

Appendix C to Annex A of LandWarNet 2020 & Beyond  
Enterprise Architecture:

## **Army Standards Profile Guidance**

In Support of Common Operating Environment (COE) v3

**Description**



**Version 1.0**

**15 August 2014**



---

## Executive Summary

The Army Chief Information Officer (CIO/G-6) and Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) have collaboratively developed a new process for the development of the Army Standards Profile Guidance, which provides a minimum set of standards as the foundation for building solutions that meet Army strategic guidance and achieve interoperability across the Enterprise. This Army proactive IT standards lifecycle process fills a gap to influence the Department of Defense (DoD) standards process, to ensure that Army imperatives continue to influence the DoD, and to provide standards guidance for solutions planning and execution.

CIO/G-6 and ASA(ALT) have executed this new process and leveraged the DOD Information Technology (IT) Standards Registry (DISR) process to create this Army Standards Profile Guidance package, which consists of this document and two Excel spreadsheets referenced in Tab A and Tab B. The Fiscal Year (FY) 14 Army Standards Profile Guidance provides technical guidance to the acquisition/testing community for COE v3 implementation in FY19 and supports Program Objective Memorandum (POM) 17-21 planning for Materiel Developers.

This Army Standards Profile Guidance package is synchronized with the CIO/G-6 “Annex A Technical Standards Guidance to LandWarNet 2020 and Beyond Enterprise Architecture” and the IT standards replace the “Army Technical Guidance Repository: Appendix A to the Guidance for 'End-State' Army Enterprise Network Architecture” dated 15 Mar 2012.

Points of contact for this action are Mr. John F. Sellner, Information Architecture Division, [john.f.sellner.civ@mail.mil](mailto:john.f.sellner.civ@mail.mil), (703) 545-1474 and Shi T. Zhu, Lead Electronics Engineer, Architecture and Standards Branch, [shi.t.zhu.civ@mail.mil](mailto:shi.t.zhu.civ@mail.mil), (443) 395-7373.

---

---

## **Table of Contents**

Executive Summary .....	ii
1 Introduction.....	1
1.1 Background .....	1
1.2 Purpose.....	4
1.3 Scope .....	4
2 Approach.....	5
2.1 Stakeholder Involvement.....	5
2.1.1 CIO/G-6.....	5
2.1.2 ASA(ALT) COE CEWG and COE SoS IPT .....	5
2.1.3 PoRs .....	6
2.1.4 AIC Testing Community.....	6
2.1.5 Training and Doctrine Command (TRADOC).....	6
2.1.6 Army Business Community .....	6
2.1.7 Army Intelligence Community .....	6
2.2 Inputs Used for Identifying Standards.....	6
2.2.1 DISR Baseline .....	6
2.2.2 Joint Information Environment (JIE) .....	7
2.2.3 LandWarNet Capability Sets (LWN CS) .....	7
2.2.4 Army Network Campaign Plan (ANCP).....	8
2.2.5 CIO/G-6 Guidance and Inputs .....	11
2.2.6 ASA(ALT) Guidance.....	12
2.2.7 Input from ASA(ALT) CEWG's .....	12
2.2.8 ASA(ALT) COE SoS StdV-1's .....	12
2.2.9 PoRs .....	12
2.3 Selection of Standards for the Army Standards Profile Guidance .....	12
2.3.1 Army Standards Profile Guidance Development.....	12
2.3.2 ATGR Standard Profiles .....	13
2.3.3 How Standards Are Identified for the Army Standards Profile Guidance .....	15
2.4 COE Standards Lifecycle Management Process.....	19
2.5 How to Use the Army Standards Profile Guidance.....	21
2.5.1 Description and Tour of the Army Standards Profile Guidance Spreadsheet.....	22
2.5.2 Example: Big Data and Cloud Computing .....	22
2.5.3 Example: Network Integration Evaluation Technical Architecture (NIE TA).....	23
Tab A Army Standards Profile Guidance for COEv3 - Core .....	25
Tab B Army Standards Profile Guidance for COEv3 - Use Cases .....	26
Acronyms.....	27

---

## List of Figures

Figure 1: Army Enterprise Architecture, including Annex A Technical Standards.....	1
Figure 2: Army Standards Profile Guidance package as part of Annex A Technical Standards .....	2
Figure 3: Notional Timeline Overlay for DISR Baseline, COE Updates, and Software/Application Updates .....	3
Figure 4: Layers versus COE Computing Environments (CEs).....	5
Figure 5: JIE and LWN Capability Taxonomy.....	8
Figure 6: Network Capacity Domain of ANCP (Source: Army Network Campaign Plan briefing, April 2014).....	9
Figure 7: Enterprise Services Domain of ANCP (Source: Army Network Campaign Plan briefing, April 2014).....	9
Figure 8: Network Operations & Security Domain of ANCP, Standards & Personnel focus (Source: Army Network Campaign Plan briefing, April 2014) .....	10
Figure 9: Network Operations & Security Domain of ANCP, Information Assurance focus (Source: Army Network Campaign Plan briefing, April 2014) .....	10
Figure 10: Network Operations & Security Domain of ANCP, Net Management focus (Source: Army Network Campaign Plan briefing, April 2014).....	10
Figure 11: JIE and JCA Capability Taxonomy.....	11
Figure 12: DISR Statuses .....	13
Figure 13: Technology-based Profiles (See DISR Statuses Legend in Figure 12) .....	14
Figure 14: GOTS-based Profile (See DISR Statuses Legend in Figure 12) .....	14
Figure 15: GTP-based Profile (See DISR Statuses Legend in Figure 12) .....	15
Figure 16: Example Mapping of JIE and LWN Capabilities to ATGR Standard Profiles	16
Figure 17: Mapping of JIE and JCA Capabilities to ATGR Standard Profiles .....	17
Figure 18: Example of JCA Mapping of 6.2.3. Core Enterprise Services .....	17
Figure 19: ATGR Standard Profiles with Standards (See DISR Statuses Legend in Figure 12) .....	18
Figure 20: JIE Capabilities and LWN Capabilities .....	19
Figure 21: COE Standards Lifecycle Management Process.....	20
Figure 22: Profiles for "Provide Assured Information and Services" LWN Capability Supporting Big Data and Cloud .....	23
Figure 23: Standards for "Cloud Infrastructure Management" Profile Supporting Big Data and Cloud (See DISR Statuses Legend in Figure 10) .....	23
Figure 24: Profiles Supporting NIE for LWN Capability "Provide C2 On the Move" .....	24
Figure 25: Standards Supporting NIE for "Mobile Ad Hoc Network (MANET)" Profile (See DISR Statuses Legend in Figure 10).....	24

# 1 Introduction

## 1.1 Background

There is a unified series of Army Enterprise Architecture guidance. Figure 1 depicts this cohesive whole.

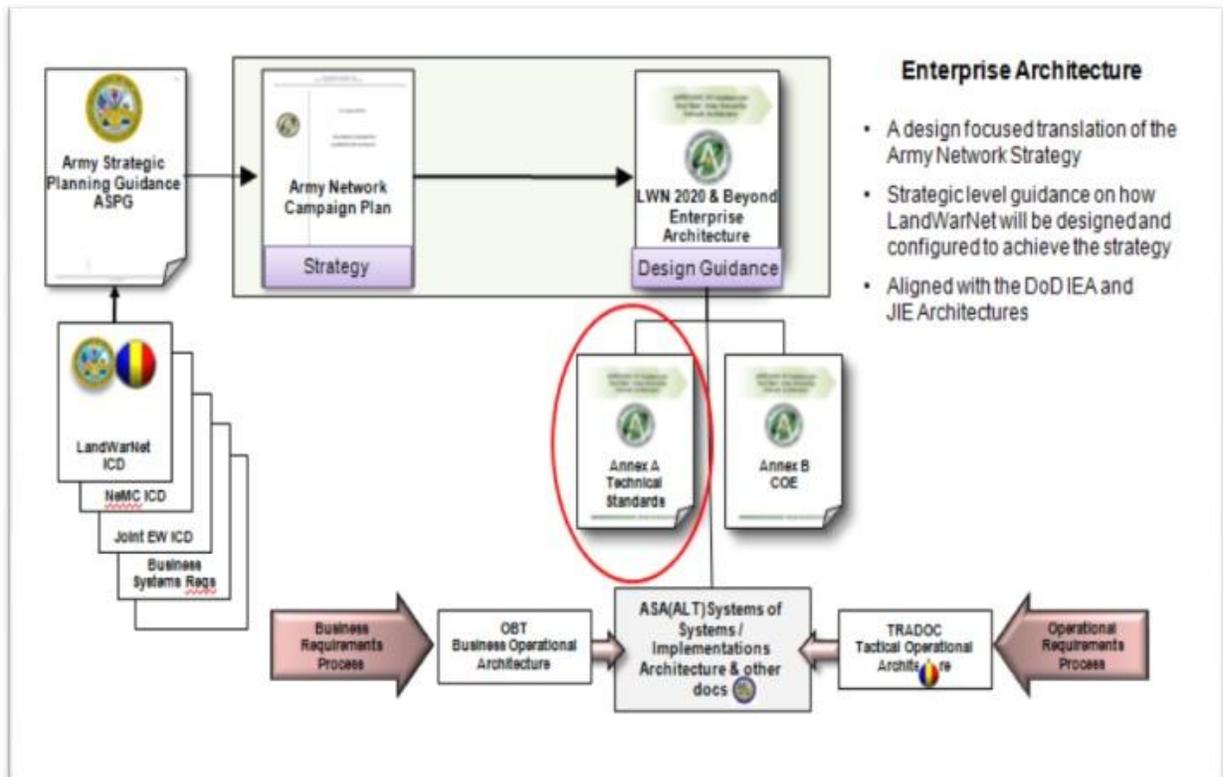


Figure 1: Army Enterprise Architecture, including Annex A Technical Standards

In Figure 1, circled in red, is “Annex A Technical Standards of LWN 2020 & Beyond Enterprise Architecture”. Annex A is the overarching Army Enterprise Architecture guidance for technical standards.

Figure 2 shows that this “Army Standards Profile Guidance package in support of COEv3” falls under Annex A, as depicted in the Army Enterprise Architecture in Figure 1. The “Army Standards Profile Guidance package in support of COEv3” that is an Appendix to Annex A.

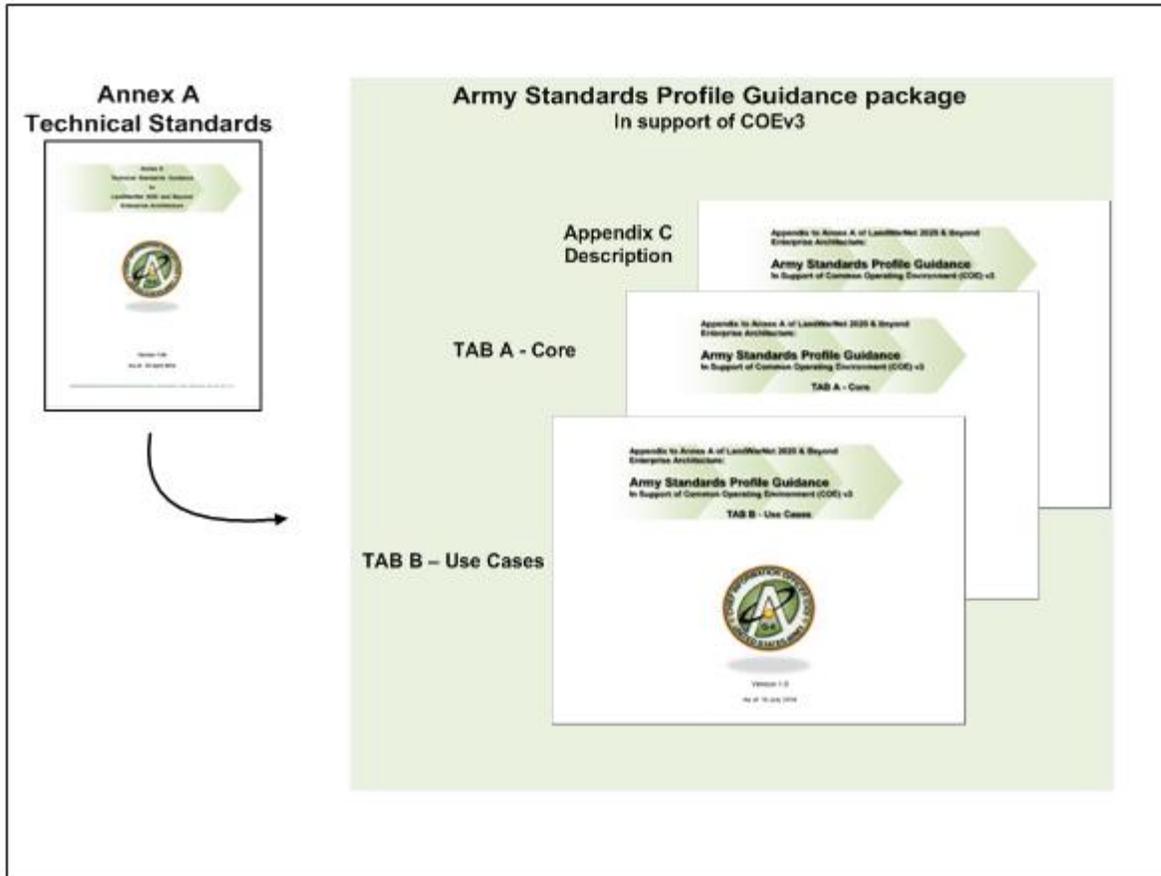


Figure 2: Army Standards Profile Guidance package as part of Annex A Technical Standards

The Army Standards Profile Guidance for COEv3 from CIO/G-6 provides a technical guidance package to achieve strategic Army technical goals, integrate multitier requirements, and assist the management of technology baselines in accordance with required timelines. As shown in Figure 2, it consists of:

- This document that provides descriptions and related background information
- Excel spreadsheet referenced in Tab A, which provides the core IT standards guidance
- Excel spreadsheet referenced in Tab B, which supplements the core IT standards guidance with Use Cases

Standards-based technical guidance is the foundation for achieving traceability from Army Imperatives to the materiel solutions used by the Total Force. CIO/G-6 and ASA(ALT) continue to create and improve processes for developing and implementing technical guidance for Materiel Solution Developers. In October 2010, ASA(ALT) and the CIO/G-6 released guidance for the COE. ASA(ALT) subsequently developed a comprehensive COE Implementation Plan. In addition, the former Software Blocking (SWB) Integrated Product Team (IPT) is now operating under COE governance. Efforts are ongoing to coordinate technical guidance processes of CIO/G-6 (top-down Army imperatives) and ASA(ALT) (bottom-up solutions).



---

## 1.2 Purpose

The Army Standards Profile Guidance establishes the annual process for the Army to manage IT standards at the enterprise level. It also provides the first installment of Army enterprise IT standards guidance, the first step in the process, to inform the acquisition community in support of Army system interoperability and integration.

At the time of creating this initial Army Standards Profile Guidance, the Army lacked an Enterprise process for defining a set of technical standards for interoperability of Army communications and information technology systems. An end-to-end process for identifying technical standards for the Army will provide the opportunity to better synchronize Army technical capabilities using the established DISR process with improved coordination between ASA(ALT) and CIO/G-6.

The purpose of this document is to provide guidance to the COEv3 StdV-1 development efforts COE IPT. This document, driven by a top-down approach based on Army Imperatives, Network Imperatives and Joint Capabilities, is intended to guide the selection of standards pre-contract, and with the expectation that the standards will be vetted, reviewed, and reshaped based on PoR constraints. The CIO/G-6 top-down processes are merged with the ASA(ALT) bottom-up process to achieve a strategically driven but practical solution.

This COE Standards Lifecycle Management Process was informed by the Network Synchronization Working Group (NSWG) guidance, supports the AIC, supports implementation based on the COE v3 SoS StdV-1, and aligns to DoD CIO Information Technology Standards guidance.

In its final form, the Army Standards Profile Guidance will be the result of comprehensive collaboration among stakeholders. The Army Standards Profile Guidance publication is an important input to the implementable StdV-1s created for the Mission Areas, which support Weapon System Reviews (WSRs) and POM planning. The Army Standards Profile Guidance applies across all Mission Areas, will reflect the final approved Mission Area StdV-1s, and supports joint interoperability and AIC testing.

## 1.3 Scope

The scope of this Army Standards Profile Guidance is defined in both operational and technical dimensions. Operationally, it encompasses the entire Army Enterprise, rather than a single mission area only, as was the case for COE SoS StdV-1/2's for COEv1 and COEv2 (i.e. the WMA), and therefore includes the following Mission Areas:

- Warfighter Mission Area (WMA)
- Business Mission Area (BMA)
- Enterprise Information Environment Mission Area (EIEMA, or IEMA)

- Defense Intelligence Mission Area (DIMA)

Along technical dimensions, it encompasses all five layers in Figure 4 as follows:

- Layer 1. Network/Transport
- Layer 2. Hardware/Devices
- Layer 3. Software Development Infrastructure
- Layer 4. Cross Cutting Capabilities
- Layer 5. End-User Applications (Web and Native)

Figure 4 shows these five layers covered by the Army Standards Profile Guidance for COE v3 versus Layers 3 and 4 covered by the COE v1/v2 SoS StdV-1/2.

Layer									Owner	
5. End-User Applications	Web	Web Applications								PoRs/ Industry
	Native	Applications	Applications	Applications	Applications	Applications	Applications	Applications	Applications	
4. Cross-Cutting Capabilities	Common technical standards and technologies across multiple CEs.								COE TAB	
3. Software Infrastructure	Background Services	Services	Services	Services	Services	Services	Infrastructure Services	Services	COE CEWGs	
	SDK	SDK		SDK	SDK	SDK	Web SDK	PaaS SDK		
	OS	OS		OS	OS	OS	VM Template			
2. Hardware/Devices	Embedded Platform Devices		Phones, Tablets, Devices	Embedded Computers	Laptops	Servers	Servers	Phones, Tablets, PCs	Platform IPT	
1. Network/Transport	IA/Cyber								Network Design Cell	
	NetOps									
	IP Network									
	Transport									
		RTSCE	Sensor	Mobile	Mounted	Command Post	DC/Cloud	JJIM	v15	
COE Computing Environments (CEs)										

Figure 4: Layers versus COE Computing Environments (CEs)

## 2 Approach

### 2.1 Stakeholder Involvement

This effort requires input from all of the key stakeholders, including:

#### 2.1.1 CIO/G-6

CIO/G-6, as the Chief Technical Architect for the Army, is the lead for this effort.

#### 2.1.2 ASA(ALT) COE CEWG and COE SoS IPT

ASA(ALT) provides input from two sides:

1. COE Computing Environment Working Groups (CEWG's)
2. COE SoS IPT

---

The COE CEWG's are responsible for working with the PoRs binned to each particular CE to develop plans for implementing technical standards moving forward. The COE SoS IPT is responsible for coordinating standards based on ability of the PoRs, given constraints such as schedule, resources, and performance, to maintain interoperability and facilitate a successful AIC for all IPT member programs.

### **2.1.3 PoRs**

The COE SoS IPT represents the PoR community related to implementation of standards. However, the IPT does not represent all PoRs in the larger Army community, and therefore the scope of the Army Standards Profile Guidance is greater than the scope of the COE SoS StdV-1/2. Represented PoRs are responsible for participating and providing input as to the technologies they are using and plan to use. The objective is to closely synchronize, over time, the standards that PoRs are using or intend to use, as documented in the COEv3 SoS StdV-1, with the Army Standards Profile Guidance.

### **2.1.4 AIC Testing Community**

The AIC testing community conducts the testing required for AIC of the COE baseline. AIC testing will use the COE v3 SoS StdV-1 to inform the testing effort. This iteration of the testing uses Control Point testing to facilitate interoperability during integration and mission thread based testing during AIC. The AIC testing community provides input to ensure this technical guidance will properly set the stage for testing.

### **2.1.5 Training and Doctrine Command (TRADOC)**

TRADOC provides high-level strategic guidance, including the capabilities represented in the LandWarNet (LWN) Initial Capabilities Documents (ICDs) for both Mission Command (MC) and Network-enabled Mission Command (NeMC). These ICDs provide the scope and breakdown guidance for the Army Standards Profile Guidance.

### **2.1.6 Army Business Community**

The Army Business Community, through input from the BMA is an Army enterprise stakeholder and provides guidance and feedback as appropriate.

### **2.1.7 Army Intelligence Community**

The Army Intelligence Community, through input from the DIMA is an Army enterprise stakeholder and provides guidance and feedback as appropriate.

## **2.2 Inputs Used for Identifying Standards**

This section shows the various inputs and processes used to identify the standards found in the Army Standards Profile Guidance, with the aim of creating traceability from DoD standards to Army Imperatives.

### **2.2.1 DISR Baseline**

The FY14 Army Standards Profile Guidance is based on DISR Baseline 14-1.0. It

---

---

includes DISR standards (Mandated and Emerging). Non-DISR standards that are applicable to Army capabilities in recent or future implementations can also be used. However, non-DISR standards need to be added to the DISR baseline using the DISR CR process, or otherwise a waiver is required. DISR Retired standards can be used also, but a waiver is required.

### 2.2.2 Joint Information Environment (JIE)

The JIE provides a high-level categorization for Army LWN capabilities. The following high-level capabilities were used for the LWN mappings, discussed in further detail in section 2.2.3 below:

- Access
- Connect
- Defend
- Monitoring & Compliance
- Operate
- Processes & Models
- Share
- Standards & Policy

The following reduced list of these high-level capabilities, oriented to the network, were used for the Joint Capability Area (JCA) mappings, discussed in further detail in section 2.2.4 below:

- Access
- Connect
- Defend
- Operate
- Share

In addition to the JIE taxonomy, JIE StdV-1s standards have been used as input.

### 2.2.3 LandWarNet Capability Sets (LWN CS)

The LWN CS capabilities were used as inputs for grouping the technical standards. LWN capabilities were derived from the LWN ICD's for MC and NeMC. They map to the high-level JIE architecture as described in section 2.2.2. Figure 5 shows the JIE and LWN capability taxonomy.

JIE Capability	LWN Capability
Access	Enterprise Identity & Access Management (IdAM)
	Digital User and Service Attributes
	Role-Based Access to Networks
Connect	Provide C2 On the Move
	Provide Dismounts Voice and/or Data to Pass PLI & C2 Data
	Provide Enterprise Network Transport (End-to-End)
	Provide JIIM Interoperability
	Provide Range Extension via Aerial Layer
	Provide Satellite connectivity to Bde, Bn, Co
	Provide Tiered Transport Capability
Defend	Capability to Establish Integrated Network Defense-in-Depth
	Enable Cross Domain Security Enforcement
	Enable HBSS & Personal Personifications to ID Activity
	Enable IE Operations Threat Assessment
Monitoring & Compliance	Adherence to Technical Interoperability Standards
	Infrastructure & Certification Accreditation
Operate	Capability to Execute Tactical Network Operations
	Capability to Integrate NetOps with Mission Partners
	Capability to Plan, Configure & Monitor Network
	Capability to Transition C2 Network Authorities
Processes & Models	Architecture Development & Use
	New Technology Implementation Through NIE
Share	Ability to Aggregate Class/Unclass Data
	Ability to Display and Manipulate the COP
	Applications to Enable Mission Command (MC) Essential Capabilities
	Capability for Cross Domain Access
	Capability to Tag & Prioritize Data for Transport
	Enable Global Collaboration (Voice, Chat, Whiteboard)
	Provide Tools for MC Rehearsal & Training
	Standard & Sharable Geospatial Foundation
	Provide Assured Information and Services
Standards & Policy	Establish Unity of Command & Unity of Effort
	Information Assurance Compliance
	Standards IE Education & Training

Figure 5: JIE and LWN Capability Taxonomy

### 2.2.4 Army Network Campaign Plan (ANCP)

The ANCP, guided by the Army Network Strategy (Near-, Mid-, Long-Term), in development by CIO/G-6, provides a JCAs-aligned taxonomy. This taxonomy was used to map to the standards, providing an additional way to trace capabilities to the technical standards.

The ANCP consists of three Domains:

1. Network Capacity Domain – ensures a resilient transport network with availability and capacity to support regionally-aligned and unified-action partners
2. Enterprise Services Domain – ensures an integrated collaborative environment that support all Army Mission Areas
3. Network Operations & Security Domain – ensures systematization of well-defined cyber security responsibilities, protection of network and information against threats, effective mission execution on the network by authorized users

These three ANCP domains are mapped to specific JCAs, which provide a standardized set of definitions that cover the complete range of military activities. The JCA, established in May 2005 by the Joint Staff with input from each of the services,

facilitates side-by-side comparisons of service contributions to joint warfighting and assists with resource management across mission areas and among the services.

The latest JCAs, updated in 2010, include:

1. Force Support
2. Battlespace Awareness
3. Force Application
4. Logistics
5. Command and Control
6. Net-Centric
7. Protection
8. Building Partnerships
9. Corporate Management and Support

The ANCP mappings to the JCA and the corresponding JCA mappings of the Army Standards Profile Guidance focus on number 6 above, the Net-Centric JCA.

The Network Capacity Domain, shown in Figure 6, focuses on Information Transport and Computing Services.

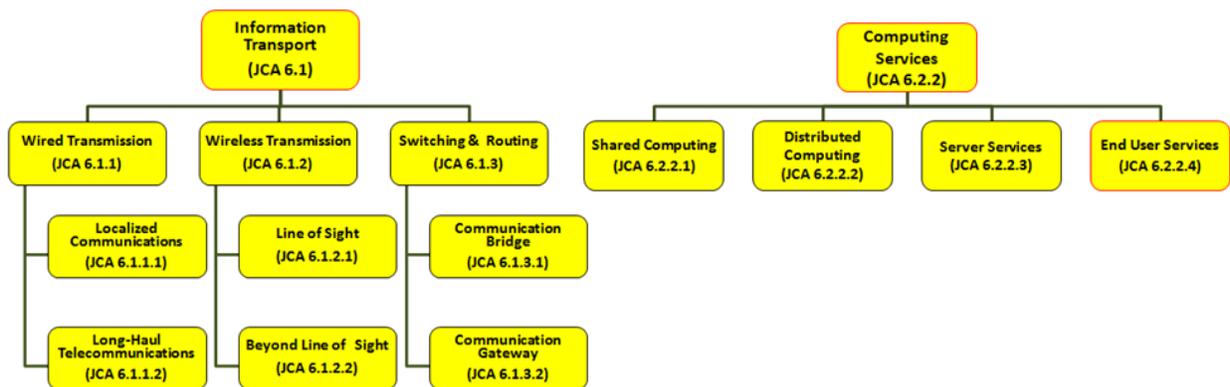


Figure 6: Network Capacity Domain of ANCP  
(Source: Army Network Campaign Plan briefing, April 2014)

The Enterprise Services Domain, shown in Figure 7, focuses on "Core Enterprise Services" and "Position, Navigation, and Timing (PNT)".

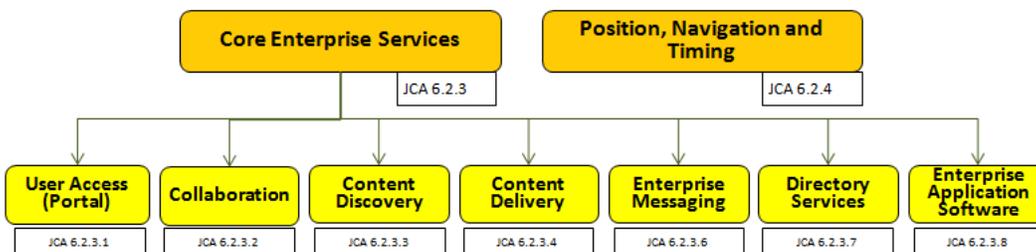


Figure 7: Enterprise Services Domain of ANCP  
(Source: Army Network Campaign Plan briefing, April 2014)

The Network Operations & Security Domain focuses on Standards & Personnel, Information Assurance, and Net Management. Figure 8 show the JCAs under Standards & Personnel:

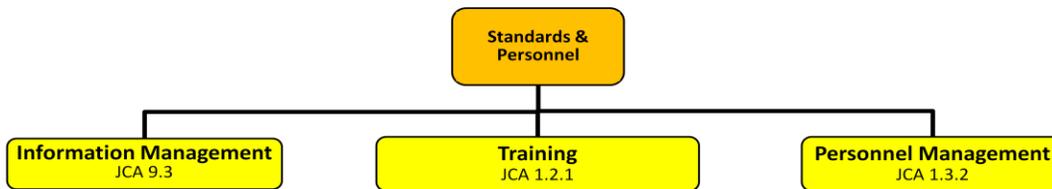


Figure 8: Network Operations & Security Domain of ANCP, Standards & Personnel focus  
(Source: Army Network Campaign Plan briefing, April 2014)

Figure 9 shows the Network Operations & Security Domain for Information Assurance:

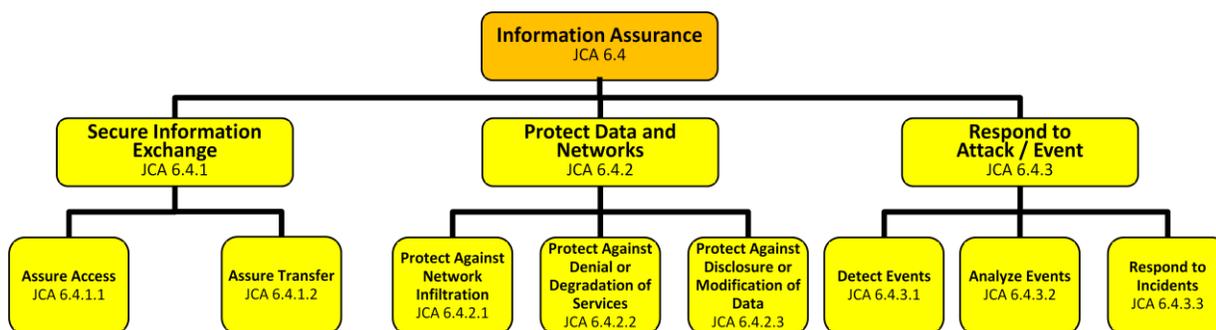


Figure 9: Network Operations & Security Domain of ANCP, Information Assurance focus  
(Source: Army Network Campaign Plan briefing, April 2014)

Figure 10 shows the Network Operations & Security Domain for Net Management:

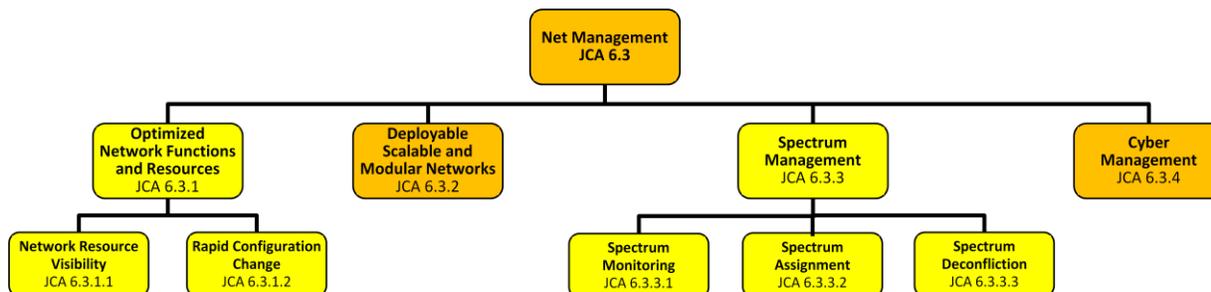


Figure 10: Network Operations & Security Domain of ANCP, Net Management focus  
(Source: Army Network Campaign Plan briefing, April 2014)

Unlike LWN, the Net-Centric JCA, shown as Tier 1 in Figure 11 below, is broken into four sub-tiers (Tier 2):

- 6.1 Information Transport
- 6.2 Enterprise Services
- 6.3 Net Management
- 6.4 Information Assurance

These sub-tiers do not map one-to-one to JIE capabilities, and they further decompose into a Tier 3 and a Tier 4.

Figure 11 shows the complete taxonomy used the JCA mapping:

JIE Capability	JCA (Tier 1)	JCA (Tier 2)	JCA (Tier 3)	JCA (Tier 4)					
Access	6 Net-Centric	6.2 Enterprise Services	6.2.3 Core Enterprise Services	6.2.3.7 Directory Services					
		6.4 Information Assurance	6.4.1 Secure Information Exchange	6.4.1.1 Assure Access					
Connect		6.1 Information Transport	6.1.1 Wired Transmission	6.1.1.1 Localized Communications	6.1.1.2 Long-Haul Telecommunications				
				6.1.2 Wireless Transmission	6.1.2.1 Line of Sight	6.1.2.2 Beyond Line of Sight			
			6.1.3 Switching and Routing	6.1.3.1 Communication Bridge	6.1.3.2 Communication Gateway				
				6.4 Information Assurance	6.4.1 Secure Information Exchange	6.4.1.2 Assure Transfer			
Defend		6.4.2 Protect Data and Networks	6.4.2.1 Protect Against Network Infiltration	6.4.2.2 Protect Against Denial or Degradation of Services	6.4.2.3 Protect Against Disclosure or Modification of Data				
			6.4.3 Respond to Attack / Event	6.4.3.1 Detect Events	6.4.3.2 Analyze Events	6.4.3.3 Respond to Incidents			
				6.3 Net Management	6.3.1 Optimized Network Functions and Resources	6.3.1.1 Network Resource Visibility	6.3.1.2 Rapid Configuration Change		
Operate		6.3.2 Deployable Scalable and Modular Networks	6.3.2.1 Network Resource Visibility	6.3.2.2 Rapid Configuration Change	N/A				
			6.3.3 Spectrum Management	6.3.3.1 Spectrum Monitoring	6.3.3.2 Spectrum Assignment	6.3.3.3 Spectrum Deconfliction			
				6.3.4 Cyber Management	N/A				
			Share	6.2 Enterprise Services	6.2.2 Computing Services	6.2.2.1 Shared Computing	6.2.2.2 Distributed Computing	6.2.2.3 Server Services	6.2.2.4 End User Services
6.2.3 Core Enterprise Services		6.2.3.1 User Access (Portal)				6.2.3.2 Collaboration	6.2.3.3 Content Discovery	6.2.3.4 Content Delivery	6.2.3.6 Enterprise Messaging
	6.2.4 Position, Navigation and Timing	6.2.4.1 Provide Position, Navigation and Timing Information				6.2.4.2 Utilize Position, Navigation and Timing			

Figure 11: JIE and JCA Capability Taxonomy

### 2.2.5 CIO/G-6 Guidance and Inputs

CIO/G-6 references used to create this Army Standards Profile Guidance include:

- ANCP
- Army Network Strategy 2025
- LandWarNet 2020 & Beyond Strategy
- LWN 2020 & Beyond End State Architecture, Annexes A & B
- CIO/G-6 Reference Architectures
- Army Data Strategy
- COE Testing Strategy

The standards from these guidance documents are contained in the CIO/G-6 Army

---

Technical Guidance Repository (ATGR), which is a repository of DISR and non-DISR standards that are part of CIO/G-6 guidance.

In addition, the EIEMA provides input.

### **2.2.6 ASA(ALT) Guidance**

ASA(ALT) Guidance includes:

- COE Implementation Plan
- COE CE Control Point Specifications
- COE Integrated Systems Engineering Plan (ISEP)

### **2.2.7 Input from ASA(ALT) CEWG's**

The ASA(ALT) CEWGs consist of PoRs assigned to a primary CE. The CEWG's hold regular meetings to discuss CE business, including the standards the member PoRs use. CEWG members vet these standards over time, providing valuable cross-collaboration among PoRs. Schedule, cost, and quality considerations influence these inputs.

### **2.2.8 ASA(ALT) COE SoS StdV-1's**

The prior versions of the COE SoS StdV-1/2s have been used as input. The COE SoS StdV-1s are managed during their lifecycles to ensure that changes in standards are identified and that a process exists to implement specifications and upgrades necessary to support Material Development. As the StdV-1s evolve during the life cycle, the updated baselines serve as input to future baselines.

### **2.2.9 PoRs**

PoRs will identify new standards as part of technical enhancements that will efficiently support their development. If these "standards" – including technical standards, tools, profiles and specifications - are not identified within DISR, ASA(ALT) will track them and identify them to the CIO/G-6. CIO/G-6 will review them and coordinate for inclusion in the DISR as appropriate. PoRs are also the key components within the COE CE WGs.

## **2.3 Selection of Standards for the Army Standards Profile Guidance**

This section shows how CIO/G-6 selects standards in a top-down process for inclusion in a Technical Architecture. It also shows how to use this information to create a StdV-1/2 that complies with guidance.

### **2.3.1 Army Standards Profile Guidance Development**

The Army Standards Profile Guidance informs the implementable COE v3.0 SoS StdV-1, but many of the standards can be included in an StdV-2 by the COE SoS and PoRs depending upon implementation considerations. StdV-2 candidate standards are marked within the spreadsheet, and decisions on where to put those standards can be

---

based on the following guidance regarding StdV-1s and StdV-2s:

- **StdV-1** – Represents the set of standards used by Material Developers within a given Mission Area unique to a baseline. DISR Mandated standards are required when applicable. However, a DISR Retired or non-DISR standard can be used if a DISR Waiver is obtained. In addition, an Emerging or non-DISR standard may be added to the StdV-1 if a CR for inclusion of the standard in DISR is submitted and approved.
- **StdV-2** – includes standards that are not DISR Mandated and are for future planning purposes (three to five years), or next reset cycle implementation. DISR Emerging standards and non-DISR standards, including GOTS, can be considered for the StdV-2. Emerging standards within the StdV-2 are presented for consideration and are not automatically required for implementation by any Mission Areas.

### 2.3.2 ATGR Standard Profiles

ATGR Technical Profiles (Profiles) are a convenient way to categorize groups of related standards. This is helpful in the development of guidance, such as the Army Standards Profile Guidance, because these aggregations of standards make it easier to identify candidate standards. For the same reason, the ATGR is a recommended web-based tool for the CEs and PoRs to use to develop their StdV-1/2s.

Each Profile provides a grouping or categorical group which consists of a minimum set of the standards. There are three types of profiles defined in this document:

1. Technology-based Profile
2. Government Off The Shelf (GOTS) based Profile
3. GIG Technical Profile (GTP) based Profile

Note DISR statuses in Figure 12:

DISR Status	Description
M	DISR Mandated Standard (standard provides interoperability)
E	DISR Emerging Standard (expected to become mandated within 3 years)
A	DISR Active (Information/Guidance Document)
N	Non-DISR Standard (Standards and Specifications)
G	Non-DISR Information/Guidance Document and Executive Order
I	Implementation (Application, Service, Solution, Toolkit)

Figure 12: DISR Statuses

A Technology-based Profile contains one or more standards associated with a technology. Figure 13 shows an example of Technology-based Profiles for “Biometric Validation” and “Cloud Storage”.

ATGR Standard Profile	Standard ID	Standard Title	DISR Status
Biometric Validation	ANSI INCITS 385-2004	Face Recognition Format for Data Interchange, May 13, 2004	M
	ANSI/INCITS 378-2004	Finger Minutiae Format for Data Interchange	M
	ANSI/INCITS 381-2004	Finger Image-Based Data Interchange Format	M
	DoD EBTS v3.0	DoD Electronic Biometric Transmission Specification, version 3.0, 8 December 2011	M
	ISO/IEC 19794-6:2011	Biometric data interchange formats Part 6: Iris image data	M
	ISO/IEC 19794-7:2007 w/Cor1:2009	Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data w/Corrigendum 1:2009	M
Cloud Storage	Topology and Orchestration Specification for Cloud Applications (TOSCA)	Enables the interoperable description of application and infrastructure Cloud services, the relationships between parts of the service, and the operational behavior of these services – independent of the supplier creating the service and any particular Cloud Provider or hosting technology.	N
	Virtual Machine Disk Format (VMDK)	The format is a container for virtual hard disk drives to be used in virtual machines.	N

**Figure 13: Technology-based Profiles**  
(See DISR Statuses Legend in Figure 12)

A GOTS-based Profile contains one or more government solutions, designated as “I” for Implementation (Application, Service, Solution, Toolkit), such as Army Mobility Service, JIE Solution Architecture, etc. Figure 14 shows an example of GOTS-based Profiles for “JIE Satellite Communications Gateway Solution Architecture”, “Distributed Common Ground Station-Army (DCGS-A) Cloud”, and “Army Mobility Service”.

ATGR Standard Profile	Standard ID	Standard Title	DISR Status
JIE Satellite Communications Gateway Solution Architecture	JIESATCOM GW SG-SA	Joint Information Environment Increment 1 Satellite Communications (SATCOM) Gateway (GW) Solution Architecture (SG-SA); <a href="https://sadie.nmci.navy.mil/JAFE/arch_projects/arch_detail.aspx?ID=1391">https://sadie.nmci.navy.mil/JAFE/arch_projects/arch_detail.aspx?ID=1391</a>	I
Distributed Common Ground Station-Army (DCGS-A) Cloud	DCGS-A Cloud	Distributed Common Ground Station-Army Cloud; <a href="http://dcgsa.apg.army.mil/">http://dcgsa.apg.army.mil/</a>	I
Army Mobility Services	AMS	Army Mobility Services; <a href="http://ciog6.army.mil/Portals/1/Policy/2013/Army%20Mobility%20Strategy_26NOV2013.pdf">http://ciog6.army.mil/Portals/1/Policy/2013/Army%20Mobility%20Strategy_26NOV2013.pdf</a>	I

**Figure 14: GOTS-based Profile**  
(See DISR Statuses Legend in Figure 12)

A GTP-based Profile represents a DISR-published ‘approved for use’ Profile. Figure 15 shows an example of a GTP-based Profile for “GTP043 - XMPP IM/Chat Federation”. In this document, the standards of selected GTPs have been updated to the current DISR Baseline 14-1.

ATGR Standard Profile	Standard ID	Standard Title	DISR Status
GTP043 - XMPP IM/Chat Federation	IETF RFC 2782	A DNS RR for specifying the location of services (DNS SRV), February 2000	M
	IETF RFC 4422	Simple Authentication and Security Layer (SASL), June 2006	E
	IETF RFC 5246	The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008	M
	IETF RFC 6120	Extensible Messaging and Presence Protocol (XMPP): Core, March 2011	M
	IETF RFC 6121	Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence, March 2011	M
	IETF RFC 6122	Extensible Messaging and Presence Protocol (XMPP): Address Format, March 2011	M

**Figure 15: GTP-based Profile**  
(See DISR Statuses Legend in Figure 12)

In the Army Standards Profile Guidance spreadsheet, Profiles are used as part of a two-step mapping process:

- **Capability-to-Profile** – Profiles are mapped to LWN, JCA, and JIE capabilities. The “LWN-to-ATGR Profiles” tab shows mapping of JIE Capability-to-LWN Capability-to-ATGR Standard Profile. Similarly, the “JCA-to-ATGR Profiles” tab shows mapping of JIE Capability-to-JCA Capability-to-ATGR Standard Profile. Multiple Profiles can map to a single capability, or a single Profile can map to multiple capabilities.
- **Profile-to-Standards** – Profiles are mapped to Standards in the “ATGR-Profiles-to-Standards” tab, which lists all of the standards associated with each Profile. A Profile typically maps to multiple standards; however, a single standard can map to multiple Profiles.

### 2.3.3 How Standards Are Identified for the Army Standards Profile Guidance

Standards are identified from the ATGR mappings. At the highest level of mapping, JIE Capability is mapped to LWN Capability, which in turn is mapped to ATGR Standard Profiles. ATGR Standard Profiles are groupings of standards that support a specific sub-capability. For example, from the “LWN-to-ATGR Profiles” tab of the Tab A spreadsheet, Figure 16 shows that the JIE Capability “Access” includes three LWN capabilities. The third LWN Capability in that grouping is “Role-Based Access to Networks”, and it maps to three Profiles: “Authoritative Attribute Exchange Service”, “Role Based Access Control (RBAC)”, and “Digital Signature”.

JIE Capability	LWN Capability & Definition	ATGR Standard Profiles & Definitions	
Access	Enterprise Identity & Access Management (IdAM)	Authentication Management Services	
		Common Access Card (CAC)	
		Credential Management	
		Digital Certificate (PKI)	
		DoD Identity Synchronization Services Solution Architecture	
		Identity Based Access Control (IBAC)	
		Identity and Access Management (IdAM)	
		Identity Management	
		Policy in Authentication	
	Policy in Credentialing		
	Secure Shell		
	Digital User and Service Attributes		Authoritative Attribute Exchange Service
			Digital Signature
			DISA Authentication Gateway Service Solution Architecture
			Encryption & Decryption
JIE White Pages Service Solution Architecture			
Role-Based Access to Networks		Key Exchange	
		Attribute Based Access Control (ABAC)	
		Authoritative Attribute Exchange Service	
		Digital Signature	
Connect	Provide C2 On the Move	GTP003 - Ku-Band Satellite Communications	
		GTP004 - Ka-Band Satellite Communications	
		Mobile Ad Hoc Network (MANET)	
		Mobile IPv4 Performance Optimization	
		Mobile IPv6	
		Mobile IPv6 Basic Mobility Services	
		Over-the-Air-Rekeying (OTAR)	
		Point of Presence (PoP)	
		SIPR-NIPR Access Point (SNAP)	
		Tactical Radio BLOS Communications	
		Tactical Radio Interface Specification	
		Tactical Radio LOS Communications	
		WIN-T Soldier Network Extensions (SNE)	
		Wireless LAN (WLAN)	
		Wireless Network after Next (Wnan)	

Figure 16: Example Mapping of JIE and LWN Capabilities to ATGR Standard Profiles

Figure 17 shows a similar mapping, but for JCA, instead of LWN, capabilities. It is extracted from the “JCA-to-ATGR Profiles” tab of the Tab A spreadsheet.

JIE Capability	JCA (Tier 1)	JCA (Tier 2)	JCA (Tier 3)	JCA (Tier 4)	ATGR Standard Profiles & Definitions
Access	6 Net-Centric	6.2 Enterprise Services	6.2.3 Core Enterprise Services	6.2.3.7 Directory Services	Directory Management Services
					Directory Services (X.500)
					DoD Enterprise Directory Services
					JIE Directory Services Solution Architecture
					JIE White Pages Service Solution Architecture
					XML Directory Schema
		6.4 Information Assurance	6.4.1 Secure Information Exchange	6.4.1.1 Assure Access	Identity and Access Management (IdAM)
					Attribute Based Access Control (ABAC)
					Biometric Validation
					Common Access Card (CAC)
					Digital Certificate (PKI)
					Digital Signature
					Identity Based Access Control (IBAC)
					Key Exchange

Figure 17: Mapping of JIE and JCA Capabilities to ATGR Standard Profiles

The JCA Capabilities are provided in four tiers, or four levels of decomposition. Figure 17 shows that there are six Profiles, starting with “Directory Management Services” and ending with “XML Directory Schema”, in the last column. They map to JCA (Tier 1) “6 Net Centric”, JCA (Tier 2) “6.2 Enterprise Services”, JCA (Tier 3) “6.2.3 Core Enterprise Services”, and JCA (Tier 4) “6.2.3.7 Directory Services” under JIE Capability “Access”. The full JCA taxonomy is shown in Figure 11 – JIE and JCA Capability Taxonomy.

Figure 18 also provides an example of a JCA Mapping from Tier 3, 6.2.3. Core Enterprise Services, as mapped to the ANCP.

JCA (Tier 3)	JCA (Tier 4)	ATGR Standard Profiles & Definitions
6.2.3 Core Enterprise Services	6.2.3.1 User Access (Portal) 6.2.3.2 Collaboration	Army Data Strategy
		Army Knowledge Online
		LandWarNet Services Catalog
		Enterprise Content Management and Collaboration Service (ECMCS)
		Army Mobility Services
		Army Unified Capabilities
		Defense Connect Online
		DoD Enterprise Services
		Enterprise Content Management and Collaboration Service (ECMCS)
		GTP043 - XMPP IM/Chat Federation
		JIE Unified Capabilities Solution Architecture
		milSuite
		Video Teleconferencing
		Voice & Video over Internet Protocol (VVoIP)
Web Conferencing and Web Collaboration		

Figure 18: Example of JCA Mapping of 6.2.3. Core Enterprise Services

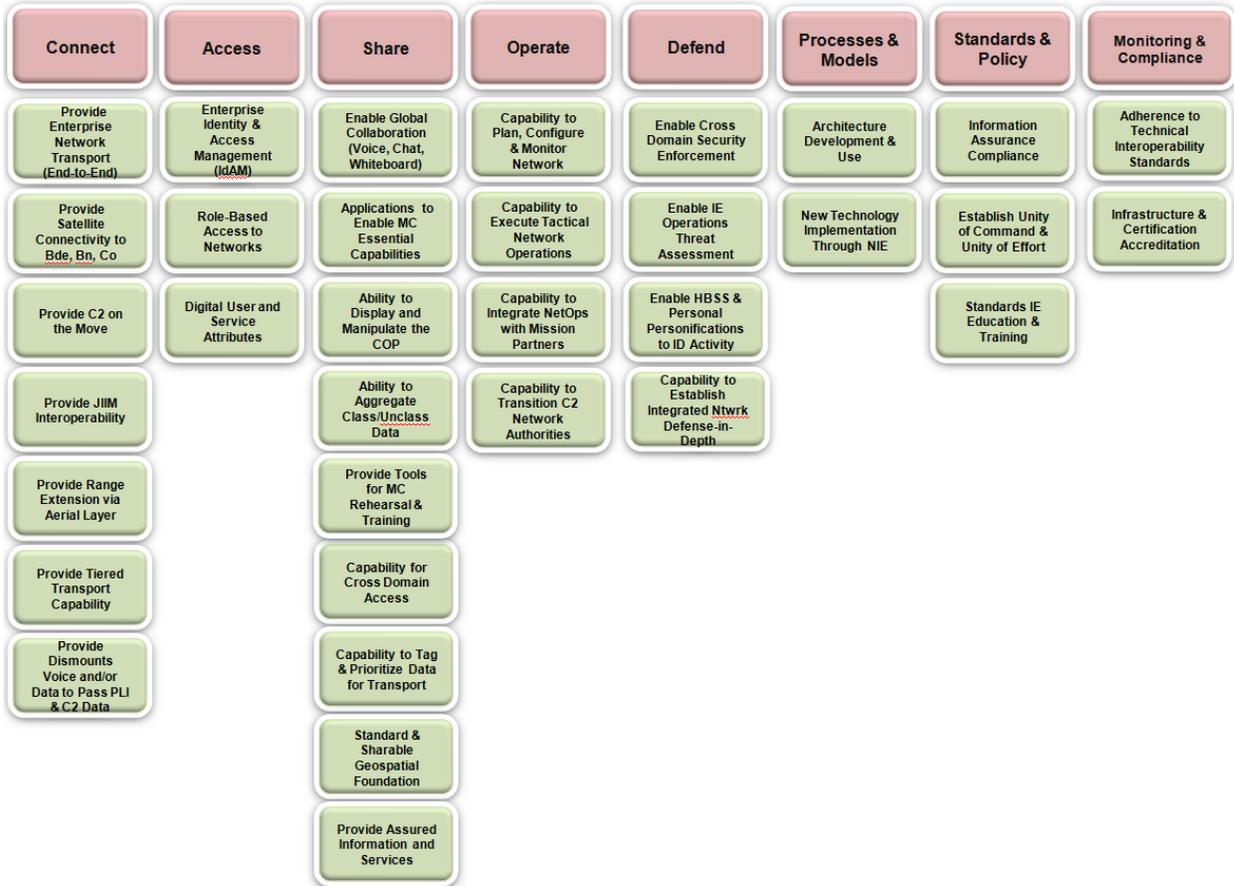
The “ATGR Profiles-to-Standards” tab provides the standards for the Profiles, regardless of whether you used the LWN or JCA capability mappings. Each Profile maps to multiple individual standards independently of the Army Standards Profile Guidance or any other specific Technical Architecture. Figure 19 shows the mapping, including ATGR Standard Profiles Name, Standard ID, Standard Title, DISR Status, and DISR Service Area.

ATGR Standard Profile	Standard ID	Standard Title	Status	Service Area
Application Data Sharing	ITU-T T.120	Data protocols for multimedia conferencing, July 1996	M	Video Teleconferencing
	ITU-T T.122:1998	Multipoint Communications Service - Service Definition, February 1998	M	Video Teleconferencing
	ITU-T T.123:1999	Network - Specific Data Protocol Stacks Multimedia Conferencing, May 1999	M	Video Teleconferencing
	ITU-T T.124:1998	Generic Conference Control, February 1998	M	Video Teleconferencing
	ITU-T T.125:1998	Multipoint Communications Service Protocol Specification, February 1998	M	Video Teleconferencing
	ITU-T T.126:1997	Multipoint Still Image and Annotation Protocol, July 1997	M	Video Teleconferencing
	ITU-T T.127	Multipoint Binary File Transfer Protocol, August 1995	M	Video Teleconferencing
	ITU-T T.128	Multipoint Application Sharing, February 1998	M	Video Teleconferencing
Army Data Strategy	ADS	Army Data Strategy; <a href="http://ciog6.army.mil/Portals/1/InfoSheet/04-ADS_Info%20Paper%20(1p)_v1.pdf">http://ciog6.army.mil/Portals/1/InfoSheet/04-ADS_Info%20Paper%20(1p)_v1.pdf</a>	I	N/A
Army Enterprise Service Desk	AESD	Army Enterprise Service Desk; <a href="https://esd-crm.csd.disa.mil/">https://esd-crm.csd.disa.mil/</a>	I	N/A
Army Knowledge Online	AKO	Army Knowledge Online; <a href="https://www.us.army.mil">https://www.us.army.mil</a>	I	N/A
Army Mobility Services	AMS	Army Mobility Services; <a href="http://ciog6.army.mil/Portals/1/Policy/2013/Army%20Mobility%20Strategy_26NOV2013.pdf">http://ciog6.army.mil/Portals/1/Policy/2013/Army%20Mobility%20Strategy_26NOV2013.pdf</a>	I	N/A
Army Unified Capabilities	AUC	Army Unified Capabilities; <a href="http://ciog6.army.mil/Portals/1/Architecture/Army%20UC%20RA%20v1.0--03%20October13%20reduced%20size%2019%20Nov%202013.pdf">http://ciog6.army.mil/Portals/1/Architecture/Army%20UC%20RA%20v1.0--03%20October13%20reduced%20size%2019%20Nov%202013.pdf</a>	I	N/A

**Figure 19: ATGR Standard Profiles with Standards**  
(See DISR Statuses Legend in Figure 12)

To help users understand and select the appropriate ATGR Standard Profiles and standards, definitions are provided for the LWN Capability and ATGR Standard Profile.

Figure 20 shows the complete set of mappings between JIE Capabilities and LWN Capabilities, as derived from the LWN MC ICD and NeMC ICD.



**Figure 20: JIE Capabilities and LWN Capabilities**  
(derived from the LWN and Network-enabled Mission Command ICDs)

The process used to identify the standards is as follows:

1. Extract from the ATGR the set of standards from the JIE Capabilities-to-LWN Capabilities-to-ATGR Standard Profiles-to-standards mapping.
2. Analyze the resulting list for matches to COEv2 StdV-1.
3. Identify the mismatches due only to versioning differences.
4. Analyze the results by repeating the above steps against the draft COE M/HH StdV-1, and ensure all standards are covered. Disregard items in M/HH that are not standards.
5. Analyze and identify ATGR Standard Profiles that can alternatively provide the functionality of standards from COEv2 and M/HH that did not have a match to the current list.

This process will continue in order to update and fine-tune the list for the final deliverable. The completed mappings will be added to the ATGR.

## 2.4 COE Standards Lifecycle Management Process

This section shows the various inputs, thought processes, and protocols used to

include or exclude the standards found in this Army Standards Profile Guidance.

Figure 21 illustrates the agreement between ASA(ALT) and CIO/G-6 on the COE Standards Lifecycle Management Process. This process will be adjusted in the future to accommodate the nuances of each Mission Area (MA).

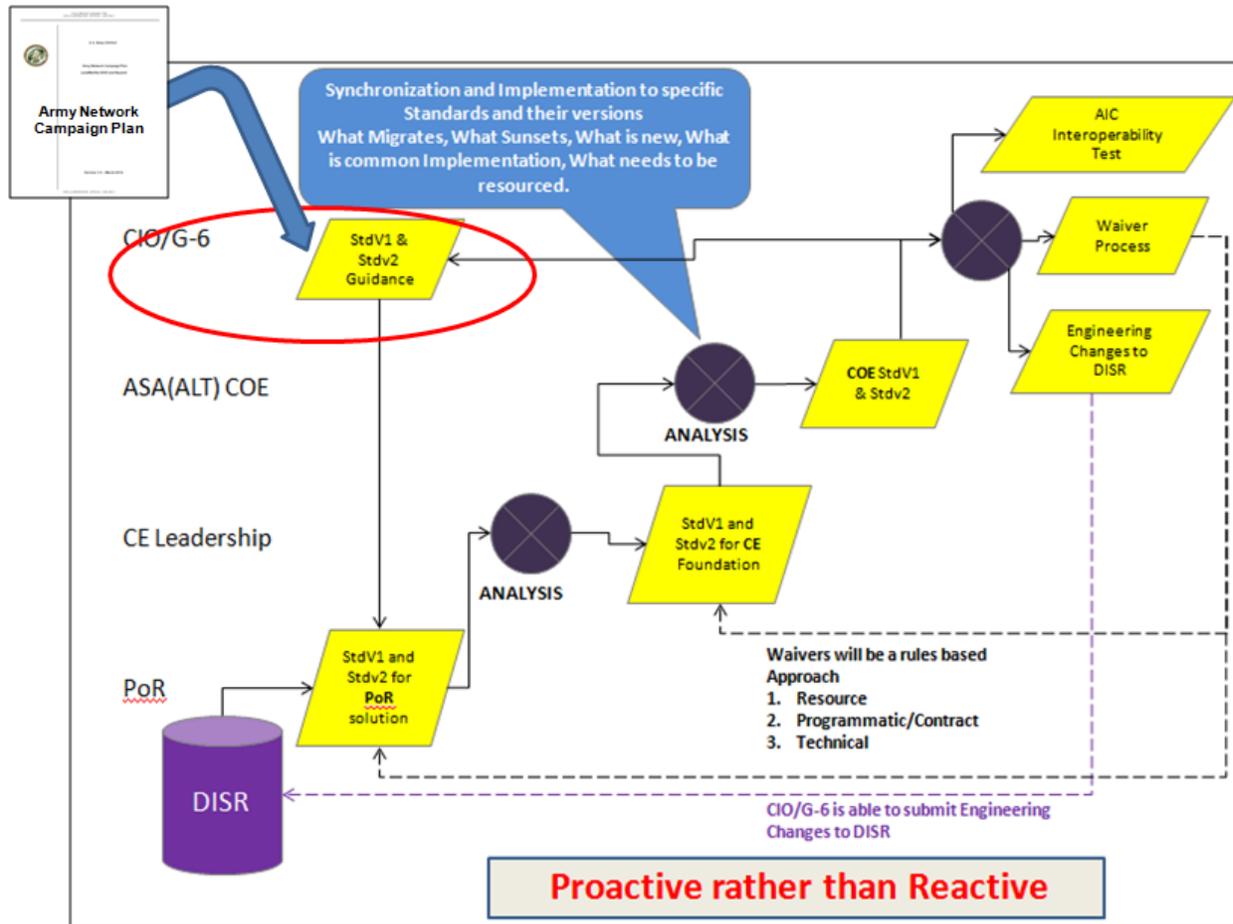


Figure 21: COE Standards Lifecycle Management Process

The process proceeds as follows:

1. CIO/G-6 produces the StdV-1/2 guidance, or Army Standards Profile Guidance, informed by the ANCP (shown in upper left area in Figure 21 circled in red)
2. PoRs use the guidance to gather standards that will meet their needs
3. PoR StdV-1/2s are analyzed and rolled up to a CE-level StdV-1/2
4. The CE-level StdV-1/2 is analyzed and rolled up to a COE-level StdV-1/2
5. COE-level StdV-1/2 is analyzed, waivers and CRs are initiated as required, and input is provided to AIC testing. This is the final baseline implementation version, approved by the PoRs, CEs, and COE Technical Advisory Board (TAB). It is configuration-managed by ASA(ALT).

Figure 21 does not fully depict, but presumes, ongoing collaboration among ASA(ALT), PoRs, and CIO/G-6 in Steps 1-4 for a given COE. A given cycle is

---

complete when all differences are resolved, a COE-level Army Standards Profile Guidance is approved, and the COE StdV-1/2 is approved by the PoRs, CEs, and TAB. At that point, configuration control for the particular COE version is turned over to ASA(ALT), as outlined in Step 5 above, and separate ASA(ALT) processes govern the approval by PoRs of any changes to the baseline. Separate from these ASA(ALT) configuration management processes, CIO/G-6 then initiates the process for the next annual Army Standards Profile Guidance, where every three years it supports a new COE version. CIO/G-6 is working to expand the process detailed in Figure 21 to incorporate other entities in addition to ASA(ALT), specifically the other Mission Areas.

Two established DISR processes are included in Figure 21:

1. DISR waiver process – shown as “Waiver Process”
2. DISR CR process - shown as “Engineering Changes to DISR”

A PoR traditionally submits a waiver for each Retired standard it intends to include in its StdV-1. However, there is a streamlined process whereby the waiver is submitted on an SoS basis on behalf of a group of programs for multiple Retired standards used across the programs. In the future, this process will be codified for the Army with an Army waiver process, including development of a CONOPS. A DISR waiver is required to use any Retired or non-DISR standard, and the COE SoS waiver combines all identified Retired standards that are needed across the COE into one waiver. CIO/G-6 evaluates waiver requests based upon the increased capability and backward compatibility of replacement standards for the individual standards included in the waiver request.

A CR is submitted when a PoR needs a standard that is not in DISR, or is not of Mandated status. A sponsor, typically a lead PoR, or an agent such as CIO/G-6 submits each individual CR to DISR for consideration as part of a well-established vetting process that is available three times annually. The Army Standards Profile Guidance includes non-DISR standards that may be CR candidates, and it is published well in advance to permit the CR process to take its course. Once the CR is approved, the standard is added to the DISR as Mandated or Emerging.

## **2.5 How to Use the Army Standards Profile Guidance**

This section provides detailed information on how to use the Army Standards Profile Guidance spreadsheet. Examples are provided within this section, specifically Big Data and Cloud Computing (section 2.5.2) and Network Integration Evaluation Technical Architecture (NIE TA) (section 2.5.3). In addition, a supplemental spreadsheet for specific “Use Cases” is provided. See Tab B for details.

---

### 2.5.1 Description and Tour of the Army Standards Profile Guidance Spreadsheet

The Army Standards Profile Guidance package, which consists of this document and the two spreadsheets referenced in Tab A and Tab B, enables the ability to search and select appropriate standards. Using the breakdowns described and illustrated in section 2.4.1 above, a user can drill down through the capability hierarchy and identify standards in a number of ways, including the following:

1. Use the “LWN-to-ATGR- Profiles” tab to trace through JIE Capability to LWN Capability to ATGR Standard Profile.
2. Use the “JCA-to-ATGR- Profiles” tab to trace through JIE Capability to JCA Capabilities (four (4) tiers) to ATGR Standard Profile to standard.
3. Use the “ATGR Profiles-to-Standards” tab to trace the Profiles to lists of standards.
4. Use the “Standards Only” tab to sort, extract, or review standards. In that tab, each standard is listed only once in alphabetical order, independent of Profiles. This tab includes all standards in the Army Standards Profile Guidance and constrains choices to those specified.

PoRs can use the spreadsheets to ensure compliance with Army and DoD guidance. The mapping and standard listings were developed by CIO/G-6, so it represents Army Technical Guidance. It also incorporates the JIE guidance hierarchy for capabilities, as well as the LWN capabilities, providing further assurance that when the PoR using it will be in compliance. The spreadsheets also enable the PoR to search logically, drilling down through the mapping, to identify ATGR Standard Profiles associated with the JIE and LWN capabilities. Each ATGR Standard Profile contains associated standards from which the PoR can choose. PoRs will select from standards that were vetted as described above. This will help facilitate interoperability and consistency across systems, consistent with the objective of the COE.

### 2.5.2 Example: Big Data and Cloud Computing

Based on the update to the "Initial Capabilities Document (ICD) For (U) LandWarNet" dated 5 March 2014, the capability "Provide Assured Information and Services" was added to the JIE Capabilities to LWN Capabilities taxonomy, shown in Figures 5 and 20. That capability relates closely to ‘Big Data’ and ‘Cloud Computing’, illustrating how the Army Standards Profile Guidance contains numerous Profiles that include developing technologies.

Figure 22 associates this LWN capability with the JIE Capability “Share”. It includes twenty-three (23) Profiles with developing technologies that support ‘Big Data’ and ‘Cloud Computing’ solutions.

JIE Capability	LWN Capability (definition omitted)	ATGR Standard Profiles (definition omitted)
Share	Provide Assured Information and Services (Capability for Cloud Computing and Big Data)	Army Unified Capabilities
		Cloud Data Virtualization Management
		Cloud Infrastructure Management
		Cloud Security
		Cloud Storage
		Data Management, Securing data stores, Key management, and ownership of data
		Data Privacy
		Data Provider - Interfaces
		Data Provider - Metadata
		Data Source - Audio, Picture, Multimedia, and Hypermedia
		Data Source - Flat Files Structure
		Data Source - Sensor network data
		Data Source - Spatial Data
		Data Source - SQL Databases
		Data Source - Streaming Data – Video
		Data Source - Streaming Data/Textual
		Data Source - Text
		Data Source - XML Documents
		Distributed Common Ground Station-Army (DCGS-A) Cloud
		HTML 5 Mobile Application Development
Infrastructure Security		
Integrity and Reactive Security		
JIE Core Data Center Solution Architecture		

Figure 22: Profiles for "Provide Assured Information and Services" LWN Capability Supporting Big Data and Cloud

For example, one of these Profiles, "Cloud Infrastructure Management", from the "ATGR Profiles to Standards" tab, contains three standards, shown in Figure 23.

Standard ID	Standard Title	DISR Status	DISR Service Area
DSP0004 v2.7.0	Common Information Model (CIM) Infrastructure, Version 2.7.0, 2012-04-22	E	System Management Services
DSP0263 v1.0.1	Cloud Infrastructure Management Interface 5 (CIMI) Model and RESTful HTTP-based Protocol: An Interface for Managing Cloud Infrastructure, 2012-09-12	E	Network Technologies
GFD-P-R.184	Open Cloud Computing Interface - Infrastructure, June 21, 2011	N	

Figure 23: Standards for "Cloud Infrastructure Management" Profile Supporting Big Data and Cloud (See DISR Statuses Legend in Figure 10)

The standards identified in Figure 23 are representative of what PoRs will encounter within these Profiles. They include standards with DISR status of 'E', or Emerging, and 'N', or non-DISR. Although these three standards were flagged for possible inclusion in the StdV-2, they could mature in a timeframe for inclusion in DISR. CIO/G-6 can provide assistance with CRs to make this happen.

### 2.5.3 Example: Network Integration Evaluation Technical Architecture (NIE TA)

The Army Standards Profile Guidance supports the NIE by providing an enterprise technical architecture that maps to any NIE capability. The NIE is driven by the gaps that are identified early in the Agile Process. For example, one gap for which solutions may be sought is the LWN capability "C2 on the Move". The Army Standards Profile Guidance shows the "C2 on the Move" capability in the "LWN-to-ATGR- Profiles" tab, as shown in Figure 24. "C2 on the Move" includes 15 Profiles, including some that refer to GTPs in the DISR, and others that refer to specific system nodes within the NIE systems architecture, such as Point of Presence (PoP) and SIPR-NIPR Access Point (SNAP).

JIE Capability	LWN Capability (definition omitted)	ATGR Standard Profiles (definition omitted)
Connect	Provide C2 On the Move	GTP003 - Ku-Band Satellite Communications
		GTP004 - Ka-Band Satellite Communications
		Mobile Ad Hoc Network (MANET)
		Mobile IPv4 Performance Optimization
		Mobile IPv6
		Mobile IPv6 Basic Mobility Services
		Over-the-Air-Rekeying (OTAR)
		Point of Presence (PoP)
		SIPR-NIPR Access Point (SNAP)
		Tactical Radio BLOS Communications
		Tactical Radio Interface Specification
		Tactical Radio LOS Communications
		WIN-T Soldier Network Extensions (SNE)
		Wireless LAN (WLAN)
Wireless Network after Next (Wnan)		

Figure 24: Profiles Supporting NIE for LWN Capability “Provide C2 On the Move”

The Point of Presence (PoP) and SIPR-NIPR Access Point (SNAP) Profiles simply provide links to the appropriate information sites on these system capabilities. The GTP profiles provides a list of the latest ‘Mandated’ standards listed on DISR as specified for those GTPs. Other Profiles, like the “Mobile Ad Hoc Network (MANET)”, provide primarily ‘non-DISR’ standards, shown in Figure 25.

ATGR Standard Profile	Standard ID	Standard Title	DISR Status
Mobile Ad Hoc Network (MANET)	ETF RFC 3626	Optimized Link State Routing Protocol (OLSR), October 2003	A
	ETF RFC 5444	Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format, February 2009	N
	ETF RFC 5497	Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs), March 2009	N
	ETF RFC 5614	Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding, August 2009	N
	OSPFv3-MDR	MANET Extension of OSPF using CDS Flooding	N

Figure 25: Standards Supporting NIE for “Mobile Ad Hoc Network (MANET)” Profile (See DISR Statuses Legend in Figure 10)

These standards can support solutions to any gap identified for any NIE. The Army Standards Profile Guidance provides detailed information about the technical standards the Army is working on. Vendors are not necessarily required to implement these standards, but are required to provide interoperability. Once the gaps are identified, CIO/G-6 can generate a list of the gap-related standards and technologies and coordinate any public release as required.

---

## **Tab A Army Standards Profile Guidance for COEv3 - Core**

The first of two Excel spreadsheets that accompanies this document is the core data portion of the Army Standards Profile Guidance for COEv3. It provides the standards, the mappings to JIE, JCA and LWN capabilities, and ATGR Standard Profiles. It also provides definitions for the JIE and LWN capabilities and ATGR Standard Profiles. The file name for this Excel spreadsheet is:

“20140815-Appendix\_C-TAB\_A-Core-Army\_Standards\_Profile\_Guidance\_in\_Support\_of\_COE\_v3.xlsx”

---

## Tab B Army Standards Profile Guidance for COEv3 - Use Cases

The second of two Excel spreadsheets that accompanies this document provides additional data that supplements the first spreadsheet (referenced in Tab A), or core data portion of the Army Standards Profile Guidance for COEv3.

This Excel spreadsheet provides a set of the “Use Cases” for the following:

- Big Data
- Cloud Computing
- Content Discovery & Delivery
- Cyber Security
- Geospatial Intelligence
- Multiprotocol Label Switching (MPLS)
- Network Operations (NetOps)
- Unified Capabilities (UC)

Each Use Case provides a listing of standards that apply to a set of the capabilities, generalized scenario, or example, in support of the architecture design and implementation decisions. The user can select any needed standards from the Use Case standards listing based on their program’s specific scope.

The purpose of these Use Cases is to provide pre-selected listings of standards that apply to specific broad capabilities of special significance or importance to the Army. All standards pre-selected for a Use Case are extracted from the LWN or JCA mapping contained in the Army Standards Profile Guidance for COEv3 spreadsheet.

The Use Cases are provided to assist users in identifying standards for particular areas of interest. Other Use Cases will be added as interest and needs demand. Each individual Use Case includes a detailed scope for the Use Case.

The file name for this Excel spreadsheet is:

“20140815-Appendix\_C-TAB\_B-Use\_Cases-Army\_Standards\_Profile\_Guidance\_in\_Support\_of\_COE\_v3”

---

## Acronyms

AIC	Army Interoperability Certification
ANCP	Army Network Campaign Plan
ASA (ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ATGR	Army Technical Guidance Repository
BMA	Business Mission Area
CAC	Common Access Card
CE	Computing Environments
CE WG	Computing Environment Working Group
CIO	Chief Information Officer
COE	Common Operating Environment
DIMA	DoD Intelligence Mission Area
DISR	Department of Defense IT Standards Registry
DoD	Department of Defense
EIEMA	Enterprise Information Environment Mission Area
ICD	Initial Capabilities Document
IT	Information Technology
JCA	Joint Capability Area
JIE	Joint Information Environment
LAN	Local Area Network
LWN	LandWarNet
LWN CS	LandWarNet Capability Sets
MC	Mission Command
NeMC	Network-enabled Mission Command
NetOps	Network Operations
POM	Program Objective Memorandum
PoR	Program of Record
SAIS-AOD	CIO/G-6 Information Architecture Division
SoS	System of Systems
StdV-1	Standards Profile
StdV-2	Standards Forecast
SWB	Software Blocking
TRADOC	Training and Doctrine Command
WMA	Warfighter Mission Area
WSR	Weapon System Review