuration Management Services	The set of Operate Services that assure implementation, update, and management of network/platform configurations, software patches and upgrades, and hardware upgrades of components operating on the network. It ensures that all deployed IA devices and mechanisms incorporate approved features, functions, capabilities, and settings necessary to support their intended mission. This includes security critical versions, patches, interface standards, lifecycle configuration, mode and option settings, and crypto algorithms. (GIG 2.0)	23-May-13
2.2.3.1	Configuration Control Service	The Configuration Management Service that provides an interface between users and the configuration management services, and between configuration control and change management.	23-May-13
2.2.3.2	Configuration Change Schedule Service	The Configuration Management service that coordinates with Change Management services to disseminate, coordinate, and implement configuration changes for network/platforms, software patches and upgrades, and hardware upgrades of components.	23-May-13
2.2.3.3	Release Management Service	The Configuration Management Service that manages releases (to include, but not limited to, upgrades, modifications, and new software/firmware/hardware) onto the network.	23-May-13

Number	Service	Description	AV-2 Team Reviewed
2.2.3.4	Configuration Record Service	The Configuration Management service that provides output information to Computing and Data Storage Services (within the Common Operating Environment) on configuration records and the configuration management database.	18-Apr-13
2.2.3.5	Configuration Search Service	The Configuration Management Service that coordinates with Discovery services to provide the ability to search information on the network relevant to change management affecting networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes.	23-May-13
2.2.3.6	Configuration Archival Service	The Configuration Management service that coordinates file storage (archival/retention) for supported network services and systems.	18-Apr-13
2.2.3.7	Configuration Performance Reporting Service	The Configuration Management service that coordinates with Performance Management services to provide details on configuration management service and system capacity audits and key performance indicators.	23-May-13
2.2.3.8	Configuration Security Control Service	The Configuration Management Service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	24-May-13
2.2.4.	Incident Response Services	The set of Operate Services that identifies, reports, tracks and resolves information technology faults, incidents, and problems that lead to a service degradation. (ANA, GIG, ITIL). (Trouble tickets is the general term for incident and problem records).	4-Apr-13
2.2.4.1	End User Device Service	The Incident Response service that provides system administrative support to end user computing devices in order to resolve information technology faults, incidents, and problems that lead to a service degradation. (For example, remoting in to a user's device in order to perform maintenance activities.)	30-May-13

Number	Service	Description	AV-2 Team Reviewed
2.2.4.2	Incident Identification and Reporting Service	The Incident Response service that alerts, characterizes, and reports events and incident notifications from users and supported network devices and services to incident technicians.	30-May-13
2.2.4.3	Incident Resolution Service	The Incident Response service that processes workarounds and incidents records for incident technicians. (Trouble tickets is the general term for incident and problem records).	30-May-13
2.2.4.4	Incident Tracking Service	The Incident Response service that provides status reporting on incident records, incident metrics, and problem records through their lifecycles. (Trouble tickets is the general term for incident and problem records).	6-Jun-13
2.2.4.5	Incident Trend Service	The Incident Response service that generates fault, incident, and problem statistics for configuration items for the purposes of determining patterns in incidents/problems, etc. (Trouble tickets is the general term for incident and problem records).	6-Jun-13
2.2.4.6	Problem Resolution Service	The Incident Response service that processes problem records and problem resolutions for the problem manager. (Trouble tickets is the general term for incident and problem records).	4-Apr-13
2.2.4.7	Incident Search Service	The Incident Response service that coordinates with Discovery services to provide the ability to search information on the network relevant to incidents.	30-May-13
2.2.4.8	Incident Archival Service	The Incident Response service that coordinates file storage (archival/retention) for supported network services and systems.	30-May-13
2.2.4.9	Incident Response Performance Reporting Service	The Incident Response service that coordinates with Performance Management services to provide details on Incident Response service and system capacity audits and key performance indicators.	4-Apr-13
2.2.4.10	Incident Security Control Service	The Incident Response service that coordinates with NetOps Operate (Audit) and Defend services to manage malware detection, malware software, security auditing, encryption, and	30-May-13

Number	Service	Description	AV-2 Team Reviewed
		information assurance policies settings.	
2.2.5	Performance Management Services	The set of Operate Services that provide monitoring, threshold detection, performance analysis (up/down times, SLA compliance, usage rates, mean time between failure, incident resolution times, etc.) and tuning. These services also implement changes related to performance and capacity of network information systems and services. (ANA)	16-May-13
2.2.5.1	Performance Management Monitoring Service	The Performance Management Service that processes inputs from supported network services and systems on capacity audits, and key performance indicators.	16-May-13
2.2.5.2	Performance Management Improvement Service	The Performance Management Service that tunes (make minor configuration setting changes to respond to performance degradations), and implements changes related to performance and capacity of network information systems and services.	4-Apr-13
2.2.5.3	Performance Management Search Service	The Performance Management service that coordinates with Discovery services to provide the ability to search and retrieve information on the network relevant to performance management.	16-May-13
2.2.5.4	Performance Management Forecasting Service	The Performance Management service that assists the performance manager in developing capacity management plans, forecasts, and service level agreements.	16-May-13
2.2.5.5	Performance Management Archival Service	The Performance Management service that coordinates file storage (archival/retention) for supported network services and systems.	16-May-13
2.2.5.6	Performance Management Reporting	The Performance Management service that outputs details on network service and system capacity management plans, forecasts, SLAs, and key performance indicators.	16-May-13

Number	Service	Description	AV-2 Team Reviewed
	Service		
2.2.5.7	Performance Management Security Control Service	The Performance Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	16-May-13
2.2.6	Computing Infrastructure Management Services	The set of Operate Services that direct or allocate the necessary computing infrastructure and related services to allow the DoD to operate according to net-centric principles. These services ensure that adequate processing, storage, and related infrastructure services are in place to dynamically respond to computing needs and to balance loads across the infrastructure. (DIEA)	23-May-13
2.2.6.1	Computing Infrastructure Cloud Broker Service	The Computing Infrastructure Management service that coordinates cloud service allocations with DoD procured cloud service providers (through the DoD Executive Agent).	23-May-13
2.2.6.2	Computing Infrastructure Allocation Service	The Computing Infrastructure Management service that provides the ability to dynamically allocate processing and storage capacities among supporting cloud and/or dedicated data center service providers.	23-May-13
2.2.6.3	Computing Infrastructure Change Service	The Computing Infrastructure Management service that coordinates with Change Management for the processing of change schedules affecting computing infrastructure.	23-May-13
2.2.6.4	Computing Infrastructure Control Service	The Computing Infrastructure (CI) Management service that coordinates service allocations, services requests, change schedules, and operation requirements between the CI Management Services and the CI Manager.	23-May-13

Number	Service	Description	AV-2 Team Reviewed
2.2.6.5	Computing Infrastructure Requirements Service	The Computing Infrastructure Management service that processes service requests for computing infrastructure services to include computing and data storage services, and cloud services. (Note: a service request pertains to services that have already been approved for use on the network. If the request or requirement pertains to a new service, refer to the change management service.)	25-May-13
2.2.6.6	Computing Infrastructure Performance Monitoring Service	The Computing Infrastructure Management service that processes capacity management plans and key performance indicators.	4-Apr-13
2.2.6.7	Computing Infrastructure Search Service	The Computing Infrastructure Management service that coordinates with Discovery services to provide the ability to search information on the network relevant to infrastructure management.	23-May-13
2.2.6.8	Computing Infrastructure Archival Service	The Computing Infrastructure service that coordinates file storage (archival/retention) for supported network services and systems.	4-Apr-13
2.2.6.9	Computing Infrastructure Performance Reporting Service	The Computing Infrastructure Management service that coordinates with Performance Management services to provide details on Computing Infrastructure management service and system capacity audits and key performance indicators.	24-May-13
2.2.6.10	Computing Infrastructure Security Control Service	The Computing Infrastructure Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	23-May-13

Number	Service	Description	AV-2 Team Reviewed
2.2.7.	NetOps Situation Awareness Services	The set of Operate Services that provide a tailorable view of commander's critical information services status pertaining to network capabilities, performance, security, schedules, and external information feeds (e.g. from operational, intelligence, and commercial sources), and an assessment of potential impacts to achieving commanders' intent. (GIG)	6-Jun-13
2.2.7.1	NetOps Situation Awareness Management Service	The NetOps Situation Awareness service that provides Situation Awareness management of user preferences, such as subscriptions, layout, update frequencies, alerts, network visualization tables and maps, etc.	6-Jun-13
2.2.7.2	NetOps Situation Awareness Subscription Service	The NetOps Situation Awareness service that provides access to published information feeds on a one-time or recurring basis.	6-Jun-13
2.2.7.3	NetOps Situation Awareness Secure Transfer Service	The NetOps Situation Awareness service that provides access to secure transfer services that enable the secured transfer of files, data, text, web searches, etc., within and between security domains.	18-Apr-13
2.2.7.4	NetOps Situation Awareness Monitoring Service	The NetOps Situation Awareness service that provides information pertinent to operating and managing the network, to include: incident metrics, change status, release and configuration data, internal (DoD) and external (commercial) data sources relating to network operations and military operations.	19-Apr-13
2.2.7.5	NetOps Situation Awareness Search Service	The NetOps Situation Awareness service that coordinates with Discovery services to provide the ability to search information on the network.	6-Jun-13

Number	Service	Description	AV-2 Team Reviewed
2.2.7.6	NetOps Situation Awareness Archival Service	The NetOps Situation Awareness service that coordinates file storage (archival/retention) for supported network services and systems.	6-Jun-13
2.2.7.7	NetOps Situation Awareness Performance Reporting Service	The NetOps Situation Awareness service that coordinates with Performance Management services to provide details on Network Situation Awareness management service and system capacity audits and key performance indicators.	6-Jun-13
2.2.7.8	NetOps Situation Awareness Security Control Service	The NetOps Situation Awareness service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	7-Jun-13
2.2.8.	Audit Services	The set of Operate Services that perform an evaluation of a system, service, network or product (software or device) in order to ascertain the validity, reliability, and security of information and to provide an assessment of a system's/service's internal control.	20-Apr-13
2.2.8.1	Security Event Management Service	The Audit Service that provides security event monitoring and notification services, and manages a security event database to include generating, transmitting, storing, analyzing, and disposing of computer security log data, for future and predictive evaluation. (Derived from NIST SP 800-92)	21-Apr-13
2.2.8.2	Asset Management Service	The Audit Service that identifies, tracks, monitors and reports on the transfer and allocation of IT assets (e.g. radios, servers, storage and processing devices, software, firmware), and creates, edits, and displays asset log data. Additionally the service identifies and tracks organizational responsibilities for managing, securing, and using IT assets (to include details on	15-Mar-13

Number	Service	Description	AV-2 Team Reviewed
		individual points of contact).	
2.2.8.3	Audit Management Service	The Audit Service that enables managers to conduct audits through the development and promulgation of audit scripts, instructions, plans, etc.	11-Apr-13
2.2.8.4	Audit Search Service	The Audit service that coordinates with Discovery services to provide the ability to search information on the network.	30-May-13
2.2.8.5	Audit Archival Service	The Audit service that coordinates file storage (archival/retention) for supported network services and systems.	30-May-13
2.2.8.6	Audit Performance Reporting Service	The Audit service that coordinates with Performance Management services to provide details on audit services and system capacity audits and key performance indicators.	30-May-13
2.2.8.7	Audit Security Control Service	The Audit service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	30-May-13
2.2.9	Information Resource Planning Services	The set of Operate Services that support planning of budgeting, and controlling of information resources throughout their life-cycle through the creation, modification, and monitoring of service level agreements, organizational level agreements, and monitoring of performance indicators.	21-Mar-13
2.2.9.1	Information Resource Planning Service Level Agreement Service	The Information Resource Planning service that through the creation, modification, and monitoring of service level agreements (agreements EXTERNAL to the Army pertaining to network service performance and responsibilities) supports planning of budgeting, manipulating, and controlling of information throughout its life-cycle.	30-May-13

Number	Service	Description	AV-2 Team Reviewed
2.2.9.2	Information Resource Planning Search Service	The Information Resource Planning service that coordinates with Discovery services to provide the ability to search information on the network.	27-Jun-13
2.2.9.3	Information Resource Planning Archival Service	The Information Resource Planning service that coordinates file storage (archival/retention) for supported network services and systems.	27-Jun-13
2.2.9.4	Information Resource Planning Performance Reporting Service	The Information Resource Planning service that coordinates with Performance Management services to provide details on and service level agreements and organizational level agreements.	27-Jun-13
2.2.9.5	Information Resource Planning Security Control Service	The Information Resource Planning service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	27-Jun-13
3	Net Assurance: Access & Defend Services	The NetOps Services that protect information and information assets by detecting, reporting, and resolving security issues; and provides the ability and means to communicate (to both human and machine users) with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions (derived from CNSSI 4009).	6-Jun-13
3.1	Access Services	The set of services that provides the ability and means to communicate (to both human and machine users) with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions	30-May-13

Number	Service	Description	AV-2 Team Reviewed
		(derived from CNSSI 4009).	
3.1.1	Access Control Services	The set of Access Services that provide the process of granting or denying specific requests for obtaining and using information and related information processing services (derived from CNSSI 4009). This provides users the benefit of being able to log in to multiple applications with a reduced number of verifications, and in some cases only one verification.	13-Jun-13
3.1.1.1	Access Authorization Service	The Access Control service that monitors and grants access privileges for other authorized entities (derived from CNSSI 4009).	13-Jun-13
3.1.1.2	Access Policy Service	The Access Control service that establishes and enforces Information Assurance policies (such as password configurations, login credentials, login attempts, one verification log-in, etc.) applicable to access control for person and non-person entities.	13-Jun-13
3.1.1.3	Access Privilege Management Service	The Access Control service that creates and updates access privilege databases.	13-Jun-13
3.1.1.4	Access Search Service	The Access Control service that coordinates with Discovery services to provide the ability to search information on the network.	13-Jun-13
3.1.1.5	Access Archival Service	The Access Control service that coordinates file storage (archival/retention) for supported network services and systems.	30-May-13
3.1.1.6	Access Performance Reporting Service	The Access Control service that provides details on access management service, system capacity audits and key performance indicators.	30-May-13

Number	Service	Description	AV-2 Team Reviewed
3.1.1.7	Access Security Control Service	The Access Control service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	11-Apr-13
3.1.2	Identification and Authentication (IAW DoDI 8520.03) Services	The set of Access Services that manages the identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others and verifies the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data (derived from CNSSI 4009).	11-Apr-13
3.1.2.1	Identity Management Service	The Identification and Authentication (IAW DoDI 8520.03) Service that manages the identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others (derived from CNSSI 4009).	13-Jun-13
3.1.2.2	Attribute Management Service	The Identification and Authentication(IAW DoDI 8520.03) Service that distributes DoD person, persona (role) and personnel attributes to applications and services in a controlled, consistent, and secure manner.	18-Apr-13
3.1.2.3	Credential Management Service	The Identification and Authentication (IAW DoDI 8520.03) Service that provides (acquire, modify, upgrade) network entry points and monitors authentication (IAW DoDI 8520.03) information changes.	11-Apr-13
3.1.2.4	Authentication (IAW DoDI 8520.03) Management Service	The Identification and Authentication (IAW DoDI 8520.03) Service that verifies the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data (derived from CNSSI 4009).	13-Jun-13

Number	Service	Description	AV-2 Team Reviewed
3.1.2.5	Identification Release Management Service	The Identification and Authentication (IAW DoDI 8520.03) service that coordinates with Configuration Management services to manage identification releases.	11-Apr-13
3.1.2.6	Identification Search Service	The Identification and Authentication (IAW DoDI 8520.03) service that coordinates with Discovery services to provide the ability to search information on the network.	11-Apr-13
3.1.2.7	Identification Archival Service	The Identification and Authentication (IAW DoDI 8520.03) service that coordinates file storage (archival/retention) for supported network services and systems.	11-Apr-13
3.1.2.8	Identification Performance Reporting Service	The Identification and Authentication (IAW DoDI 8520.03) Service that coordinates with Performance Management services to provide details on capacity audits and key performance indicators for identification management services.	11-Apr-13
3.1.2.9	Identification Security Control Service	The Identification and Authentication (IAW DoDI 8520.03) service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	11-Apr-13
3.2	Defend Services	The set of services that provides the functionality required to ensure data and services are secured and trusted across DoD.	30-May-13
3.2.1	Security Metadata Management Services	The set of Defend Services that provide (acquire, improve, maintain) the ability to mark a data asset to accurately reflect the security classification or sensitivity guidance required (e.g., classification, dissemination controls, releasability, declassification) so that it can be identified and inform authorization and dissemination decisions.	13-Jun-13
3.2.1.1	Metadata Marking Rules Service	The Security Metadata Management service that provides security rule sets pertaining to classification and declassification metadata tags.	13-Jun-13

Number	Service	Description	AV-2 Team Reviewed
3.2.1.2	Metadata Security Management Service	The Security Metadata Management service that provides support to developing security rule sets based on IA policies.	13-Jun-13
3.2.1.3	Metadata Search Service	The Security Metadata Management service that coordinates with Discovery services to provide the ability to search information on the network.	23-May-13
3.2.1.4	Metadata Archival Service	The Security Metadata Management service that coordinates file storage (archival/retention) for supported network services and systems.	23-May-13
3.2.1.5	Metadata Performance Reporting Service	The Security Metadata Management service that coordinates with Performance Management services to provide details on Security metadata Management service and system capacity audits and key performance indicators.	23-May-13
3.2.1.6	Metadata Security Control Service	The Security Metadata Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	23-May-13
3.2.2	Cryptography Management Services	The set of Defend Services that manage the allocation, distribution, maintenance and use of cryptographic keying and encryption material. (Derived from DIEA)	30-May-13
3.2.2.1	Cryptography Management Encryption Key Service	The Cryptography Management service that provides encryption key dissemination to supported network services.	30-May-13
3.2.2.2	Cryptography Management Search Service	The Cryptography Management service that provides the ability to securely search and retrieve information on encryption keys. (For example: determine which keys are available to support a specific coalition environment.)	31-May-13

Number	Service	Description	AV-2 Team Reviewed
3.2.2.3	Cryptography Management Archival Service	The Cryptography Management service that coordinates file storage (archival/retention) for supported network services and systems.	31-May-13
3.2.2.4	Cryptography Management Performance Reporting Service	The Cryptography Management service that coordinates with Performance Management services to provide details on Cryptographic Management service and system capacity audits and key performance indicators.	30-May-13
3.2.2.5	Cryptography Management Security Control Service	The Cryptography Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	30-May-13
3.2.3	Secure Transfer Services	The set of Defend Services that supply the functional capabilities necessary to ensure secure file transfer within and across disparate security domains.	13-Jun-13
3.2.3.1	Secure Transfer Disseminate Service	The Secure Transfer service that secures (encrypts) and forwards data to intended audiences within or across security domains.	13-Jun-13
3.2.3.2	Secure Transfer Configuration Service	The Secure Transfer service that enables updates from the change and configuration management services, including releases (patches).	30-May-13
3.2.3.3	Secure Transfer Search Service	The Secure Transfer service that coordinates with Discovery services to provide the ability to search information on the network.	30-May-13
3.2.3.4	Secure Transfer Archival Service	The Secure Transfer service that coordinates file storage (archival/retention) for supported network services and systems.	30-May-13
3.2.3.5	Secure Transfer Performance Reporting Service	The Secure Transfer service that coordinates with Performance Management services to provide details on Secure Transfer service and system capacity audits and key performance indicators.	30-May-13

Number	Service	Description	AV-2 Team Reviewed
3.2.3.6	Secure Transfer Security Control Service	The Secure Transfer service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	30-May-13
3.2.4	Information Assurance Management Services	The set of Defend Services that defend information and information systems by ensuring their availability, integrity, authentication (IAW DoDI 8520.03), confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (derived from CNSSI 4009).	13-Jun-13
3.2.4.1	Information Assurance Vulnerability Analysis Service	The Information Assurance service that alerts personnel to vulnerability analyses and changes in information operations condition postures, and recommends corrective action to mitigate potential threats.	13-Jun-13
3.2.4.2	Information Assurance Policy Service	The Information Assurance service that promulgates malware definitions, malware software, and information assurance policies (including risk mitigation rules and other rules based on INFOCONs) to supported network services and systems (devices).	13-Jun-13
3.2.4.3	Information Assurance Threat Mitigation Response Service	The Information Assurance service that implements corrective actions to reduce the impact of IA threats and potential threat to network services, systems, and devices.	13-Jun-13
3.2.4.4	Information Assurance Search Service	The Information Assurance service that coordinates with Discovery services to provide the ability to search information on the network.	30-May-13
3.2.4.5	Information Assurance Archival Service	The Information Assurance service that coordinates file storage (archival/retention) for supported network services and systems.	13-Jun-13

Number	Service	Description	AV-2 Team Reviewed
3.2.4.6	Information Assurance Management Performance Reporting Service	The Information Assurance service that coordinates with Performance Management services to provide details on Information Assurance service and system capacity audits and key performance indicators.	30-May-13
3.2.4.7	Information Assurance Security Control Service	The Information Assurance Management service that coordinates with NetOps Operate and Defend services to manage malware detection, malware software, security auditing, encryption, and information assurance policies settings.	13-Jun-13

Section 2: NetOps Service Alignments

The purpose of this section is to provide program managers and others with a quick reference guide that depicts how NetOps services support Joint and Army capabilities and activities, and show a cross reference to NetOps services in this AV-2 to the NetOps services previously described by Communities of Interest. It also shows how NetOps services align to industry descriptions such as the Information Technology Infrastructure Library (ITIL) and the Telemangement Forum Framework. It also depicts a fit-for-purpose view of various DoDAF models presented together.

Table A-2 – NetOps Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	0	NetOps Services	Technical capabilities for managing, operating and defending the Army's portion of the GIG.		
CV-7 Service to Capability Mapping	Joint References	JCA	Net Centric	GIG 2.0 ORA	A5.2 Enable GIG C2 through NetOps	SvcV-5 Service to Activity Mapping
		DOD IEA	NA	ANA Operational Activity	NetOps	
		NMA	3.2.2 Network Management	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Network Management Service (NMS-NetMan)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	NetOps	Enterprise Services		
		Cyber	DOD Information Network Operations	Cybersecurity		
	Industry References	ITIL	IT Service Mgt (ITSM)	Joint Command and Control		
		TM Forum	Applications	Data Center Consolidation		

Table A-3 - Content Management Share Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	1	Content Management: Share Services	The set of NetOps services that provide the functionality required to enable information and information assets to be used within and across mission areas (DIEA), through monitoring, managing, and facilitating the visibility and accessibility of information within and across the LandWarNet (derived from GIG 2.0).		
CV-7 Service to Capability Mapping	Joint References	JCA	5.2.3 Share Knowledge and Situational Awareness	GIG 2.0 ORA	A2.1.2 Share Information	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.3 Share Services	ANA Operational Activity	To Be Determined	
		NMA	2.2 Information & Data Management Capability Area	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Enterprise Services and Applications Management (1)	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Information Dissemination Mgt/Content Staging (1)	Data Strategy Implementation		
		Cyber	Content Management	Document Management		
	Industry References	ITIL	Knowledge Management	Joint Use Applications		
		TM Forum	Knowledge Management	Section 508 Disabilities Access		

Table A-4 - Directory Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	1.1	Directory Management Services	The set of Share Services that provide (acquire, improve, maintain) a shared information infrastructure for locating, managing, administering, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects.		
CV-7 Service to Capability Mapping	Joint References	JCA	5.2.2.3 Define Knowledge Structure	GIG 2.0 ORA	A1.3.1 Manage Enterprise Directory	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.2.3 Directory Management Services	ANA Operational Activity	Not Applicable	
		NMA	2.1.2 Directory	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Active Directory Services Mgt (2)	Joint Use Applications		DOD CIO CPG Priorities
		NetOps IPT	Directory Services (3)	Enterprise Services		
		Cyber	To be determined	Data Strategy Implementation		
	Industry References	ITIL	Knowledge Management	Section 508 Disabilities Access		
		TM Forum	Not Applicable	0		

Table A-5 - Content Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	1.2.	Content Management Services	The set of Share Services that collect, manage, discover, cache, distribute, retrieve, subscribe, share and publish information in any form or medium. (Derived from DIEA and GIG 2.0)		
CV-7 Service to Capability Mapping	Joint References	JCA	5.2.2.3 Define Knowledge Structure	GIG 2.0 ORA	A5.2.4 Conduct GIG Content Management (GCM)	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.3.1 Content Management Services	ANA Operational Activity	Manage Knowledge Base	
		NMA	2.2.2 Content Management	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Global Content Management Services (GCMS)	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Information Computing (2)	Data Strategy Implementation		
		Cyber	Content Management	Joint Use Applications		
	Industry References	ITIL	Knowledge Management	Section 508 Disabilities Access		
		TM Forum	Content Management	0		

Table A-6 - Content Collection Service Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	1.2.3	Content Collection Service	The Content Management service that collects (pulls) data from other NetOps services for discovery and publication purposes.		
CV-7 Service to Capability Mapping	Joint References	JCA	5.2.2.3 Define Knowledge Structure	GIG 2.0 ORA	A2.1.2 Share Information	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.3.1.1 Content Discovery Services	ANA Operational Activity	Manage Knowledge Base	
		NMA	2.2.2.1 Collection	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	0	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	To Be Determined	Data Strategy Implementation		
		Cyber	Not applicable	Document Management		
	Industry References	ITIL	Knowledge Management	Joint Use Applications		
		TM Forum	CM Distribution & Acquisition	Section 508 Disabilities Access		

Table A-7 - Enterprise Management Connect & Operate Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.	Enterprise Management: Connect & Operate Services	The set of NetOps services that provide the functionality required to support near-real-time operational management of the LandWarNet to include situational awareness, computing infrastructure management, change and configuration control, and end user support (incident and problem resolution)		
CV-7 Service to Capability Mapping	Joint References	JCA	6.3 Net Management	GIG 2.0 ORA	A5.2.2 Provide GIG Enterprise Management (GEM)	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.1 Operate Services	ANA Operational Activity	Operate	
		NMA	3.0 Network Operations & Security LOE	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Enterprise Support (1)	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Network Mgt/Enterprise Svc Management (1)	Network Optimization/ Normalization		
		Cyber	Network Management.	Joint Use Applications		
	Industry References	ITIL	Service Operations	Section 508 Disabilities Access		
		TM Forum	Service Mgt & Ops	0		

Table A-8 - Connect Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.1	Connect Services	The set of services that provides (acquires, improves, maintains) the ability for any user or service to reach any other or identify and use any other service.		
CV-7 Service to Capability Mapping	Joint References	JCA	6.1 Information Transport	GIG 2.0 ORA	A3.2.2 Provide Global Connectivity to Support the warfighter	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.1 Connect Services	ANA Operational Activity	Produce Technical Solutions	
		NMA	1.1 Transport	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	IP Transport Management (1)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Not Applicable	Communications Transport and DISN		
		Cyber	To be determined	Enterprise Services		
	Industry References	ITIL	Operate Services	Commercial Mobile Solutions		
		TM Forum	Data, Radio, Transport	Section 508 Disabilities Access		

Table A-9 - Satellite Communication Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.1.1	Satellite Communication Management Services	The set of Connect Services that provide (acquire, improve, maintain) telecommunications through the use of communications satellites.		
CV-7 Service to Capability Mapping	Joint References	JCA	6.1 Information Transport	GIG 2.0 ORA	A5.2.2.9 Provide Satellite Communications Management	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.1.1 Commercial Satellite Communication Services	ANA Operational Activity	Produce Technical Solutions	
		NMA	1.1.1 Operational Transport	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	SATCOM Management Service (SMS)	Commercial Mobile Solutions		DOD CIO CPG Priorities
		NetOps IPT	Satcom Net Mgt (2)	Network Optimization/ Normalization		
		Cyber	Satellite Communications Management	Enterprise Services		
	Industry References	ITIL	N/A	Position, Navigation and Timing (PNT)		
		TM Forum	Radio	Section 508 Disabilities Access		

Table A-10 - Wired Networking Services Alignments

		Number	Name	Description		
AV-2	Service Definition	2.1.2	Wired Networking Services	The set of Connect Services that provide (acquire, improve, maintain) the seamless transmission of information (voice, video, or data) (through a physical connection) by using the set of communication protocols, including IP and non-IP protocols.		
CV-7	Joint References	JCA	6.1.1 Wired Transmission	GIG 2.0 ORA	A3.2.2 Provide Global Connectivity to Support the warfighter	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.1.5 Wired Communication Services	ANA Operational Activity	Produce Technical Solutions	
		NMA	1.1.2 Institutional Transport	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	0	Communications Transport and DISN		DOD CIO CPG Priorities
		NetOps IPT	Wired Net Mgt (2)	Network Optimization/ Normalization		
		Cyber	To be determined	Joint Use Applications		
	Industry References	ITIL	N/A	Section 508 Disabilities Access		
		TM Forum	Transport	0		

Table A-11 - Wireless Communication Services Alignments

		Number	Name	Description			
AV-2 Service Definition	Service	2.1.3	Wireless Communication Management Services	The set of Connect Services that provide (acquire, improve, maintain) communications through means such as radio frequency, microwave, or infrared (IR) that transfer information (voice, video, data) via emanations within the electromagnetic spectrum supporting IP and Non-IP (e.g. tactical) networks.			
CV-7 Service to Capability Mapping	Joint References	JCA	6.3.2 Deployable Scalable and Modular Networks	GIG 2.0 ORA	A3.2.2 Provide Global Connectivity to Support the warfighter	SvcV-5 Service to Activity Mapping	
		DOD IEA	S1.1.4 Wireless Communication Services	ANA Operational Activity	Produce Technical Solutions		
		NMA	1.1.1 Operational Transport	Defense Spectrum	0		
Cross Reference	COI Term	NETCOM	Wireless IP Network Management (2)	Network Optimization/ Normalization		DOD CIO CPG Priorities	
		NetOps IPT	Radio Net Mgt (2)	Communications Transport and DISN			
		Cyber	Network Management.	Commercial Mobile Solutions			
	Industry References	ITIL	N/A	Enterprise Services			
		TM Forum	Radio	Section 508 Disabilities Access			

Table A-12 - Operate Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.	Operate Services	The set of services that enable the ability to dynamically allocate and configure networks, services and the underlying physical assets to enable situational awareness, protection and operational management of the IE. (DIEA)		
CV-7 Service to Capability Mapping	Joint References	JCA	6.3.4 Cyber Management	GIG 2.0 ORA	A5.2.2 Provide GIG Enterprise Management (GEM)	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.1 Operate Services	ANA Operational Activity	Operate	
		NMA	3.2 Operate the Network	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	IT Systems Management Service (SysMan)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Not Applicable	Enterprise Services		
		Cyber	0	Joint Command and Control		
	Industry References	ITIL	Service Operations	Joint Use Applications		
		TM Forum	Service Management Domain	Section 508 Disabilities Access		

Table A-13 - Spectrum Management Operations Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.1.	Spectrum Management Operations Services	The set of Operate Services that include the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations.		
CV-7 Service to Capability Mapping	Joint References	JCA	6.3.3 Spectrum Management	GIG 2.0 ORA	A5.2.2.8 Provide Joint Spectrum Management	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.1.4 Wireless Communication Services	ANA Operational Activity	Manage Electromagnetic Spectrum Situation Awareness	
		NMA	3.2.1.1 Functional Interoperability with Unified Action Partners	Defense Spectrum	A3 Perform SM Operations	
Cross Reference	COI Term	NETCOM	Spectrum/Frequency Mgt Service (SFMS)	Spectrum		DOD CIO CPG Priorities
		NetOps IPT	Frequency Mgt (2)	Joint Use Applications		
		Cyber	Electromagnetic Spectrum Operations	Joint Command and Control		
	Industry References	ITIL	Service Operations	0		
		TM Forum	Radio	0		

Table A-14 - Change Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.2	Change Management Services	The set of Operate Services that coordinate and disseminate configuration change schedules for networks, data assets, services, applications, and device settings in conformance with standard change and configuration processes. (Derived from DIEA)		
CV-7 Service to Capability Mapping	Joint References	JCA	6.3.1.2 Rapid Configuration Change	GIG 2.0 ORA	A5.2.2.3 Provide Change Management	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.1.1 Change Management Services	ANA Operational Activity	Manage Change	
		NMA	3.2.2.6 Rapid Configuration Change	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Configuration Mgt Database Support Service (2)*	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Network Change Management (3)	Joint Use Applications		
		Cyber	To Be Determined	Section 508 Disabilities Access		
	Industry References	ITIL	Change Management	0		
		TM Forum	Strategic and Enterprise Planning	0		

Table A-15 - Configuration Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.3	Configuration Management Services	The set of Operate Services that assure implementation, update, and management of network/platform configurations, software patches and upgrades, and hardware upgrades of components operating on the network. It ensures that all deployed IA devices and mechanisms incorporate approved features, functions, capabilities, and settings necessary to support their intended mission. This includes security critical versions, patches, interface standards, lifecycle configuration, mode and option settings, and crypto algorithms. (GIG 2.0)		
CV-7 Service to Capability Mapping	Joint References	JCA	6.3.1.2 Rapid Configuration Change	GIG 2.0 ORA	A5.2.2.4 Provide Configuration Control	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.1.1 Change Management Services	ANA Operational Activity	Manage Configuration	
		NMA	3.2.2.6 Rapid Configuration Change	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Enterprise Services Mgt System/Service (ESMS2)	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Net Config Mgt (2)	Joint Use Applications		
		Cyber	To Be Determined	Section 508 Disabilities Access		
	Industry References	ITIL	IT Asset and Configuration Mgt	0		
		TM Forum	Enable Service Configuration & Activation	0		

Table A-16 - Incident Response Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.4	Incident Response Services	The set of Operate Services that identifies, reports, tracks and resolves information technology faults, incidents, and problems that lead to a service degradation. (ANA, GIG, ITIL)		
CV-7 Service to Capability Mapping	Joint References	JCA	4.3.1 Inspect	GIG 2.0 ORA	A5.3.2.3 Respond to GiG Situation; A5.2.3.7 Perform Threat/ Incident Management	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.1.7 End User Device Services	ANA Operational Activity	Manage Incident	
		NMA	2.3.2 Service Desk	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	To Be Determined	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Net Ops Service Delivery (2)	Joint Use Applications		
		Cyber	To Be Determined	Cybersecurity		
	Industry References	ITIL	Incident Management	0		
		TM Forum	Service Mgt & Ops	Section 508 Disabilities Access		

Table A-17 - Performance Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.5	Performance Management Services	The set of Operate Services that provide monitoring, threshold detection, performance analysis (up/down times, SLA compliance, usage rates, mean time between failure, incident resolution times, etc.) and tuning. These services also implement changes related to performance and capacity of network information systems and services. (ANA)		
CV-7 Service to Capability Mapping	Joint References	JCA	6.3.1 Optimized Network Functions and Resources	GIG 2.0 ORA	A5.2.2.7 Provide Performance Management	SvcV-5 Service to Activity Mapping
		DOD IEA	S3.3 Monitoring and Compliance Services	ANA Operational Activity	Manage Performance	
		NMA	3.2.2.7 Performance Management	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Service Level Manager (2)*	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Manage Network Performance Data (3)	Joint Use Applications		
		Cyber	To Be Determined	Data Strategy Implementation		
	Industry References	ITIL	Performance Management	Network Optimization/ Normalization		
		TM Forum	Service Performance Management	Section 508 Disabilities Access		

Table A-18 - Computing Infrastructure Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.6	Computing Infrastructure Management Services	The set of Operate Services that direct or allocate the necessary computing infrastructure and related services to allow the DoD to operate according to net-centric principles. These services ensure that adequate processing, storage, and related infrastructure services are in place to dynamically respond to computing needs and to balance loads across the infrastructure. (DIEA)		
CV-7 Service to Capability Mapping	Joint References	JCA	6.2.1.2.1 Shared Computing Infrastructure	GIG 2.0 ORA	A3.1 Provide Computing Infrastructure	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.3.6.2 Infrastructure as a Service	ANA Operational Activity	Manage Capacity	
		NMA	1.2 Computing	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	IAVM Computing Platform Management (2)	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Not Applicable	Joint Use Applications		
		Cyber	To Be Determined	Data Center Consolidation		
	Industry References	ITIL	Service Operations	Network Optimization/ Normalization		
		TM Forum	Not Applicable	Section 508 Disabilities Access		

Table A-19 - NetOps Situation Awareness Services Alignment

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.7	NetOps Situation Awareness Services	The set of Operate Services that provide a tailorable view of commander's critical information services status pertaining to network capabilities, performance, security, schedules, and external information feeds (e.g. from operational, intelligence, and commercial sources), and an assessment of potential impacts to achieving commanders' intent. (GIG)		
CV-7 Service to Capability Mapping	Joint References	JCA	2 Battlespace Awareness	GIG 2.0 ORA	A5.2.1 Manage GIG Situational Awareness	SvcV-5 Service to Activity Mapping
		DOD IEA	S3.3 Monitoring and Compliance Services	ANA Operational Activity	Manage Situation Awareness	
		NMA	3.2.2.10 Realtime NW Awareness (for Network Management)	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Network Common Op Picture, Sit Aware, Risk Mgt (2)	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Net Monitoring (2)	Joint Use Applications		
		Cyber	Cyberspace Situational Awareness	Joint Command and Control		
	Industry References	ITIL	Service Operations	Network Optimization/ Normalization		
		TM Forum	Not Applicable	Section 508 Disabilities Access		

Table A-20 - Audit Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.8	Audit Services	The set of Operate Services that perform an evaluation of a system, service, network or product (software or device) in order to ascertain the validity, reliability, and security of information and to provide an assessment of a system's/service's internal control.		
CV-7 Service to Capability Mapping	Joint References	JCA	9.1.2 Audit, Inspection and Investigation	GIG 2.0 ORA	A4.1.3 Develop GIG Audit Requirements Policy	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.3.8 Audit Services	ANA Operational Activity	Manage IT Asset	
		NMA	3.2.1.2.1 Asset Visibility	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	IAVM IP Network IP Vulnerability Scanner (2)*	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Not Applicable	Enterprise Services		
		Cyber	To Be Determined	Joint Use Applications		
	Industry References	ITIL	Audit	0		
		TM Forum	Detect Potential Security Threats	0		

Table A-21 - Information Resource Planning Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	2.2.9	Information Resource Planning Services	The set of Share Services that support planning of budgeting, and controlling of information resources throughout their life-cycle through the creation, modification, and monitoring of service level agreements, organizational level agreements, and monitoring of performance indicators.		
CV-7 Service to Capability Mapping	Joint References	JCA	9.3 Information Management	GIG 2.0 ORA	A2.2 Provide Information Infrastructure	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.3.2 Information Management Services	ANA Operational Activity	Determine Information Requirements	
		NMA	0	Defense Spectrum	S1.3.1 Content Management Services	
Cross Reference	COI Term	NETCOM	Information Staging Mgt (2)	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Information Dissemination Mgt/Content Staging (1)	Adaptive Planning and Execution (APEX)		
		Cyber	Information Dissemination Management	Joint Command and Control		
	Industry References	ITIL	Knowledge Management	Joint Use Applications		
		TM Forum	Service Configuration Management	Section 508 Disabilities Access		

Table A-22 - Net Assurance Access & Defend Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.	Net Assurance: Access & Defend Services	The NetOps Services that protect information and information assets by detecting, reporting, and resolving security issues; and provides the ability and means to communicate (to both human and machine users) with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions (derived from CNSSI 4009).		
CV-7 Service to Capability Mapping	Joint References	JCA	6.4 Information Assurance	GIG 2.0 ORA	A5.2.3 Conduct GIG Network Defense (GND)	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.2 Defend Services	ANA Operational Activity	Defend	
		NMA	3.0 Network Operations & Security LOE	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Network Access Control Service (NAC)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Security Management (1)	Enterprise Services		
		Cyber	Network Assurance	Cybersecurity		
	Industry References	ITIL	Information Security Management	Joint Use Applications		
		TM Forum	Security Mgt	Section 508 Disabilities Access		

Table A-23 - Access Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.1	Access Services	The set of services that provides the ability and means to communicate (to both human and machine users) with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions (derived from CNSSI 4009).		
CV-7 Service to Capability Mapping	Joint References	JCA	6.4.1.1 Assure Access	GIG 2.0 ORA	A1.2 Provide Joint / Enterprise Level Access Control	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.2 Access Services	ANA Operational Activity	Manage Access	
		NMA	3.1.4.2 Secure Access	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Network Access control (2)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Computing Environment Defense (2)	Enterprise Services		
		Cyber	To be determined	Cybersecurity		
	Industry References	ITIL	Access Mgt	Joint Use Applications		
		TM Forum	PKI & Digital Certificates	Section 508 Disabilities Access		

Table A-24 - Access Control Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.1.1	Access Control Services	The set of Access Services that provide the process of granting or denying specific requests for obtaining and using information and related information processing services (derived from CNSSI 4009). This provides users the benefit of being able to log in to multiple applications with a reduced number of verifications, and in some cases only one verification.		
CV-7 Service to Capability Mapping	Joint References	JCA	6.4.1.1 Assure Access	GIG 2.0 ORA	A1.2 Provide Joint / Enterprise Level Access Control	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.2 Access Services	ANA Operational Activity	Manage Access	
		NMA	3.1.4.2 Secure Access	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Network Access control (2)	Cybersecurity		DOD CIO CPG Priorities
		NetOps IPT	Computing Environment Defense (2)	Enterprise Services		
		Cyber	To be determined	Section 508 Disabilities Access		
	Industry References	ITIL	Access Mgt	Joint Use Applications		
		TM Forum	PKI and Digital Certificates	0		

Table A-25 - Identity and Authentication Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.1.2	Identification and Authentication (IAW DoDI 8520.03) Services	The set of Access Services that manages the identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others and verifies the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data (derived CNSSI 4009).		
CV-7 Service to Capability Mapping	Joint References	JCA	6.2.2.4 Content Delivery	GIG 2.0 ORA	A1.1 Provide Joint / Enterprise Level Identity Management and Authentication	SvcV-5 Service to Activity Mapping
		DOD IEA	S1.2.2 Identification and Authentication Services	ANA Operational Activity	Manage Identity	
		NMA	3.1.4.2.1 Authentication	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Identity Management Services (IDMan)	Enterprise Services		DOD CIO CPG Priorities
		NetOps IPT	Identity Management Services (2)	Joint Use Applications		
		Cyber	To Be Determined	Cybersecurity		
	Industry References	ITIL	Access Mgt	Section 508 Disabilities Access		
		TM Forum	Employee Identity Mgt	0		

Table A-26 - Defend Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.2	Defend Services	The set of services that provides the functionality required to ensure data and services are secured and trusted across DoD.		
CV-7 Service to Capability Mapping	Joint References	JCA	6.4.2 Protect Data and Networks	GIG 2.0 ORA	A5.2.3 Conduct GIG Network Defense (GND)	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.2 Defend Services	ANA Operational Activity	Defend	
		NMA	3.1.4 Protect	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Host Security Services (HSS), Network Intrusion Prevention Services (NIPS), Wireless Intrusion Prevention Services (WIPS), Security Incident & Event Management Services (SIEMS), Insider Threat Management Services(ITM)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Security Supporting Infrastructure Defense (2)	Joint Use Applications		
		Cyber	Defensive Cyberspace Operations	Cybersecurity		
	Industry References	ITIL	Information Security Management	0		
		TM Forum	Security Management	0		

Table A-27 - Security Metadata Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.2.1	Security Metadata Management Services	The set of Defend Services that provide (acquire, improve, maintain) the ability to mark a data asset to accurately reflect the security classification or sensitivity guidance required (e.g., classification, dissemination controls, releasability, declassification) so that it can be identified and inform authorization and dissemination decisions.		
CV-7 Service to Capability Mapping	Joint References	JCA	2.1.3.1 Data Transformation	GIG 2.0 ORA	A4.3.5 Define and Develop Data/Service Standards	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.2.1 Security Metadata Management Services	ANA Operational Activity	Protect Networks And Services	
		NMA	2.1.5.3 Indexing/Metadata Tagging	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	To Be Determined	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	File Security Management (3)	Joint Use Applications		
		Cyber	To Be Determined	Cybersecurity		
	Industry References	ITIL	Information Security Management	0		
		TM Forum	Not Applicable	0		

Table A-28 - Cryptographic Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.2.2.	Cryptography Management Services	The set of Defend Services that manage the allocation, distribution, maintenance and use of cryptographic keying and encryption material. (Derived from DIEA)		
CV-7 Service to Capability Mapping	Joint References	JCA	6.4.1 Secure Information Exchange	GIG 2.0 ORA	A4.3.2 Define and Develop IA Standards	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.2.3 Cryptography Management Services	ANA Operational Activity	Protect Networks And Services	
		NMA	3.1.4.3 Secure Information & Exchange	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Cryptographic Security Management Service (CSMS)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Network Encryption (3)	Joint Use Applications		
		Cyber	To Be Determined	Cybersecurity		
	Industry References	ITIL	Information Security Management	0		
		TM Forum	Not Applicable	0		

Table A-29 - Secure Transfer Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.2.3.	Secure Transfer Services	The set of Defend Services that supply the functional capabilities necessary to ensure secure file transfer within and across disparate security domains.		
CV-7 Service to Capability Mapping	Joint References	JCA	6.4.1 Secure Information Exchange	GIG 2.0 ORA	A5.2.3.1 Provide Secure Transfer Services	SvcV-5 Service to Activity Mapping
		DOD IEA	A2.3.4.2 Standardize Data-in-Transit Protection	ANA Operational Activity	Protect Networks And Services	
		NMA	3.1.4.3 Secure Information & Exchange	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Multi-level Classification Mgt (2)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Enclave / Boundary Defense (2)	Joint Use Applications		
		Cyber	To Be Determined	Cybersecurity		
	Industry References	ITIL	Information Security Management	Communications Transport and DISN		
		TM Forum	Transport	0		

Table A-30 - Information Assurance Management Services Alignments

		Number	Name	Description		
AV-2 Service Definition	Service	3.2.4	Information Assurance Management Services	The set of Defend Services that defend information and information systems by ensuring their availability, integrity, authentication (IAW DoDI 8520.03), confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (derived from CNSSI 4009).		
CV-7 Service to Capability Mapping	Joint References	JCA	3.1.4.7 Cyberspace (MTS)	GIG 2.0 ORA	A4.2.9 Develop IA Policy	SvcV-5 Service to Activity Mapping
		DOD IEA	S2.2.2 Information Assurance Management Services	ANA Operational Activity	Implement Information Operations Condition	
		NMA	3.1.4 Protect	Defense Spectrum	0	
Cross Reference	COI Term	NETCOM	Backup & Recovery Management Service (B&RMS)	Network Optimization/ Normalization		DOD CIO CPG Priorities
		NetOps IPT	Network Infrastructure Defense (2)	Joint Use Applications		
		Cyber	To Be Determined	Cybersecurity		
	Industry References	ITIL	Information Security Management	0		
		TM Forum	Vulnerability Management	0		

Glossary of Acronyms

ANA: Army NetOps Architecture
AV: All Viewpoint
COE: Common Operating Environment
COI: Community of Interest
CV: Capability Viewpoint
DIEA: DoD Information Enterprise Architecture, some sources also use DoD IEA.
DoD CIO CPG: DoD Chief Information Officer Capability Planning Guidance
GIG ORA: Global Information Grid Operational Reference Architecture (version 2.0)
IDM: Information Dissemination
ITIL: Information Technology Infrastructure Library
JCA: Joint Capability Area
JCSFL: Joint Common Systems Functions List
NIST SP: National Institute of Standards in Technology Special Publication
NMA: Network Mission Area
OV: Operational Viewpoint
SvcV: Services Viewpoint
SV: Systems Viewpoint
TM Forum: Telemanagement Forum

References to other architectures and frameworks

ANA Operational Viewpoint Version 1.0
ANA Systems Viewpoint Version 1.0
DoD Information Enterprise Architecture Version 2.0
GIG Operational Reference Architecture Version 2.0
ITIL Version 3.0
TM Forum Framework