Definitions and Guidance for the Common Operating Environment

Annex B to LandWarNet 2020 and Beyond Enterprise Architecture

Version 2.0

As of: 1 August 2014

Executive Summary

On 28 December 2009, the Vice Chief of Staff of the Army directed CIO/G-6 to develop "as-is" and "end-state" network architectures to guide evolution of network procurements and enhancements. In 2011 the Army instituted the Common Operating Environment (COE), a centrally approved set of computing technologies and standards that will enable rapid development of secure and interoperable applications to which the network must adhere. COE addresses the specifics of the standards-based network model and defines minimum configurations for the Army computing environments from the Enterprise server to mobile and small handheld devices.

Since then, CIO/G-6 developed the *LandWarNet 2020 and Beyond Enterprise Architecture* to provide direction in support of the Army Network Strategy and to provide the acquisition community and industry with the minimum technical standards for development of future network and network dependent systems. The Definitions and Guidance for the Common Operating Environment (COE) document is a key part of the broader enterprise network architecture.

The Army Enterprise enables Unified Land Operations[1] through all phases of training and deployment. The *Definitions and Guidance for the COE* defines:

- Network considerations
- Computing Environments (CEs)
- Technical Reference Model (TRM)
- Control Points and Testing for the COE

Implementation of this architecture will enable the Army to develop, test, certify, accredit and deploy software capabilities more rapidly. Additionally, it will improve overall security and interoperability and reduce costs without the introduction of harmful or unexpected behavior.

Approved by:

BLOHM.GARY.W.1228949589

Digitally signed by BLOHM.GARY.W.1228949589
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=BLOHM.GARY.W.1228949589
Date: 2014.07.30 16:09:24 -04'00'

Gary W. Blohm
Director Army Architecture Integration Center

[1] Army Doctrine Publication 3-0, dated 10 Oct 2011

Table of Contents

1 Introduction

1.1 Background

Over the past several years the Army has managed Warfighting, Business and Enterprise Network Modernization Strategies separately. Current plans are to integrate Warfighting, Business and Enterprise Network Modernization by synchronizing these strategies based on an Army Common Operating Environment (COE).

On 28 December 2009, the Vice Chief of Staff of the Army directed CIO/G-6 to develop "as-is" and "end-state" network architectures to guide the evolution of network procurements and enhancements. Since then, CIO/G-6 developed the *LandWarNet 2020 and Beyond Enterprise Architecture*[2] and related documents to provide direction for the entire Army Enterprise Network and to provide the acquisition community and industry with the minimum technical standards for development of future network and network dependent systems. This *Annex B - Definitions and Guidance for the COE* is a key part of the broader Army enterprise network architecture which is the Army Service component of the DoD Information Enterprise (encompassing the Joint Information Environment (JIE). See LandWarNet 2020 and Beyond Enterprise Architecture for more details.

Achieving the vision of a COE and *LandWarNet 2020 and Beyond* is highly dependent on the alignment and synchronization of Army processes, including strategy development, portfolio management, architecture and acquisition. It is key that LandWarNet stakeholders, principally ASA(ALT), the Training and Doctrine Command (TRADOC), Forces Command (FORSCOM), the Office of Business Transformation (OBT), and Headquarters, Department of the Army (HQDA), understand and share this vision, and jointly align their Information Technology (IT) strategies and activities with the desired LandWarNet end-state as described in the *LandWarNet 2020 & Beyond Strategy*, *LandWarNet Integrated Network Plan* and *LWN 2020 & Beyond Enterprise Architecture.* Well-defined, understandable and commonly shared enterprise network architecture is a primary method by which the Army will achieve the required unity of effort, and promote information sharing and interoperability among Army systems. Figure 1 provides a visual of the requirements, strategy and architecture alignment.

[2] Signed 07 Aug 2013

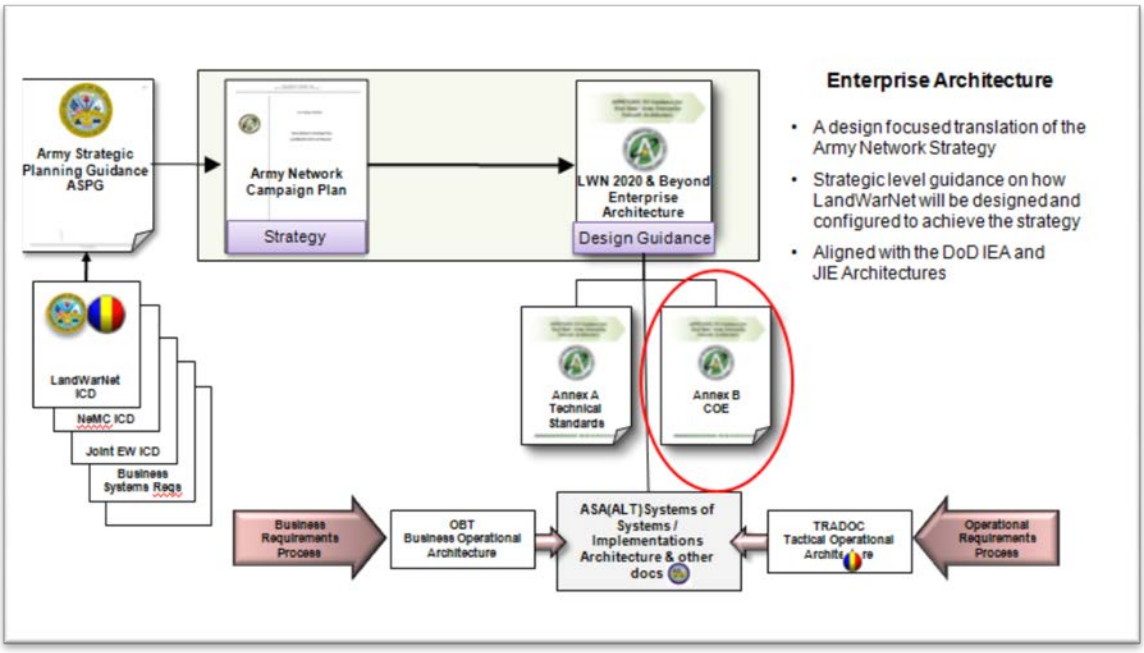

Figure 1: Requirements, Strategy and Architecture Alignment

The *LandWarNet 2020 and Beyond Enterprise Architecture* and related documents are considered living documents. They will continue to evolve in a coordinated manner in order to keep up with the rapid changes in technology. This document is the revision of the first version of Annex B (old Appendix C) approved in Oct 2010. Annex B will be validated and updated as required and posted on the public CIO/G-6 (Architecture) website: http://ciog6.army.mil/.

Annex A (Technical Standards Guidance) is supported by the Army Technical Guidance Repository (ATGR) containing standards based on the Department of Defense (DoD) IT Standards Registry (DISR) baseline and process. The ATGR is accessible with a Common Access Card (CAC). All standards posted in the ATGR will be used in the development of technical profiles, as well as building blocks for the hardware and software device configurations.

Stakeholders can submit Change Requests for Annex B to the CIO/G-6 Architecture Configuration Control Team (ACCT). More information can be found on https://www.kc.army.mil/TRM_TOOL/default.aspx.

1.2 Purpose

Execution of the *Army Network Strategy - Empowering America's Army Through LandWarNet* and *LWN 2020 & Beyond Enterprise Architecture* will result in unified Army Mission Command and Network Modernization strategies to support Army Investments/Program Objective Memorandum (POM) strategy. An implemented COE will greatly increase the end-to-end information interoperability, promote operational

relevancy and decrease time for development and certification while reducing overall costs. It will better enable interoperability from the standpoint of information exchanges with coalition and other partners.

The purpose of Annex B is to provide terms of reference definitions and architecture guidance for the implementation of the COE to achieve a balance between unconstrained innovation and standardization. Annex B establishes the Technical Reference Model (TRM) to define how COE fits within the enterprise network architecture. The TRM establishes the IT ecosystem that standards will support. Annex A (Technical Standards Guidance) to the LandWarNet Enterprise Architecture combined with the ATGR will provide the guidance for the CIO/G-6 to produce an Annual Standards View (StdV-1) Standards Profile to guide the development of COE. Emerging standards that promise to address capability gaps will be analyzed, rigorously tested and when mature enough for the operational environment, incrementally incorporated into the glide path to end-state EA. In the commercial sector, off-the-shelf devices, i.e. Commercial Off-the-Shelf (COTS) have become inexpensive relative to specialized Army-developed hardware and software.

With a COE, the Army establishes a framework similar to industry best practices. In addition, Army communities of interest are better enabled to produce and/or acquire high-quality applications quickly and cheaply, improve security and defense posture, reduce the complexities of configuration and support, and streamline and facilitate training. This is a wholesale shift from the Army's traditional procurement of systems with dedicated software and hardware. Applications will now be designed, developed and deployed on a common computing environment, allowing the end user to download what is needed when it is needed. It should be noted that when COTS out-of-the-box solutions do not satisfy a military-specific requirement, traditional Army procurement processes will be utilized to address these requirements by exception.

2 Army Common Operating Environment

This Section will present the definitions, constructs, and considerations associated with the COE. The COE can be viewed from several perspectives. The materials presented herein are organized according to the overall required computing devices, the network and physical connectivity that affect them. The foundation for the evolutionary development of the Computing Environments (CEs) is based on sets (i.e. profiles) of approved technical standards that are required to effectively implement the COE. This foundation is consistent with and complimentary to the Army enterprise network architecture, and it will provide overarching network considerations and define the CEs that support the execution of Army missions.

The COE will leverage Open Source and COTS solutions and other commercial capabilities first, using Army open source selection policies and practices. Establishing standard interfaces through the use of open standards will enable continuous modernization while reducing system reset and upgrade/life-cycle costs. [3]This will be accomplished by leveraging market-leading COTS technologies to the fullest extent possible, and utilizing approved solutions for military-specific needs. Customization of packaged applications will be minimized and re-use of existing packages will be exploited wherever possible.

Implementation of COE will enable the Army to develop, test, certify, security accredit and deploy software capabilities more rapidly by improving security, interoperability and reducing costs. The CIO/G-6 and the ASA(ALT) are committed to setting the conditions for the Army to produce or acquire high-quality applications rapidly, while reducing the complexities embedded in the design, development, and testing and deployment cycle. Annex B and the *ASA(ALT) COE Implementation Plan* provide direction to Government and industry partners to standardize information resources, systems, end-user environments and the software development kits required to produce them. It is necessary to establish streamlined enterprise software development processes that rely on common pre-certified, accredited and reusable software components and develop deployment strategies that give users direct access to new capabilities.

2.1 The Common Operating Environment Perspective

The COE, when implemented across the Army, will greatly increase interoperability, agility and security; decrease the time for development and delivery to the field, and reduce overall costs.

The COE v1.0 baseline focuses on generating enhanced situational awareness, improved performance and realized efficiencies to the Warfighter through the implementation of CE systems and Cross-Cutting Capabilities (CCCs). It is documented by authoritative information in the COE Implementation Plan revision 3.0

[3] Federal Acquisition Regulation (FAR) Part 12, section 12.5.2.1 Commercial Off the Shelf (COTS), dated 29 May 2014

and the Integrated System Engineering Plan (ISEP). This guidance will be incorporated into an update of the COE Implementation Plan. The COE is a common software development foundation where mission applications are developed and run in support of the Army full range of operations for the Institutional and Operational Forces.

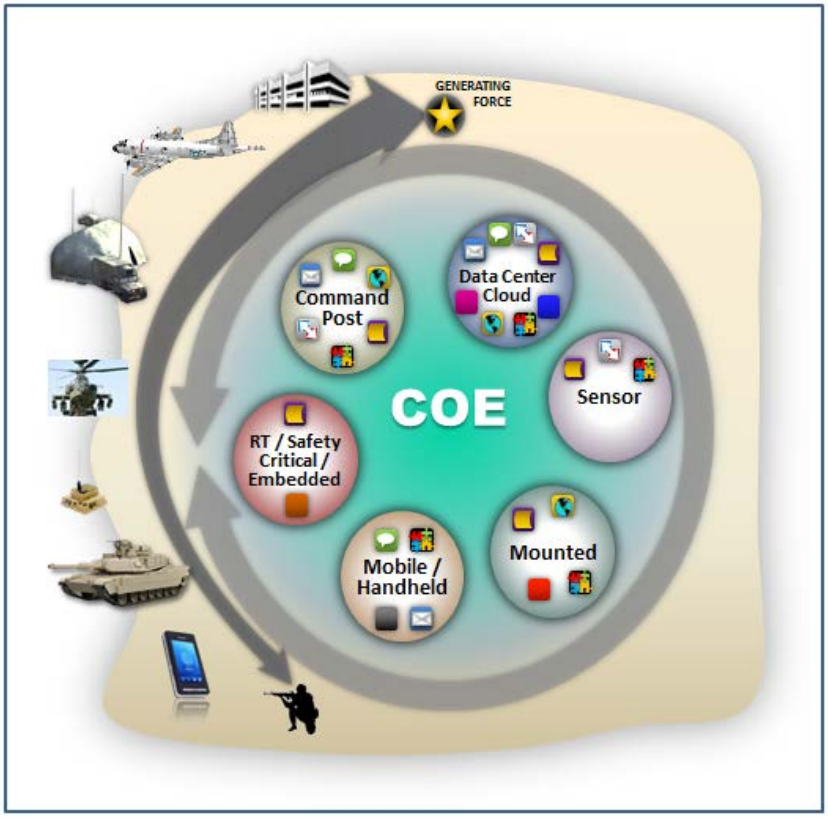

Figure 2: COE Overview

2.2 The Computing Environment (CE)

The CE is a logical grouping of systems with similar characteristics (deployment/echelonment, environmental, transport dependencies, form factors, etc.) used to organize the COE. A CE comprises the necessary hardware, operating system, libraries and software required to run applications within the COE. In order to create efficiencies, eliminate redundant activities and to inform POM investment decisions, the ASA(ALT) assigned Program Executive Offices (PEOs) leads for each CE:

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

CE Working Groups (CEWG) are organizations chartered by ASA(ALT) to produce and manage the Operating Environment for the sets of systems within the domains established by each CE's operational and environmental characteristics.

2.2.1 Data Center/Cloud/Generating Force CE

Provides a service-based infrastructure for hosting and accessing enterprise-wide software applications, services and data. The Data Center/Cloud/GF CE consists of common services and standard applications for use by a large number of users over wide area networks. This CE also includes the Army's Enterprise Resource Planning (ERP) systems. The solutions being developed include:

- Cloud Software Development Kit (SDK) (i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Cloud Management Services, and Support for Software as a Service (SaaS))
- Deployable Data Centers

2.2.2 Command Post (CP) CE

Provides client and server software and hardware, as well as common services (e.g., network management, collaboration, synchronization, planning, analysis) to implement mission command capabilities at the CP. The solutions being integrated include:

- Common Geospatial Foundation
- Ozone Widget Framework
- Hardware Consolidation

2.2.3 Mounted CE

Provides operating and run-time systems, native and common applications and services (e.g. awareness, execution functions, integration of local sensors),SDKs and standards and technologies to implement Mission Command integrated onto ground and airborne platforms. The solutions being developed include:

- Common Geospatial Foundation
- Android Operating Environment
- Mounted CE Playbook

2.2.4 Mobile/Handheld CE

Provides operating and run-time systems, native and common applications and services, SDKs and standards and technologies for hand held and wearable devices. The solutions being developed include:

- Mobile COTS Framework.

- Minimum Standards Configuration
- Common Technical Implementation (Nett Warrior)

2.2.5 Sensor CE

Provides a common interoperability layer, implementing standards and technology for data services, NetOps and security for specialized, human-controlled or unattended sensors. The Sensor CE does not specify specific hardware and software for the sensors. The solutions being developed include:

- Common Sensor Data Exchange Model
- Sensor Service Framework

2.2.6 Real-Time/Safety Critical/Embedded CE

Defines a COE for systems operating in a real-time, safety critical, or embedded environment while ensuring that opportunities for commonality and interoperability with other CEs are maintained fullest extent possible. The solutions being developed include:

- Future Airborne Capability Environment (FACE) Real-time Interoperability Framework (RTIF)
- Vehicular Integration for C4ISR/EW Interoperability (VICTORY) RTIF.
- Ordnance Interface Standards (OIS) RTIF
- Engagement Operations (EO) RTIF

2.3 Warfighting Functions

Army Doctrine Reference Publication – *3.0 Unified Land Operations* defines the following Warfighting functions: mission command, movement and maneuver, intelligence, fires, sustainment, and protection. In 2014, the Army approved adding a seventh Warfighting function – Engagement. Warfighting functions are a grouping of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives. Army forces use the Warfighting functions to generate combat power. Combat power is the total means of destructive, constructive, and information capabilities that a military unit/formation can apply at a given time. Army forces generate combat power by converting potential into effective action. The core function of each COE CE is to support the Warfighter in the execution of the seven Warfighting Functions. The COE and CE working groups will address the operational GAPs identified by TRADOCs Capability Gap Analysis and develop new capabilities that will close the GAP for their CE. TRADOC is developing requirements documents to leverage the agility of COE by developing a governance system to ensure requirements development documents are

consistent with the COE vision. The LandWarNet 2020 and Beyond Enterprise Architecture will align with the TRADOC requirements documents to meet needs of the Warfighter.

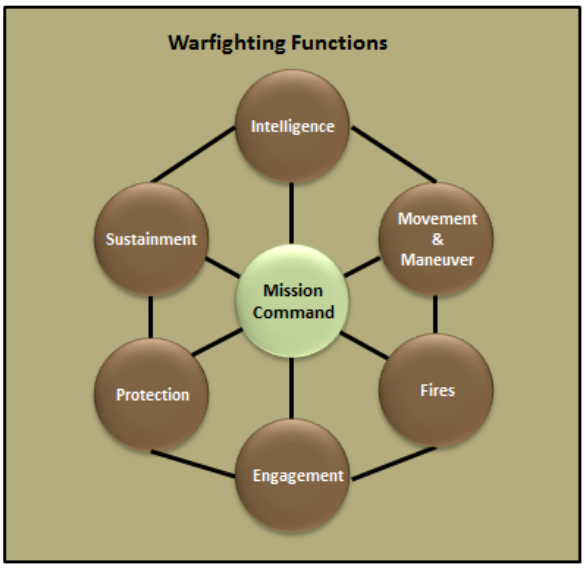

Figure 3: The Seven Warfighting Functions

The Warfighting Functional Area is the highest level of operational construct supported by Mission Command. Each Warfighting Functional Area can be broken down further into specific functions and tasks described by specific conditions performed by certain standards.

2.4 Business Mission Area (BMA) Domains

Similar to the Warfighting Functions, the BMA functional areas are organized around six anticipated BMA domains that align to areas of common operational and functional requirements. A BMA domain includes the core business functions of that mission subset and the business systems that predominately support one or more of the 15 end-to-end (E2E) business processes.[4] The focus of COE is to support Army BMA users across one or more of the COE CEs in support of the six BMA domains below. Note that the Defense Security Enterprise is under development. The COE and CEWGs will address the business operational gaps identified and develop new capabilities that will close the gaps for their CE in support of the BMA.

1. Acquisition
2. Financial Management
3. Human Resource Management
4. Logistics
5. Installations, Energy & Environment

[4] Army Business Management Strategy & Implementation Plan (ABMS) dated 3 Dec 13.

6. Defense Security Enterprise (In Development)

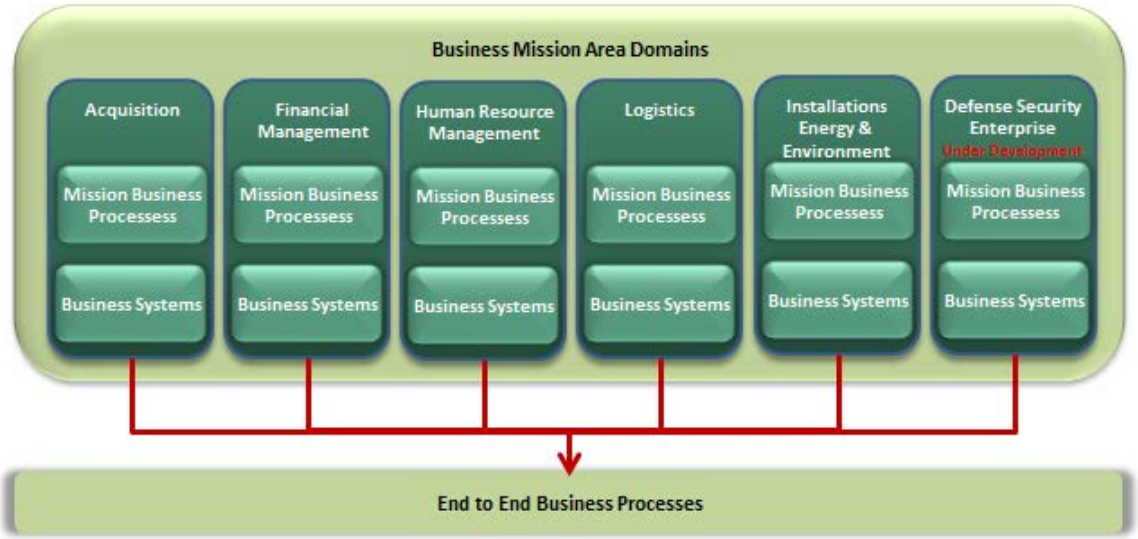

Figure 4: BMA Domains

2.5 COE Technical Reference Model (TRM)

The COE manages the planned capabilities through the COE Technical Reference Model (TRM) and the COE Technical Roadmap.[5] The COE TRM, depicted within Figure 5, illustrates the technology strategy of the COE in a single diagram. It shows the technical elements of the COE and how they fit together. It delineates the responsibilities of each COE organization and what technical domains fall outside the COE. The COE Technical Roadmap assigns planned capabilities to each layer of the TRM. The TRM does not replace, or should not be confused with, the Open System Interconnection (OSI) model that defines a networking framework for implementing protocols in seven layers.

[5] SharePoint folder [ASA(ALT)SOSE&I]>Common Operating Environment COE_WG>COE Technical Roadmap]

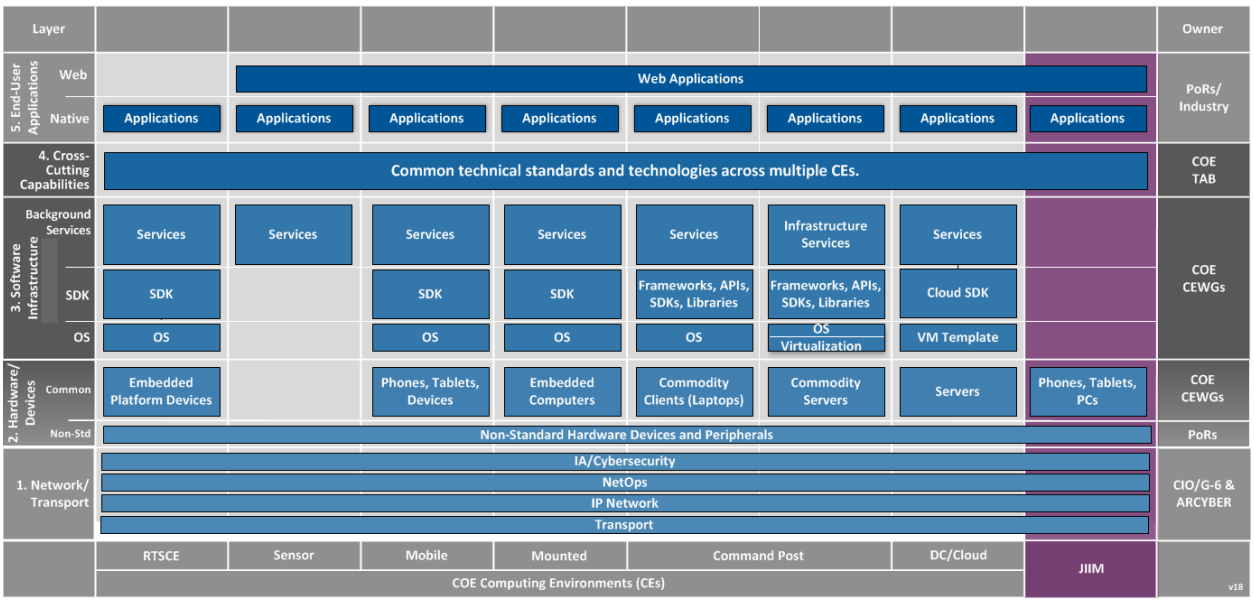

Figure 5: COE Technical Reference Model

The COE TRM uses a five-layer model to describe its technical ecosystem. Layers 1, 3 and 5 are further subdivided in the TRM for better specificity. The COE has direct responsibility for two of the five layers: 3 and 4. Every layer relies on the capabilities of the layer below it.

The columns in Figure 5 divide the TRM by organization. These are primarily the COE CEs, but also include Joint, Interagency, Intergovernmental, and Multinational (JIIM) partners. The CP CE differs from the others in that it has two sub-environments: client and server.

The leftmost column contains the names of the layers and sub-layers. The rightmost column indicates which acquisition organization has primary responsibility for its row.

Layer 5: End-User Applications

Starting with the top row, Layer 5 is the end-user applications layer. It is subdivided into web and native applications. End user applications include COTS Software (SW) and Government Off-The-Shelf (GOTS) SW applications. Web applications include Simple Object Access Control (SOAP) or Representational State Transfer (REST) web services, websites, and sophisticated web applications. Microsoft SharePoint, Tactical Ground Reporting System (TIGR) and Command Web are all web applications under this definition.

Layer 4: Cross-Cutting Capabilities (CCCs)

The CCCs occupy the next layer in the TRM and are the key component of the COE common foundation. These capabilities are common technical standards and protocols that are defined and implemented consistently across two or more CEs, e.g. Common Map Overlay, Common Chat Capability. CCCs are the cornerstone of the COE. CCCs

ensure that the applications in each CE ensure that Soldiers have the same access to a capability in any environment. CCCs materiel solutions may include COTS and/or GOTS SW applications.

Layer 3: Software Infrastructure

The Software Development Infrastructure, the second key component of the COE common foundation, is the next layer down in the TRM. This is the core of what the COE is - a means to provide commonality across the software development activities in the Army. It is subdivided into three parts: operating system (OS), SDKs and background services, and consists of both runtime and build-time components. These may include COTS and/or GOTS SW components. Together with the CCCs in Layer 4, the software development infrastructure defines the COE.

- **Operating System (OS).** The OS designates the operating system that is standard for that CE and on which all end-user applications must build; for example, Android, Linux, or Windows. The RTSCE may identify several operating systems due to the nature of its devices. The server environments are virtualized and so can support multiple OSs running over a hypervisor.
- **Software Development Kits**. The SDK layer designates a set of software libraries, frameworks, APIs and SDKs specific to the OS and the hardware of its CE, which provide many of the basic utility functions of the CE and facilitate the development of end-user applications by enabling POR focus on value-added mission capabilities. The Joint Battle Command Platform (JBC-P) Platform Development Kits (PDK), VICTORY, and FACE are examples.
- **Background Services.** The third sub-layer within the software infrastructure, as defined and developed by the Computing Environment, is background services. These are utility applications that run in the background and are not visible to end-users. These include, for instance, web servers, database servers and map servers. The Enabling Technologies that support the development of the Cross-Cutting Capabilities could be considered a Background Service that is mandated across each of the Computing Environments.

Layer 2: Hardware

The next layer in the COE TRM is the Hardware/Device layer. This layer is depicted because it is an essential component of integration and testing. Technical specifications of hardware devices, such as processor type, clock speed, memory and power consumption all affect the layers above it. They also impact the performance of and constrain the applications and services being requested for a particular mission within a specific CE.

Within ASA(ALT) two initiatives are in place for Platform-based standardization and reducing Size, Weight, and Power-Cooling (SWaP-C): VICTORY, focused on Army Ground Vehicles integration for C4ISR & EW interoperability, and FACE for Airborne Platforms.

Common hardware will leverage COTS to the fullest extent possible to reduce system

reset and upgrade/life-cycle costs. Common hardware platforms will be identified by the COE CEWGs wherever applicable, while non-standard hardware devices and peripherals will continue to be identified by PEOs/PMs as needed.

Layer 1: Network/Transport

The final layer in the COE TRM is the Network/Transport layer. It is depicted in the COE TRM because it is an important component of interdependency. This layer has sub-layers of Transport (Terrestrial, SATCOM, and Infrastructure), Internet Protocol networking (routing), NetOps and Information Assurance/Cybersecurity.

- **Transport.** A resilient transport network provides regionally-aligned forces, Homeland Defense, Defense Support of Civil Authorities (DSCA) and Unified Action Partners continuous advantage across all operational phases by leveraging existing capabilities and implementing the Army's Network 2020 and DOD's Joint Vision 2020 architectures. The measures of success are delivering increased network availability by effective use of network capacity and increasing the network capacity to Regionally-aligned/Unified Action Partners.
- **Internet Protocol (IP) Network.** IP commercial networks can provide commercial access to the Internet. Properly secured access to the Non-classified Internet Protocol Router Network (NIPRNet) can also be supported using secure access and authentication procedures and mechanisms (e.g., CAC, Web–Secure Sockets Layer, Transport Security Layer, and Virtual Private Networks). It can function on commercial networks and NIPRNet with typically good performance. NIPRNet typically provides good performance and availability. Information access within this environment can be characterized as:
    - Unclassified and releasable to the public
    - Public but regulated by firewall regulations and policies
    - Protected as 'For Official Use Only'
    - Protected as 'Controlled Unclassified Information'
- **Network Operations (NetOps).** In the context of the COE TRM, NetOps provides the ability to configure and operate all of the entities within the COE (i.e., across COE Layers 1 - 5). NetOps utilizes COE capabilities that are provided in the COE layers themselves, but provides an end-to-end function that enables the layers to work in synchrony with one another to produce an enterprise-level capability.
- **Information Assurance (IA)/Cybersecurity.** In the context of the COE TRM, IA/Cybersecurity provides the mechanisms to protect information that is saved locally, protects the data in transit to and from the cloud, and protects the data at the Enterprise cloud service broker and the IT components that reside at every COE layer. The role of IA/Cybersecurity in the COE is to assure the confidentiality, integrity, and availability in all aspects of the COE, particularly with regards to the informational interfaces between layers.

The JIIM Column

The purple column is a reminder of the joint and coalition nature of the operational environment. In addition to standardization within and across Army CEs, the COE recognizes JIIM interoperability as equally vital. The Technical Advisory Board (TAB) is responsible for ensuring that the CCCs are staffed and socialized with relevant JIIM partners.

The Owner Column

This column identifies the owner of principal responsible for each respective layer, or sub-layer where applicable, of the COE TRM.

2.6 Program Protection

Program Protection processes and procedures will apply to the development and evolution of COE hardware and software architectures, capabilities, and components. This would include the identification of vulnerabilities and the implementation of Information Assurance, Software Assurance (e.g., software design and code inspections, vulnerability and attack pattern assessments, and penetration tests), Supply Chain Risk Management and Generic Program countermeasures. Program Protection Planning has been directed by the Office of the Secretary of Defense on all acquisition programs. CIO/G-6 or ASA(ALT) will promote cursory System of Systems Information Assurance Evaluation/ Blue Team Assessment during the PEO Family of Systems testing to identify system weaknesses and vulnerabilities early in the acquisition process.

3 Control Points and Testing

In generic terms, Control Points will provide technical services for testing and verifying systems. The objective of implementing a Control Point testing methodology is to improve system integration, reduce the time necessary to identify and correct software faults and expedite attainment of Army Interoperability Certification (AIC).

Integration Test Beds will be established that replicate the communications and computing infrastructure at various echelons of the Army. These controlled or baseline configurations of equipment, with Control Point software evaluation tools, will underpin Software Quality Assurance efforts. Control Point Specifications will guide evaluation of CE portfolios of systems software to ensure proper integration, performance, effectiveness and suitability in a realistic environment. Developmental test results will be documented in the COE Verification Report and submitted to the HQDA CIO/G-6, the AIC Authority. HQDA CIO/G-6 will be the proponent for a test of the final integrated set of software by a CIO/G-6 designated Test Agent with appropriate support for certain security domains. This test will assess systems integration and interoperability performance against selected key vignettes or use cases of approved mission threads. Shortfalls in required performance will be captured in Test Incident Reports and provided the materiel development community for corrective action. An AIC will be issued for each baseline set of software successfully demonstrating it meets minimum military requirements.

3.1 Definitions and Concepts

Developing software within the COE is intended to facilitate rapid integration and engineered interoperability for Army software systems. The concept of a Control Point has been introduced to manage the development and verification of the elements that comprise the COE and to promote rapid integration. The use of CPs will enable successful Integration and Interoperability Exercises (I2E) that can expedite Army software application fielding and facilitate the ultimate goal to rapidly field capability to the Warfighter.

CPs are the primary COE construct to facilitate interoperability and provide for more efficient integration by rigorously capturing and controlling interfaces between CEs. This enables verification activities across CEs, while providing each Computing Environment more flexibility for implementing interfaces within the CE, as long as the inter-CE interfaces are met.

3.2 Definition of Control Points

The purpose of this section is to describe the concept of CPs between CEs to include the definition of terms and the mission and intent of CPs.

A Control Point is defined as the collection of interfaces between one computing environment and another that is managed by the COE Chief Engineer. Additional CPs may be defined for critical interfaces between systems within a given CE, or for critical interfaces with systems and capabilities external to the COE. The default case is the cross-CE CP, with the processes for this case defined herein.

CPs enforce interoperability, security and gateways between CEs, and provide a basis for formal verification of the interfaces.

COE engineering has identified 15 potential Control Points for COE (Figure 6):

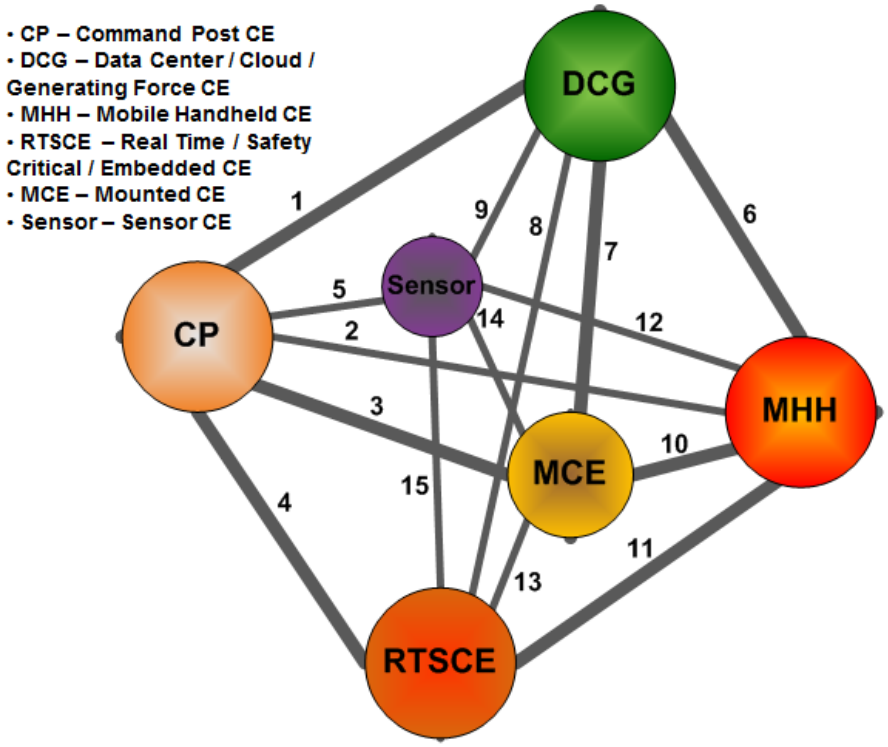

Figure 6: Control Points

The standard identification for these CPs is as follows:

1: Command Post – Data Center/Cloud/Generating Force (CP_DCG)

2: Command Post – Mobile Handheld (CP_MHH)

3: Command Post – Mounted CE (CP_MCE)

4: Command Post – Real-Time/Safety Critical/Embedded (CP_RTSCE)

5: Command Post – Sensor (CP_Sensor)

6: Data Center/Cloud/Generating Force – Mobile Handheld (DCG_MHH)

7: Data Center/Cloud/Generating Force – Mounted CE (DCG_MCE)

8: Data Center/Cloud/Generating Force – Real-Time/Safety Critical/Embedded (DCG_RTSCE)

9: Data Center/Cloud/Generating Force –Sensor (DCG_Sensor)

10: Mobile Handheld – Mounted CE (MHH_MCE)

11: Mobile Handheld – Real-Time/Safety Critical/Embedded (MHH_RTSCE)

12: Mobile Handheld – Sensor (MHH_Sensor)

13: Mounted CE – Real-Time/Safety Critical/Embedded (MCE_RTSCE)

14: Mounted CE – Sensor (MCE_Sensor)

15: Real-Time/Safety Critical/Embedded – Sensor (RTSCE_Sensor)

3.3 **Mission/Intent and Concepts for Control Points**

Control Points are the primary COE mechanism to facilitate large scale interoperability across a fielded *COE Version*. The set of systems in a Computing Environment implement the Control Point and are verified against that Control Point's Specification. Integrating the System of Systems should become a problem of managing 15[6] Control Points across the 6 Computing Environments, rather than over 5000 interface definitions against hundreds of individual systems. Investments in Control Point verification and testing provide a better Return on Investment (ROI) as they are shared across a much wider number of programs.

Control Points are established through an agreement between the two Computing Environment Working Groups and with the advice and consent of the COE Chief Engineer and the overarching COE Governance Forum. A Control Point Specification is produced for each Control Point, for each *COE version,* by the CEWGs contributing to the Control Point.

Control Point Specifications are intended to be **complete** and **comprehensive**. The Control Point Specification captures the entire interface; there should be no part of the interface not captured in the Control Point Specification. The Control Point Specification (CP Spec) includes sufficient interface details so that implementers can use the CP Spec for development and testers can use the CP Spec for interface test and verification.

The level of detail in a CP Specification is informed by real-world problems observed at CTSF and other test venues, with the expectation that negotiating the CP Spec will identify and resolve interface problems during development. The CP Specification will assist developers and testers in isolating and resolving problems prior to integration.

In addition to capturing the interfaces, the CP Spec will also document verification approaches. Thus, the CP Spec, as a basis for verification, includes both "what" and "how to test" as an agreement between the two CEs. Computing Environment Working

[6] Each CE has interfaces with 5 other CEs, yielding 30 combinations. But each CP captures both directions of the interfaces, thus 15 Control Points.

Groups and their constituent PEO/PMs can use this information to understand the verification approach. It may also be used as a basis to contribute test tools, techniques, and methodologies between the CEs that are party to the Control Point and to the integration test/verification community at large. The ability to share investments in tools is a potential cost savings/cost avoidance associated with the Control Point concept.

3.4 Life Cycle of a Control Point

3.4.1 Development Process Overview

As part of the execution of the overall COE process, each Computing Environment Working Group (CEWG) identifies changes to their existing Control Point Specifications. Additionally, the COE Chief Engineer may identify changes to Control Point Specifications, such as introducing a *Cross Cutting Capability* into the COE version. The two CEWGs meet to reconcile their inputs, preparing and then signing the Control Point Specification, guided by the COE Integrated Master Schedule (IMS) produced by the COE Chief Engineer. If the CEWGs are unable to agree on the Control Point Specification, the CEWG Leads will submit a draft Control Point Specification that identifies their agreements, along with details on where the CEWGs cannot agree. The COE Chief Engineer, working within the COE Governance Process, will resolve the issues. Once approved, the Control Point Specification will be used for formal testing/verification and certification activities, e.g., by a CEWG to establish that its constituent systems meet the requirements of the Control Point Specification, or by System of Systems integration activities, such as Family of Systems (FoS) testing.

3.4.2 COE Verification

The primary activity of COE Verification is the integration, test and verification of the software and systems that comprise the CPs within the COE. The COE Verification activity will also evaluate the CE-provided self-certification artifacts of their COE components that are not involved in a CP to ensure that they are conformant with the COE objectives with respect to standards and approved methodologies.

A preliminary COE Verification Plan will be developed by ASA(ALT) concurrently with the development of Control Point Specifications. This plan will identify the set of approved tools and techniques that will be applied to verify the proper implementation of the CPs. The plan will identify the approved tools and techniques to be used by CEs to self-certify components of the COE Baseline that are not involved in a COE Control Point. The plan will also include the integrated schedule of verification activities that are needed to conduct Control Point verification and the evaluation of CE self-certification artifacts for COE conformance. The plan may recommend procurement actions to buy/develop verification tools. The full collection of resources required to support COE verification will be specified in the COE Verification Plan.

4 Way Ahead

Implementation of the COE will enable the Army to develop, test, certify, security accredit and deploy software capabilities, IT devices/systems and National Security Systems more rapidly, improve security and interoperability and reduce costs without introduction of harmful or unexpected behavior. CIO/G-6, in conjunction with ASA(ALT), TRADOC, FORSCOM, OBT, and other stakeholders in HQDA, will assess current and planned acquisition programs prior to Weapons Systems Reviews. The next step is for ASA(ALT) to update the COE Implementation Plan (and other documents as needed) that describes the steps and schedule for moving Army systems to the COE. The plan will inform future Weapon Systems Reviews and POM investments. ASA(ALT), including PEOs and separately reporting PMs, shall comply with the definitions and guidelines in this annex and the ASA(ALT) COE Implementation Plan in order to obtain POM funding for the development and acquisition of software capabilities, IT devices/systems and National Security Systems.

The COE Technical Roadmap describes the planned capabilities by COE version for each TRM layer (e.g. COE common software foundation versions by TRM layer) on a timeline.

Other outstanding COE future initiatives related to this document, include, but are not limited to:

- The CIO/G-6 will collaboratively develop an Army Annual StdV-1/2 for each version of COE beginning with COE 3.0. Specific development guidance will be provided by ASA(ALT) to PMs and CE leads for the ASA(ALT) input into the Army Annual Standards View 1/2 for COE.
- ASA(ALT) shall examine the current workflow related to the Standards View StdV-1s created and maintained by the CEs.

Appendix A – Acronyms

ACCT	Architecture Configuration Control Team
AIC	Army Interoperability Certification
API	Application Programming Interfaces
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ATGR	Army Technical Guidance Repository
CAC	Common Access Card
CCC	Cross-Cutting Capabilities
CE	Computing Environments
CEWG	Computing Environment Working Group
CIO	Chief Information Officer
COE	Common Operating Environment
COTS	Commercial Off-The-Shelf
CP	Control Point
CS	Capability Set
DCG	Data Center Cloud Generating Force
DIL	Disconnected, Intermittent, and Low Bandwidth
DISR	Department of Defense IT Standards Registry
DoD	Department of Defense
E2E	End to End
EO	Engagement Operations
ERP	Enterprise Resource Planning
FACE	Future Airborne Capability Environment
FoS	Family of Systems
FORSCOM	Forces Command
GF	Generating Force
GOTS	Government Off-the-Shelf
HQDA	Headquarters, Department of the Army
IA	Information Assurance
IaaS	Infrastructure as a Service
I2E	Integration and Interoperability Exercises
IMS	Integrated Master Schedule
iSEP	Integrated Systems Engineering Plan
ISP	Information Support Plan
IT	Information Technology
JBC-P	Joint Battle Command - Platform
JIIM	Joint Intergovernmental, Interagency, Multi-national
MCE	Mounted Computing Environment
MHH	Mobile Handheld
NetOps	Network Operations
NIPRNet	Non-classified Internet Protocol Router Network
OBT	Office of Business Transformation
OIS	Ordnance Interface Standards

OS	Operating Systems
PaaS	Platform as a Service
PDK	Product Development Kit
PEO	Program Executive Office
PM	Project Manager
POM	Program Objective Memorandum
PoR	Program of Record
REST	Representational State Transfer
ROI	Return On Investment
RTIF	Real Time Interoperability Framework
RTSCE	Real Time / Safety Critical / Embedded
SEP	System Engineering Plan
SDK	Software Development Kit
SOAP	Simple Object Access Control
StdV1	Standard View 1
StdV2	Standard View 2
SWaP-C	Size, Weight, and Power - Cooling
TAB	Technical Advisory Board
TIGR	Tactical Ground Reporting System
TRADOC	Training and Doctrine Command
TRM	Technical Reference Model
VICTORY	Vehicular Integration for C4ISR/EW Interoperability
WG	Working Group

Appendix B – Terms and Definitions

Army Interoperability Certification (AIC). Army CIO/G-6 issuance of an official memorandum authorizing a system or group of systems for network operations based on acceptable interoperability test results. Testing was conducted by an independent test organization and demonstrated successful performance of digital interoperability and net-centric missions as defined within approved interoperability test requirements (mission threads). It is determined that utilization of the capabilities will not negatively impact network performance.

Army Technical Guidance Repository (ATGR). The ATGR is an Army CIO/G-6 tool for the management of technical standards that works with, and not in place of, DISR. The ATGR contains DISR and Non-DISR standards. It organizes technical standards into technology-based profiles and provides a unique use-case (mapping tool) to rapidly identify Army required standards.

Certification. Official recognition by competent and empowered authority that requirements have been met.

Common Operating Environment (COE). The COE is an approved set of computing technologies and standards that enable secure and interoperable applications to be rapidly developed and executed across a variety of Computing Environments.

COE Baseline. Guidance approved by the Army Acquisition Executive that establishes the contents and objectives for each COE Version. The COE Baseline includes all Control Point Specifications associated with the capabilities to be provided by the given COE baseline.

COE Governance Process. The process by which work products and guidance are reviewed, approved and published to the COE community.

COE Version. An instance of the COE that is developed tested, baselined and integrated on a three year cycle consistent with the Army Force Generation Model and IAW the Unit Set Fielding Plan.

Computing Environment (CE). A logical grouping of systems with similar characteristics used to organize the COE (deployment/echelonment, environmental, transport dependencies, form factors, etc.). A computing environment comprises the necessary hardware, operating system, libraries and software required to run applications within the COE.

Computing Environment Working Group (CEWG). An organization chartered by the Army Acquisition Executive to produce and manage the Operating Environment

for a given set of systems within a domain established by operational and environmental characteristics.

Control Point Specification. A document (or set of documents) that defines the Control Point interfaces. The Control Point Specification is produced by the CEWGs involved in the Control Point, using processes and templates established by the COE Chief Engineer and approved through the COE Governance Process.

Cross Cutting Capability (CCC). A facility defined by the COE that establishes a set of interfaces, design rules and possible implementations that are used by more than one Computing Environment. CCCs are managed by the COE Chief Engineer and are approved through the COE Governance Process. Data exchange items associated with CCCs are incorporated into the appropriate Control Points.

Department of Defense Information Technology Standards Registry (DISR) is an online repository of IT standards formerly captured in the Joint Technical Architecture (JTA), Version 6.0. DISR replaces JTA. Use of the DISR is required for JCIDS as the registry for Joint standards and approved waivers. It is a tool for Information Support Plan (ISP) and StdV-1/2 creation and registration.

Minimum Technical Standards. The baseline set of standards consisting of DISR Mandated, Non-DISR with approved waivers and Army Unique Standards that defined in the Army Annual Standards Profile (StdV-1). The StdV-1 is hosted in the Army Technical Guidance Repository (ATGR), a Web-based, on-line tool hosted by the CIO/G-6.

Standard. A document (issued by a recognized Standards Development Organization) that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. A standard may also be a specification that establishes requirements for the selection, application, and design criteria for materiel solutions (hardware and/or software).

Standard View 1 (StdV-1) Standards Profile. The listing of standards that apply to solution elements.

Standard View 2 (StdV-2) Standards Forecast. The description of emerging standards and potential impact on current solution elements, within a set of time frames.

Technical Reference Model (TRM). The COE Technical Reference Model illustrates the technology strategy of the COE in a single diagram. It shows the technical elements of the COE and how they fit together. IT delineates the responsibilities of each COE organization and what technical domains fall outside of the COE. The model provides a depiction of the layers that make up the COE, the Computing Environments that are currently part of the COE and who in the Army community is responsible for implementing or defining the standards, processes and

products that make up the COE. The objective of the TRM is to provide a structured definition of the COE software foundation or technical baseline and its associated interfaces.

Test. An examination to measure and confirm performance.

Validation. The process of determining the degree to which a system or group of systems and associated data are an accurate representation of the real world from the perspective of the intended uses. Validation methods include expert consensus, comparison of historical results, comparison with test data, peer review and independent review. (DA Pam 73-1)

Verification. The process of determining that an implementation of a system or group of systems and associated data accurately represents the developer's conceptual description and specifications. Verification evaluates the extent to which the software has been developed using sound and established engineering techniques. (DA Pam 73-1)