



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

SAIS-AOB

05 MAR 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Release of Army Technical Guidance Repository: Appendix A to the Guidance for 'End-State' Army Enterprise Network Architecture

1. References:

a. Memorandum, Vice Chief of Staff of the Army (VCSA), subject: Achieving Army Network and Battle Command Modernization Objectives, dated 28 December 2009.

b. Common Operating Environment Architecture, (Appendix C to the Guidance for 'End State' Army Enterprise Network Architecture), dated 20 October 2010.

c. DoD Instruction 8410.02, NetOps for the Global Information Grid (GIG) 19 December 2008

d. DoD Directive 8100.1, Global Information Grid (GIG) Overarching Policy, September 19, 2002

e. CJCSI 6212.01E Interoperability and Supportability of Information Technology and National Security Systems, 15 Dec 2008

f. CJCSI 3170.01G Joint Capabilities Integration and Development System, 01 Mar 2009.

g. DoDI 4630.8 Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), June 30, 2004

h. DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 5, 2004

i. DoDD 5000.01 The Defense Acquisition System, November 2007

SAIS-AOB

SUBJECT: Release of Army Technical Guidance Repository: Appendix A to the Guidance for 'End-State' Army Enterprise Network Architecture

2. As the technical architect for the Army, CIO/G6 provides this Guidance as a means to achieve the vision of the Chief of Staff of the US Army for a single, secure, standards-based network. It provides the Standards, Services, Applications, Software, and Guidance that are the mechanisms for implementing the four imperatives of the Army Network Strategy: 1. Single, Secure, Standards-Based Network; 2. Enable Global Collaboration; 3. Access at the Point of Need that is Capable, Reliable, and Trusted; 4. Deploy Integrated Capabilities throughout the Army. It aggregates all technical standards from the various appendices (B-F) of the Guidance for 'End State' Army Enterprise Network Architecture (NW Guidance) and provides the single source for technical standards and technologies for all appendices.

3. This Guidance applies across the Army as a necessary condition for achieving interoperability, implements the Common Operating Environment (COE) and Everything Over IP (EoIP) architectures, and is mapped to the LandWarNet Capability Sets (LWN CS) time frames. It includes standards for the Deployed Tactical network as well as Post/Camp/Station and Home/TDY. It provides potential opportunities for materiel developers, soldiers, resource providers, and operational planners to find efficiencies. It defines the technical framework that will enable the agile development and delivery of required capabilities to the Soldier. It helps the Army to continuously assess the Network architecture and Network performance relative to the needs of the Soldier.

4. This Guidance consists of this written document and a web repository of all the applicable technical standards. The repository enables rapid and accurate identification of the required standards. The Army Technical Guidance Repository is available at https://www.kc.army.mil/TRM_TOOL/.

5. This guidance is effective immediately. This guidance and the technical standards repository will be updated annually to refresh the standards according to the current Network Strategy, Army priorities, DoD IT Standards (DISR) baselines and the emerging technologies. Compliance by Materiel Developers is expected in the implementation of standards within the Capability Set (CS) timeframes provided and is required for the benefits of a single Army end-to-end network to be realized.

6. Points of contact for this action are COL Dana Tankins, Chief, LWN Architecture Integration Division, (703) 545-1453, dana.s.tankins.mil@mail.mil or Ms. Reeth Nakka (703) 545-1441, reeth.r.nakka.ctr@mail.mil.

Enclosure


GARY W. BLOHM
Director, Architecture Integration Center
CIO/G6

SAIS-AOB

SUBJECT: Release of Army Technical Guidance Repository: Appendix A to the Guidance for 'End-State' Army Enterprise Network Architecture

DISTRIBUTION:

PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY
COMMANDER

U.S. ARMY FORCES COMMAND

U.S. ARMY TRAINING AND DOCTRINE COMMAND

U.S. ARMY MATERIEL COMMAND

U.S. ARMY CYBER COMMAND

U.S. ARMY EUROPE AND SEVENTH ARMY

U.S. ARMY CENTRAL

U.S. ARMY AFRICA

U.S. ARMY NORTH

U.S. ARMY SOUTH

U.S. ARMY PACIFIC

U.S. ARMY SPECIAL OPERATIONS COMMAND

MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND

U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC
COMMAND

EIGHTH U.S. ARMY

U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL
COMMAND (ARMY)

U.S. ARMY MEDICAL COMMAND

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

U.S. ARMY CRIMINAL INVESTIGATION COMMAND

U.S. ARMY CORPS OF ENGINEERS

U.S. ARMY MILITARY DISTRICT OF WASHINGTON

U.S. ARMY TEST AND EVALUATION COMMAND

U.S. ARMY RESERVE COMMAND

U.S. ARMY INSTALLATION MANAGEMENT COMMAND

SUPERINTENDENT, U.S. MILITARY ACADEMY

CF:

DIRECTOR, U.S. ARMY ACQUISITION SUPPORT CENTER

Army Technical Guidance Repository
*Appendix A to the Guidance for End-State Army Enterprise
Network Architecture*



U.S. Army CIO/G-6

Version 1.0

05 MAR 2012

Executive Summary:

This Army Technical Guidance provides the means to achieve the vision of the Chief of Staff of the US Army for a single, secure, standards-based network. It provides the Standards, Services, Applications, Software, and Guidance that are the mechanisms to implement the four imperatives of the Army Network Strategy: 1. Single, Secure, Standards-Based Network; 2. Enable Global Collaboration; 3. Access at the Point of Need that is Capable, Reliable, and Trusted; 4. Deploy integrated capabilities throughout the Army. It aggregates all technical standards from the various appendices (B-F) of the "Guidance for End State Army Enterprise Network Architecture" (NW Guidance) and provides the single source for technical standards and technologies for all appendices.

This Technical Guidance applies across the Army as a necessary condition for achieving interoperability, implements the Common Operating Environment (COE) and Everything Over IP (EoIP) architectures, and is mapped to the LandWarNet Capability Sets (LWN CS) time frames. It includes standards for the Deployed Tactical network as well as Post/Camp/Station and Home/TDY. It provides potential opportunities for materiel developers, soldiers, resource providers, and operational planners to find efficiencies. It defines the technical framework that will enable the agile development and delivery of required capabilities to the Soldier. It helps the Army to continuously assess the Network architecture and Network performance relative to the needs of the Soldier.

Appendix A consists of this written document and a web repository of all the technical standards. This repository enables rapid and accurate identification of the required standards. The Army Technical Guidance Repository is available at: https://www.kc.army.mil/TRM_TOOL/

This guidance, including both this document and the Web Repository, is effective immediately and will be updated annually to refresh the technical standards according to the current Network Strategy, Army priorities, DoD IT Standards (DISR) baselines and the emerging technologies. Compliance is expected in the implementation of standards and is required for the benefits of a single Army end-to-end network to be realized. Points of contact for this action are COL Dana Tankins, Chief, LWN Architecture Integration Division, (703) 545-1453, dana.s.tankins.mil@mail.mil or Ms. Reeth Nakka (703) 545-1441, reeth.r.nakka.ctr@mail.mil.

Approved:



GARY W. BLOHM
Director, Architecture Integration Center
United States Army | CIO/G6
Pentagon, Washington, DC 20310

Version Summary:

Version	Date	Revision Summary
1.0	05 MAR 2012	Baseline: Army Technical Guidance Repository

Table of Contents

EXECUTIVE SUMMARY:	I
TABLE OF CONTENTS	III
LIST OF FIGURES AND TABLES	III
1.0 INTRODUCTION	1
1.1 Purpose.....	1
1.2 Background	1
1.3 Approach.....	2
1.4 Configuration Management (CM).....	4
This document and the technical standards repository will be revised each December by the CIO/G6. Updates to this Guidance and Repository are based on acquisition community and other stakeholders’ input. The CIO/G6 will approve and prioritize all the requirements for making changes to this document or the web repository.	4
2.0 STANDARDS AND TECHNOLOGIES	5
2.1 Appendix B: Installation Network Architecture Standards.....	8
2.2 Appendix C: Common Operating Environment (COE) Architecture Standards	9
2.3 Appendix D: Deployed Tactical Network Guidance Standards.....	9
2.4 Appendix E: Mission Assurance Standards	9
2.5 Appendix F: Network Operations (NetOps) Standards.....	9
2.6 Geospatial Architecture Standards	10
2.7 Coalition/NATO Technical Standards	10
3.0 CIO/G6 TECHNICAL ARCHITECTURE PROCESSES	12
3.1 Supporting Processes Related to Technical Guidance Development.....	12
3.2 Technical Standards Maturity Model (TSMM)	17
4.0 ACRONYM LIST	19
5.0 REFERENCES:	21

List of Figures and Tables

Figure 1: Army Network High-Level Operational Concept	3
Figure 2: Network Strategy & Architecture Document Hierarchy	4
Figure 3: App A: Document PLUS Repository	5
Figure 4: Technical Guidance Development Process	12
Figure 5: DISR Baseline Change Request (CR) Process	13
Figure 6: CIO/G6 Army Input Process to DISR Change Request (CR) Process	14
Figure 7: ISP Review Process.....	14
Figure 8: TA Validation (Non-PoR) Process.....	15
Figure 9: DISR and Army Waiver Process	16

1.0 Introduction

On 28 December 2009, the Vice Chief of Staff of the Army (VCSA) directed CIO/G6 to develop 'as is' and 'end state' network architectures to guide network development, procurement and enhancement. The Army Network Architecture Strategy – Tactical version 1.1, dated 6 April 2010, was crafted in response to the VCSA's memorandum, and this Strategy continues to evolve. CIO/G6 has also written the Guidance for 'End State' Army Enterprise Network Architecture (NW Guidance) to provide direction for the entire Army Enterprise Network. This Appendix A consolidates all of the standards from each of the NW Guidance component appendices, which includes Common Operating Environment (COE) Architecture (Appendix C), in support of the Army Network Strategy.

1.1 Purpose

The purpose of this document is to mandate the standards and technologies to be used to build

“a single, secure, standards-based, versatile infrastructure linked by networked, redundant transport systems, sensors, warfighting and business applications, and data to provide our Soldiers, Civilians, and mission partners the information they need, when they need it, in any environment, to manage the Army and enable full-spectrum operations with our Joint, Coalition and interagency partners.”

28 June 2010, the Chief of Staff, US Army (CSA)

Thus, this Technical Guidance aligns with the Army Network Strategy, which CIO/G6 is building to implement the following four imperatives, based on the CSA quotation above:

1. Single, Secure, Standards-Based Network
2. Enable Global Collaboration
3. Access at the Point of Need that is Capable, Reliable, and Trusted
4. Deploy integrated capabilities throughout the Army.

This two part Technical Guidance, consisting of this document and the corresponding Web Repository, provides the mandated standards and technologies, mapped to the NW Guidance architecture to constrain material development and facilitate stakeholder alignment with the Network Strategy.

1.2 Background

In support of the Army Campaign Plan, the CIO/G6 Strategic Objective is to transform (operationalize) LandWarNet via the Army Network Strategy. LandWarNet is the Army's contribution to the Global Information Grid (GIG). It consists of the complete end-to-end set of globally interconnected Army information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand for warfighter, policy makers, and support personnel.

Achieving COI/G6's objective of operationalizing LandWarNet will result in improved effectiveness and efficiencies for the Army and mission partners; improved Army and leveraged DoD/Joint communications and computing systems/services, software, and data security and other associated services; and improved Joint, Interagency, Intergovernmental, and Multinational (JIIM) interoperability.

This Technical Guidance document and Web Repository support this high level direction - mandating the standards and technologies that support the COE and Everything Over IP (EoIP) architecture. It provides a necessary condition and an implementation mechanism for the Army Network Strategy and facilitates

the achievement of reliable communication across echelons and Control Points¹. Since this is a dynamic process, the Army will continuously assess the Network architecture and Network performance relative to the needs of the Soldier.

The scope of this guidance includes mandating standards and technologies to support the Army-wide, enterprise-level capabilities for LWN CS 13-14, 15-16 and End State in alignment with the Army Network Strategy and NW Guidance. The standards and technologies include Mandated and Emerging DISR standards as well as commercial standards not currently in DISR. The standards are based on the DISR Baseline 2011-3.0 (current as of this writing).

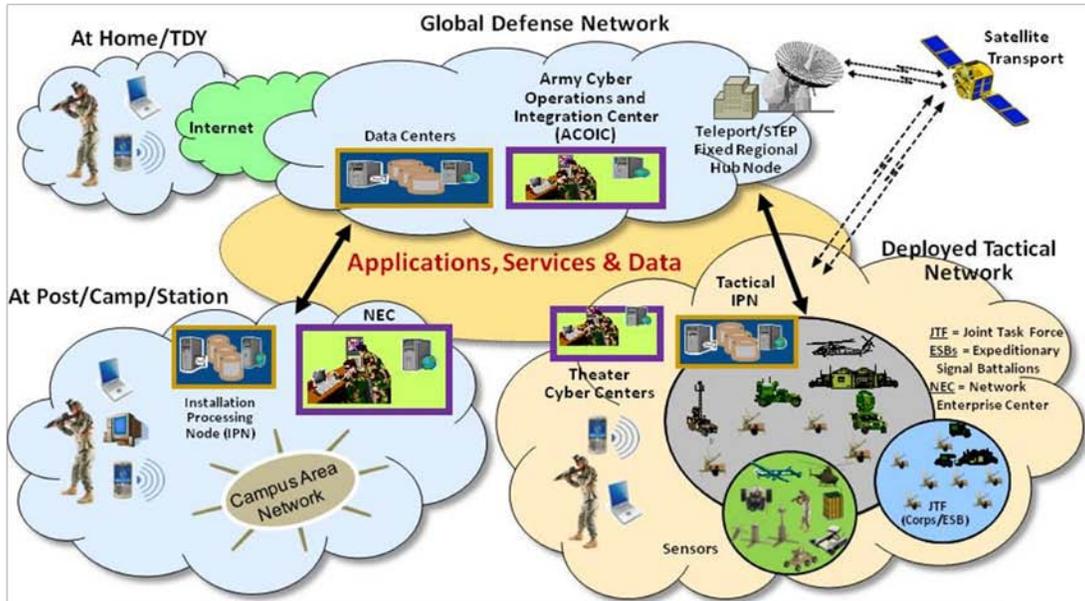
“Technology Areas” in the Web Repository were devised to categorize the content of each of the NW Guidance appendices into smaller levels of granularity. See Figure 2 for more information on these appendices. For example, Appendix C (COE) categorizes by Computing Environments, and so Computing Environments are used as Technology Areas in the Web Repository for the COE standards and technologies. Technology Areas were derived in a similar manner for the other NW Guidance appendices. Thus, each standard or technology maps to one or more Technology Areas defined in the various NW Guidance appendices. This also makes it easier for users to locate the standards and technologies they need to implement.

1.3 Approach

The CIO/G6 approach leverages the concept of the Global Defense Network, depicted in Figure 1 below. That figure provides the basis for structuring the End State appendices. Appendix B: Installation Network Guidance refers to the Post/Camp/Station component at the lower left of the figure. Appendix D: Deployed Tactical Network Guidance refers to the Deployed Tactical Network component at the lower right of the figure. Appendix C: Common Operating Environment Architecture maps to Computing Environments across the various network groupings in the figure, and Appendix E: Mission Assurance Guidance and Appendix F: Network Operations (NetOps) Guidance similarly apply across the networks.

¹ For more information on Control Points, see the COE document. <https://www.us.army.mil/suite/doc/25070472>.

LandWarNet “Powering America’s Army”



The Network Must be **Capable, Reliable and Trusted** and to Get There it has to be a **Single, Secure, Standards-Based Environment** that **Ensures Access at the Point of Need** and **Enables Global Collaboration**

2011-11-09T18:30Z

HTTP://CIOG6.ARMY.MIL

7

Figure 1: Army Network High-Level Operational Concept

The standards and technologies for each appendix have been determined through efforts that follow a combination of processes, as outlined in section 3.1 Supporting Processes Related to Technical Guidance Development. Specifically, that section illustrates processes for Technical Guidance Development, DISR Change Request, Information Support Plan (ISP) Review, Technical Architecture (TA) Validation (Non-Programs of Record (PoRs)), and DISR and Army Waiver Approval. Section 3.2 Technical Standards Maturity Model (TSMM), modeled on the Capability Maturity Model of the Software Engineering Institute (SEI), Carnegie Mellon University, is applied within the processes.

Figure 2 illustrates how this Technical Guidance fits into a series of documents that ultimately support The Army Plan (TAP), the Army Campaign Plan (ACP), and the Army Network Strategy. The policy mechanism that directly supports the Army Network Strategy is the NW Guidance, including this document and repository and Appendices B-F, which provides guidance to specific aspects of the End State NW Architecture. This document and repository is unique as it maps to each of the other appendices, providing the standards and technologies that support the parts of the Army network represented by each.

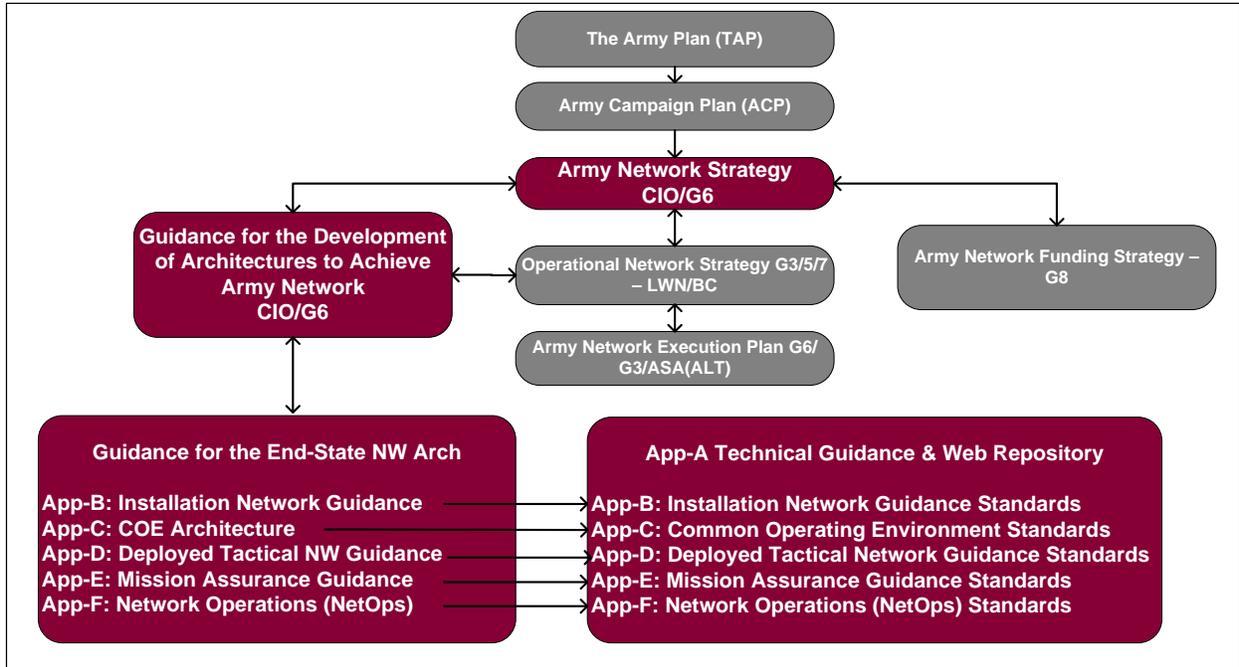


Figure 2: Network Strategy & Architecture Document Hierarchy

The Army Network Strategy document captures the Army CIO/G6 vision and the ways, means, and ends to realize the End State of a single network that enables a collaborative environment accessible to all Army Soldiers and Civilians and ensures secure and trusted operations.

1.4 Configuration Management (CM)

This document and the technical standards repository will be revised each December by the CIO/G6. Updates to this Guidance and Repository are based on acquisition community and other stakeholders' input. The CIO/G6 will approve and prioritize all the requirements for making changes to this document or the web repository.

2.0 Standards and Technologies

This Army Technical Guidance provides a web-based utility to assist stakeholders, customers, and users in Technical Architecture development and analysis. Thus, the guidance consists of this document plus the Technical Guidance repository, as shown in Figure 3. The Web Repository can be accessed at https://www.kc.army.mil/TRM_TOOL/.

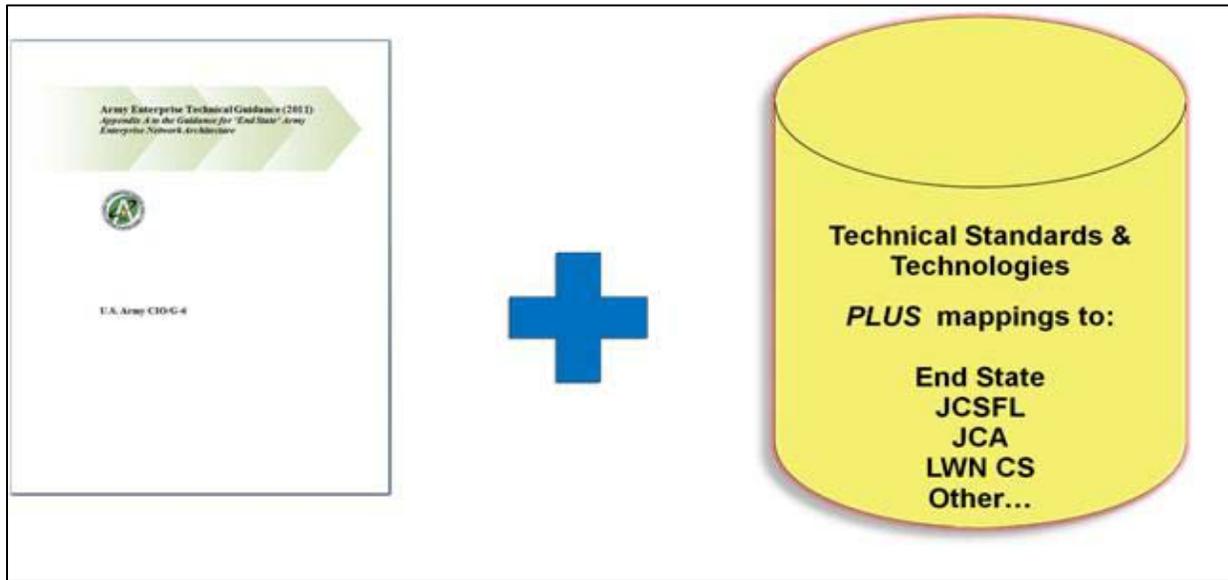


Figure 3: App A: Word Document Plus Repository

For purposes of compliance with Army Technical Guidance to the End State, users should utilize the “Appendix A” mapping in the Web Repository. For convenience in StdV/TV-1 development mappings to other guidance such as Joint Common System Function List (JCSFL), LandWarNet Capability Sets (LWN CS), and Joint Capability Areas (JCA), are also provided.

The listing found in the repository consists of the Standards, Services, Applications, Software, and Guidance mapped to the various End State appendices (B-F). Some of these standards or technologies are approved and designated as “Mandated” and “Emerging” in the DoD Information Technology Standards Registry (DISR). These are a subset of DISR, consisting of about one-third of the standards in DISR. However, there are other “forward-looking” standards and technologies, not currently listed in DISR, that support a capability anticipated in a future Capability Set timeframe. In these cases, a program or other sponsor can initiate a Change Request (CR) for bringing any “forward-looking” standards or technologies into DISR. See section 3.1, “Supporting Processes Related to Technical Guidance Development”, for more information on the DISR Change Request process. The new DISRonline web site is: <https://gtg.csd.disa.mil/uam/homepage.do>

The following table provides an explanation of the typical information you will find in reports from the repository:

Column	Status Code	Explanation
Identifier	N/A	Includes list of following elements: <ul style="list-style-type: none"> • Standard – Established norm governed by a Standard Development Organization (e.g. IEEE, IETF, W3C, etc.) • Service - A software system designed to support interoperable machine-to-machine interaction over a network • Application – Computer software, sometimes referred to as an "app", designed to help the user to perform specific tasks • Software - A collection of computer programs and related data that provide the instructions for telling a computer what to do and how to do it • Guidance - Documents that affect multiple organizations and provide a means to further clarify standards and identify relevant policies and procedures (i.e. IT-related best practices, information standards, manuals, policy, procedures, and handbooks)
Title	N/A	Title for Standard or Technology Identifier
Status	M	DISR Mandated Standard (M): Per DISRonline, "Mandated standards provide interoperability and net-centric services across the DoD enterprise. They are the minimum set of essential standards for the acquisition of all DoD systems that produce, use, or exchange information and, when implemented, facilitate the flow of information in support of the Warfighter. These standards are required for the management, development, and acquisition of new or improved systems throughout the DoD. A tag may be added to a standard. An email is sent to the DISR Secretariat requesting a sunset tag along with a defined event and date for retiring the standard. Frequently a replacement standard is also identified. An X in the "sunset" column in a standards profile identifies the sunset status."
	E	DISR Emerging Standard (E): Per DISRonline, "Emerging may be implemented, but shall not be used in lieu of a mandated standard. An emerging standard is expected to be elevated to mandatory status within three years. Use of an emerging standard in a TV-1 requires a waiver and a Technology Insertion Risk Assessment. In general, emerging standards should be placed in the TV-2."
	R	DISR Retired (R): Per DISRonline, "Retired standards should not be used in a new or upgraded system. All retired standards citations remain in the DoD IT Standards Registry (DISR). However, when selected for inclusion in a Technical Standards View (TV), a retired standard citation requires a waiver and a Technology Insertion Risk Assessment."
	N	Non-DISR Standard or Technology (N): Standards and Technologies, including Service, Application, Software, and Guidance, not available in DISR.
LWN CS	N/A	LandWarNet Capability Set timeframe (13-14, 15-16, End State)
Technical Profile	N/A	The Technical Profile provides a list of recommended standards and technologies supporting a specific functionality/service area, but needed in order to achieve the Network End State.

The Technical Guidance standards and technologies are at the core and evolve with technological advances over time. They are grouped into small families of standards called Technical Profiles, making it easier for users to identify their required standards. In addition, the data in the repository is:

- Categorized by Technology Areas for each appendix of the NW Guidance
- Aligned with LandWarNet Capability Set (LWN CS) timeframes
- Mapped to Joint Common System Function List (JCSFL)
- Mapped to DISR Service Areas

The Web Repository allows material developers and other stakeholders to drill through the repository based on these mappings in order to build a custom set of profiles or standards, exported to Excel or other file format, or as printed reports, for use in constructing StdV/TV products as mandated by the current CJCSI 6212.01x.

The table below shows examples of the key stakeholders and how the Army Technical Guidance benefits each:

Stakeholder	Feature/Benefit of Tool
CIO/G6	Search/filter repository or create reports to <ul style="list-style-type: none"> • Decision making regarding NW capabilities • Validate Technical Architectures • Create Enterprise Technical Architectures • Assess compliance of PoRs and non-PoRs with guidance • Assist with IT policy development • Readily provide updates w/o publishing entire new document
Program Manager	Search/filter repository or create reports to <ul style="list-style-type: none"> • Determine DISR support for their required capabilities • Select standards as input to their StdV/TV-1/2 • Assess their StdV/TV V-1/2 for compliance with CIO/G6 guidance • Correlate StdV/TV and SV documents • Assess possible need for waivers
Architect	Search/filter repository or create reports to <ul style="list-style-type: none"> • Determine DISR support for certain capabilities • Build domain Technical Architecture • Assess Technical Architecture across domain entities • Identify sets of standards for consideration • Correlate TV and SV documents
Army Test & Evaluation / Certification	Search/filter repository or create reports to <ul style="list-style-type: none"> • Search for interoperability standards • Identify compliant vs non-compliant standards • Assess possible integration testing issues

The sections below provide specific background regarding the standards and technologies associated with each of Appendices B thru F.

2.1 Appendix B: Installation Network Architecture Standards

The Army Installation Network, described in detail in the “Army Installation Network (Post/Camp/Station) Guidance: Appendix B to Guidance for ‘End State’ Army Enterprise Network Architecture”, includes the infrastructure and devices used by both the Generating Force and the Operating Force in CONUS and OCONUS. The Army Installation Network is comprised of two major functional/physical components: NetOps services which are received through the second-tier Theater Network Operations Centers (TNOSCs) and Installation Processing Nodes (IPNs) which are logical extensions of the APC-provided services and include installation-level or other local touch labor.

The “Technical Criteria for the Installation Information Infrastructure Architecture”, February 2010 (I3A Technical Criteria Feb 2010), which supports gathering the necessary requirements, conducting site surveys, and performing analysis, design, and implementation of IT, can be located at:

<i>For NIPRNET Technical Criteria:</i>	https://www.us.army.mil/suite/files/5745483
<i>For SIPRNET Technical Criteria:</i>	https://www.us.army.mil/suite/files/5744948

As described in the Background section above, Technology Areas have been identified for the purpose of mapping profiles (standards and technologies); however, Appendix B Technology Areas have not yet been formalized and may be updated in a future version. The Technology Areas (with general descriptions) identified in the table below were derived from the Appendix B to the NW Guidance and consist of:

Technology Area	Description
Applications/services	An entity that provides functionality to support information management
Network Technology	The conduit that supports that transfer of information
Security Technology	Technologies that specifically protect information-related assets
Network Management	Enablers for monitoring and controlling the network
Wireless	Specifically supports interconnectedness of connectionless entities
User Devices	Physical entity that supports an information management function
Storage Area Network	Asset that provides capacity to store large amounts of data on the network

2.2 Appendix C: Common Operating Environment (COE) Architecture Standards

The COE Standard Tables in Appendix C, signed on Oct 20, 2010, include a listing of standards and technologies that support the Services defined in the COE's computing environments. Given that the COE document was signed, it is now official guidance and is under configuration control. It can be accessed at <https://www.us.army.mil/suite/doc/25070472>.

This Technical Guidance includes the standards and technologies that have been updated to support the 'Network Strategy' Appendix C for the COE. The Web Repository reflects the updates that have affected the standards listed in the original COE guidance.

The updates consist of three possible scenarios:

- 1 - Replaces Retired standard as of DISR 2011-3.0 baseline
- 2 - Standard supports LWN CS and maps to COE
- 3 - Retired with no replacement as of DISR 2011-3.0 baseline

This section includes standards out of alignment with the original, signed, and configuration-controlled COE.

2.3 Appendix D: Deployed Tactical Network Guidance Standards

The Deployed Tactical Network, as described in "Appendix D: Deployed Tactical Network" (unsigned version), is the component of the Army Network used by our Soldiers in the field. The Deployed Tactical Network connects to the rest of the Army Network via Teleport, Standardized Tactical Entry Point (STEP), or Regional Hub Node (RHN) sites. Functional proponents provide applications, services and data to customers thru Area Processing Centers (APCs) and Tactical Installation Processing Nodes (IPNs). Second-tier Theater Network Operations and Security Centers (TNOSCs) provide Network Operations (NetOps) services to the Deployed Tactical Network.

2.4 Appendix E: Mission Assurance Standards

Part 1, Information Assurance

"Appendix E: Mission Assurance Guidance (Part 1, Information Assurance (IA))" describes the transformation of the Army's networks to a Global Network and the establishment of a unified architecture, in accordance with (IAW) the Global Network Enterprise Construct (GNEC) and the Army Network Modernization Strategy, require the Army to identify threats and vulnerabilities in order to implement control measures that enable us to achieve acceptable risk. Risk often results from the integration of commercial services and commercial "off-the-shelf" (COTS) products into the LandWarNet (LWN) architecture. The Information Assurance (IA) framework standards included in the Repository address, in context, the threats, vulnerabilities, and mitigation procedures required to achieve acceptable risk as part of the Army LWN modernization effort. This framework also enhances Network Operations (NetOps) in support of Army missions, functions, and operations.

Part 2, GIG DMZ Architecture

At the time of this revision, Appendix E: Mission Assurance Guidance (Part 2, GIG DMZ Architecture) was not available. No engineering analysis was performed. Updates will be performed upon availability.

2.5 Appendix F: Network Operations (NetOps) Standards

Note that the Technology Areas for Appendices C and D were already provided within these appendices themselves. However, since there is not yet a completed Appendix F: Network Operations (NetOps), this document provides three recommended Technology Areas for NetOps, which again are subject to change:

Technology Area
Enterprise Management
Network Defense
Content Management

This is based on three interdependent tasks necessary to manage Network Operations. In addition, standards and Technical Profiles are mapped to NetOps based upon the following criteria:

- If a protocol relates to the network and is 'application oriented', it is not included in NetOps.
- If a protocol is related to management of an 'application', it is considered to be part of NetOps.

2.6 Geospatial Architecture Standards

The set of geospatial standards, available in the Repository, contains all Common Operating Environment (COE) geospatial standards provided in the document entitled 'Appendix C Tab 8' plus an additional set of critical geospatial standards based on CIO/G6 guidance. The geospatial standards have been synchronized with the National Geospatial-Intelligence Agency (NGA) 5-year production strategy. The geospatial standards provided to the Army by the NGA are included to help ensure that geospatial information is readily ingestible to Army systems/users.

2.7 Coalition/NATO Technical Standards

The Coalition Interoperability Assurance & Validation (CIAV) (see CIAV CONOPS document, Version 1.0, April 2011) is designed to conduct interoperability Assurance & Validation (A&V) related to the exchange of mission critical information on the Afghan Mission Network (AMN). The listing of NATO standards that is coordinated as part of that Coalition effort can be found in the Report Repository section of the Web Repository.

The standards are listed in Allied Data Publication 34 (ADatP-34(E)), "NATO Interoperability Standards and Profiles", Volume 1 - Introduction and Management, 25 January 2011. While they are available as a separate listing in the "Report Repository" on the Repository site, they are excluded from the Army Technical Guidance database. The issue is that NATO is a separate organization under different governance, and the status of NATO standards is not synchronized with DISR. Thus, mixing NATO standards with Army standards would be cumbersome, confusing, and inconsistent. Since there are only a select few systems that interoperate with coalition systems, those systems can coordinate accordingly to support the objective of coalition interoperability.

Columns include:

1. Afghanistan Mission Network (AMN) NATO standard profile
2. Technical Standard
3. Status of subject NATO standard in DISR
4. Inclusion of standard in the current TA (App A)

The legend for the first column, Afghanistan Mission Network (AMN) NATO standard profile is:

D.3. COMMUNICATION AND NETWORK SERVICES STANDARDS

- D.4. INFRASTRUCTURE AND CORE ENTERPRISE SERVICES STANDARDS
- D.5. COMMUNITY OF INTEREST SERVICES AND DATA STANDARDS
- D.6. COMMUNITY OF INTEREST DATA AND SYSTEM INTEROPERABILITY
- D.7. GEOSPATIAL INTEROPERABILITY
- D.8. BATTLESPACE MANAGEMENT INTEROPERABILITY
- D.9. JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE INTEROPERABILITY
- D.10. BIOMETRICS DATA AND SYSTEM INTEROPERABILITY
- D.11. USER INTERFACE CAPABILITIES/APPLICATIONS

3.0 CIO/G6 Technical Architecture Processes

3.1 Supporting Processes Related to Technical Guidance Development

In alignment with the Maturity Models (MM) defined in the NW Guidance and its appendices, a Technical Standard Maturity Model (TSMM) was devised to apply the ‘maturity’ discipline to the evaluation of standards for use in different time frames, as defined by the Capability Sets. Section 3.2 Technical Standards Maturity Model (TSMM) provides details on the model. The TSMM is used in the various processes below.

This Technical Guidance supports Technical Architecture development and validation, as well as support of DoD IT Standards Registry (DISR) Change Request and Waiver processes. The process and methodology described below is the technical guidance development process the CIO/G6 uses. Based on various inputs, system engineering analysis is done to prescribe accurate technical standards to meet the NW Strategy and Capability Sets.

DISR has a well-established process for introducing new standards, vetting them, and publishing them first as Emerging status, raising them to Mandated status, sunseting, and finally moving to Retired status. The DISR processes can be found at the DISRonline web site at <https://disronline.csd.disa.mil/a/>. Below are illustrations and short discussions on support provided by CIO/G6 to these various processes related to development of the App A NW Guidance.

3.1.1 Technical Guidance Development Process

The process and methodology described below is the technical guidance development process the CIO/G6 uses. Based on various inputs, system engineering analysis is done to prescribe accurate technical standards to align with the Network Strategy and Capability Sets. Refer to the TA Development Process flowchart below.

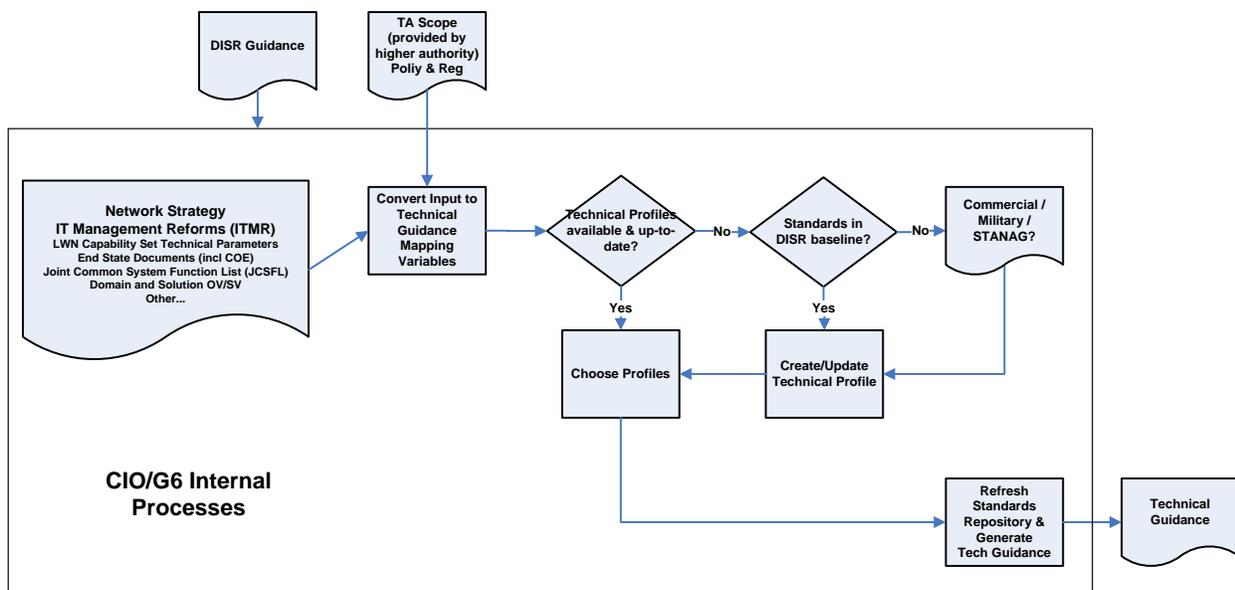


Figure 4: Technical Guidance Development Process

3.1.2 DISR Change Request Process

Change Request is a DISR process that, by definition, relates to a DISR status change for a Standard or Information Guidance. The DISR process is shown in Figure 5, and the CIO/G6 role in this process is illustrated in Figure 6.

The CR is initiated by a PM. It is first reviewed by the author's immediate organization for release. Then it is similarly reviewed by the DISR Secretariat then moved into the DISR Technical Working Group (TWG) review process. Analysis of a CR, however, goes further to assure that the technical underpinnings are sound – and leverages such best practices as Backward Compatibility (BWC) and Technical Standards Maturity Model (TSMM) to provide a consistent framework for use across standards.

Included in this process is the possibility of approval of non-DISR standards by DISR, where the standard is placed in the Organization-Unique Standards (OUS) bin. Program Managers (PMs) can readily pick and choose the standards from this OUS bin without applying for a Waiver. If a PM chooses a non-DISR standard or technology that is not an OUS, then the Waiver policy applies. For more information, see DISRonline.

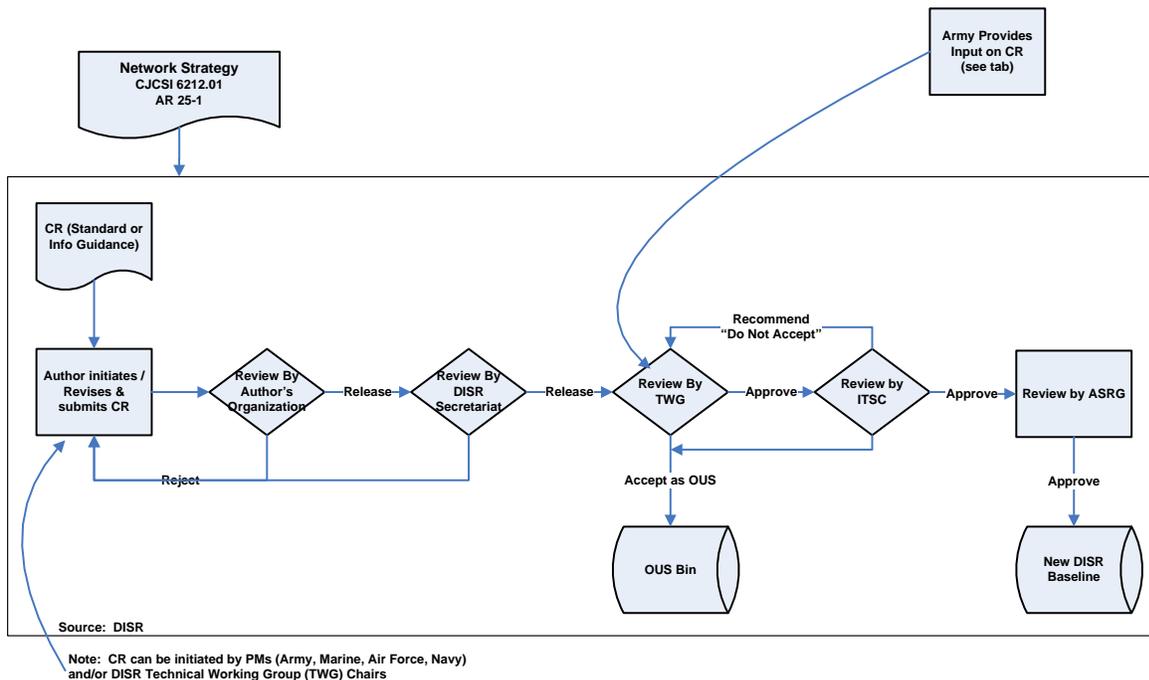


Figure 5: DISR Baseline Change Request (CR) Process

During execution of the DISR CR process, further analysis of standards is done by G6 on behalf of the Army. This sub-process of the CR process includes application of the Technical Standards Maturity Model (TSMM), outlined in greater detail in Section 3.1 in the References.

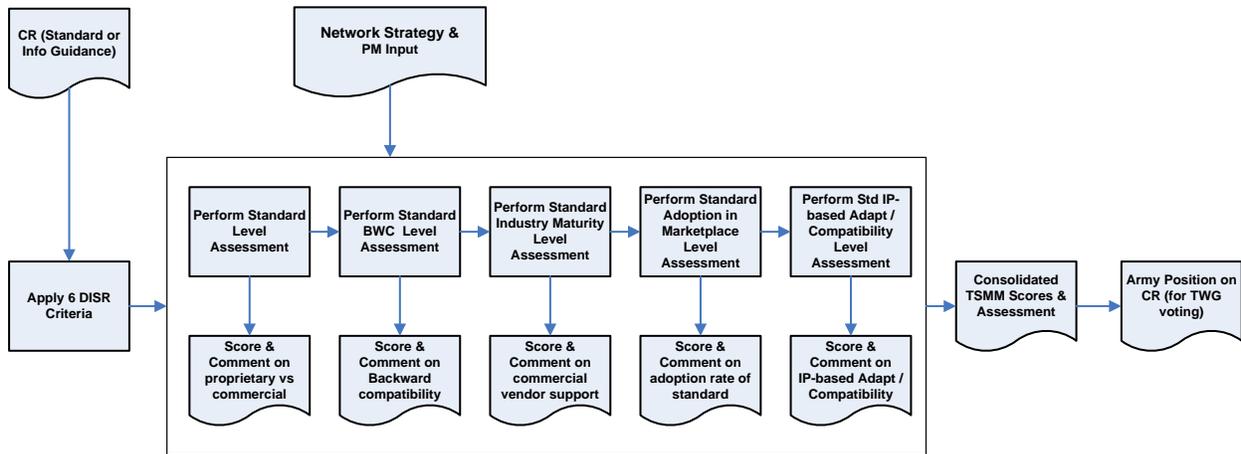


Figure 6: CIO/G6 Army Input Process to DISR Change Request (CR) Process

3.1.3 Information Support Plan (ISP) Review Process

The primary DoD guidance for the ISP Review is the current version of CJCSI 6212.01. Figure 7 depicts the internal ISP Review process for systematic analysis of ISPs, with emphasis on StdV/TV validation, including checking compliance with CIO/G6 Technical Guidance.

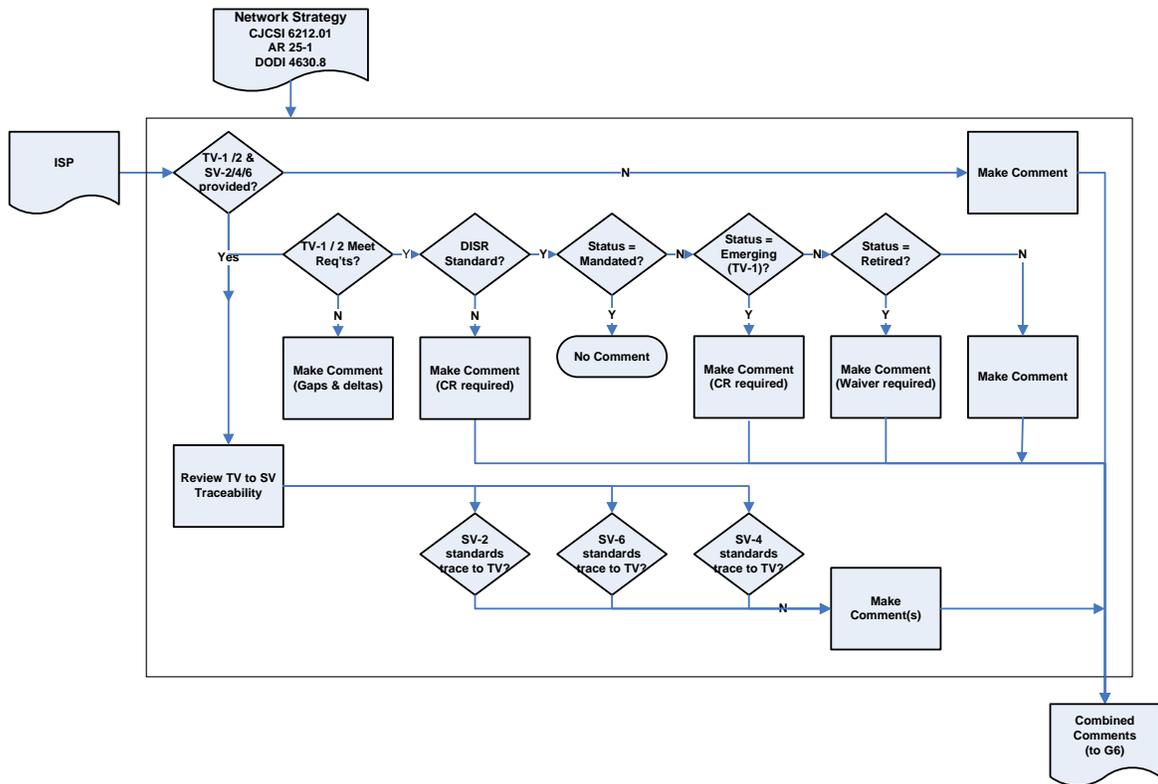


Figure 7: ISP Review Process

3.1.4 Technical Architecture (TA) Validation (Non-Program of Record (PoR)) Process

Since non-POR's are not subject to JCIDS analysis, which applies to PoR's only, TA validations are often performed. The TA validation is similar to the ISP Review and DISR Waiver processes, and thus is based on the same guidance and employs similar best practices. The primary difference is that the data provided by a non-POR may be different than for a POR, since non-PoRs are not subject to the JCIDS requirements. Thus, some improvising and common sense logic consistent with principles found in guidance for PoRs needs to be applied. The process is depicted in Figure 8 below:

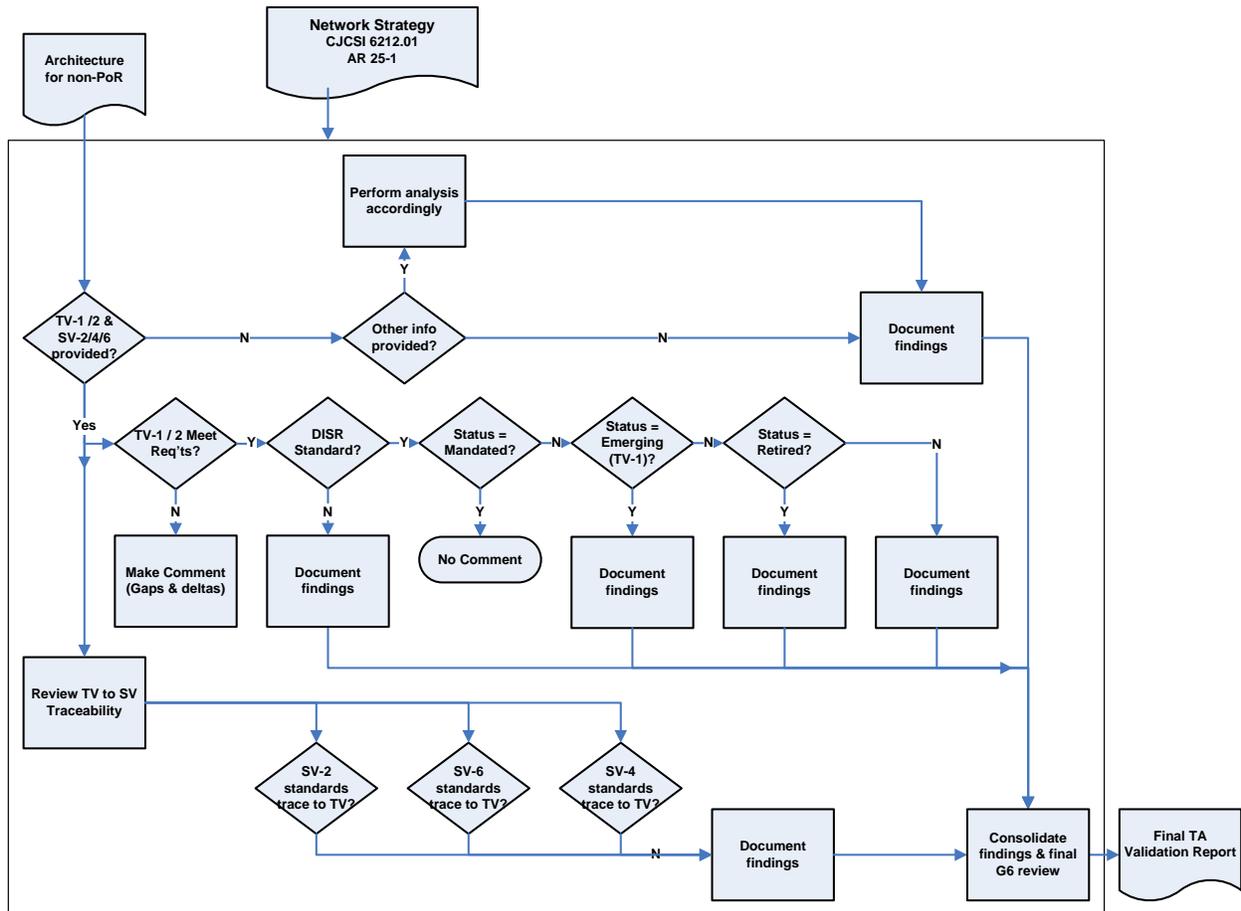


Figure 8: TA Validation (Non-PoR) Process

3.1.5 DISR and Army Waiver Approval Process

The DoD Information Technology Standards Registry (DISR) waiver process applies to Retired standards, where use of a Retired standard is requested. Guidance requires the submission of detailed documentation to substantiate the request by the submitter. Refer to the DISR and Army Waiver Approval process flowchart below:

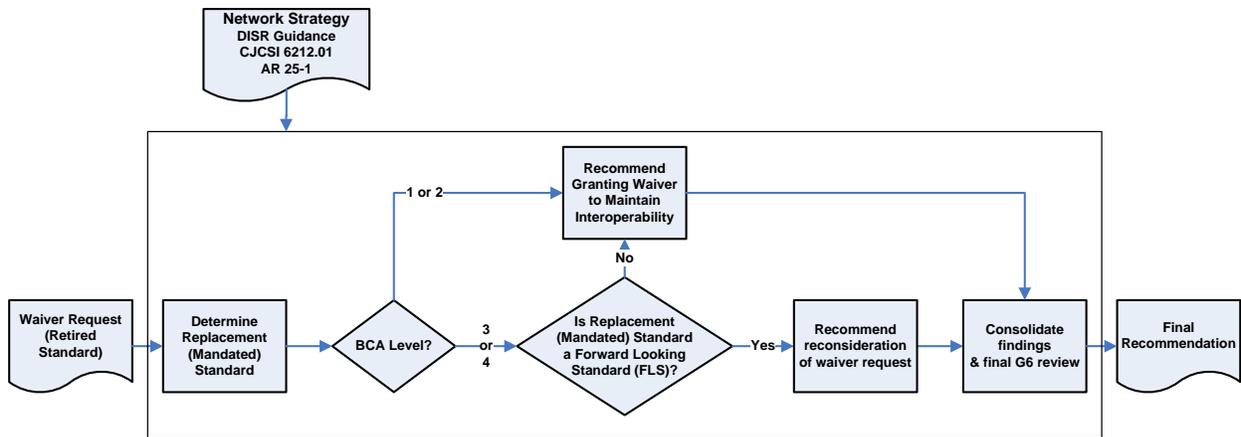


Figure 9: DISR and Army Waiver Process

For purposes of the Backward Compatibility Assessment (BCA), the Mandated replacement standard is assessed for its backward compatibility with the Retired version. It is determined whether it can be easily substituted based upon assignment of a Backward Compatibility (BWC) Level from the below chart:

The Backward Compatibility (BWC) Level	
Measures the degree to which the standard is BWC to its prior version – from not BWC to BWC at the standard level.	
Level 1	Standard is not BWC.
Level 2	Standard can be BWC with an 'external' gateway or adapter implementation.
Level 3	Standard can be BWC seamlessly by a commercial product with embedded configuration, gateway, etc.
Level 4	Standard is BWC at the standard level.

3.2 Technical Standards Maturity Model (TSMM)

In alignment with the Maturity Models (MM) defined in the Guidance for the Development of Architectures to Achieve Army Network and its appendices, a Technical Standard Maturity Model (TSMM) has been devised to apply the 'maturity' discipline to the evaluation of standards for use in different time frames, as defined by the Capability Sets.

The TSMM maturity assessment process is intended to provide analysis and information that can be used in conjunction with other evaluation criteria to provide an assessment methodology with the ability to respond to changing mission requirements. The goal is not for each and every standard to achieve Level 4 maturity, or to be replaced by one that is Level 4, but rather to understand the current maturity and determine whether investment is warranted to move up the maturity scale.

The TSMM is intended to be used to consistently assess the maturity of standards within the Technical Guidance. The TSMM measures key attributes selected for their relevance to achieving the Army's goal of developing and deploying applications from a technical standards perspective. The attributes include Standard Level, Backward Compatibility (BWC) Level, Industry Maturity Level, Adoption in Marketplace Level, and EoIP-based Adaptability/Supportability Level. In applying the TSMM, a standard is evaluated against the criteria of the four maturity levels for each of the five attributes in the model. The maturity rating assigned to each attribute is the one that most closely maps the maturity model's criteria to the characteristics observed in the specific area being assessed.

3.2.1 The Standard Level

The Standard Level identifies the source – from proprietary to widespread commercial development - of the standard as a determinant of fitness for purpose.

Standard Level	
Level 1	Standard is proprietary, and hence the property of the developer. Technical details are not known or controlled in the public domain.
Level 2	Standard is being developed by organizations for a specific COI or WG, including commercial and military.
Level 3	Standard is being developed and maintained by military standard organizations, e.g., MIL-STD (DoD) and STANAG (NATO)
Level 4	Standard is developed commercially by industry standard development organizations like IETF, ANSI, ITU, IEEE, ISO, and W3C.

3.2.2 Backward Compatibility (BWC) Level

The Backward Compatibility (BWC) Level measures the degree to which the standard is BWC to its prior version – from not BWC to BWC at the standard level.

Backward Compatibility (BWC) Level	
Level 1	Standard is not BWC.
Level 2	Standard can be BWC with 'external' gateway or adapter implementation.
Level 3	Standard can be BWC seamlessly by a commercial product with embedded configuration, gateway, etc.
Level 4	Standard is BWC at the standard level.

3.2.3 The Industry Maturity Level

The Industry Maturity measures the number and capability of supporting vendors, evaluating the degree to which the standard is 'proven' in practice. This TSMM measure is a derived version similar to the many flavors of Technology Readiness Level (TRL) in use in other DoD, NASA, and related applications to assess the maturity of evolving technologies (materials, components, devices, etc.) prior to incorporating that technology into a system or subsystem. In these other uses of the TRL, the most basic level (TRL of 1) is assigned when a technology is primarily conceptual and not even demonstrated in a laboratory. The most advanced or mature level (TRL of 9, where TRL is rated on a scale of 1 to 9, different from the 1 to 4 scale of the MM) is assigned when a technology has been qualified for usage in operational missions.

Industry Maturity Level	
Level 1	Standard does not have any viable vendors for developing and supporting it.
Level 2	Standard is being developed by a single vendor without add-on or integration interface.
Level 3	Standard is being developed by a single vendor with add-on or integration interface.
Level 4	Standard is developed by multiple vendors.

3.2.4 The Adoption in Marketplace Level

The Adoption in Marketplace measures the ubiquity of the standard in its specific community of use – from not in use to in wide use in DoD and commercial environments.

Adoption in Marketplace Level	
Level 1	Standard is not in use.
Level 2	Standard is in production use in a very limited number of implementations.
Level 3	Standard is in production use but for Army or DoD only.
Level 4	Standard is in wide use for its specific application by DoD and commercially.

3.2.5 EoIP-based Adaptability/Supportability Level

EoIP-based Adaptability/Supportability measures the level of EoIP approach headed for 'Network Vision & Strategy' Objective.

Thus, the judgments to be made from the Level assignments will be used as input to assess ability of the technology to respond to changing mission requirements, and to determine whether investment is warranted to move up the maturity scale. The TSMM levels are defined generically enough to apply broadly across standards, but specific enough to inform investment decisions.

EoIP-based Adaptability/Supportability Level	
Level 1	Standard supports EoIP for an Individual/Local/Separate Network or Application.
Level 2	Standard supports EoIP for Enterprise Network or Application with investment in adapters, gateways, or reconfigurations
Level 3	Standard supports EoIP for Enterprise Network or Application without investment in adapters, gateways, or reconfigurations.
Level 4	Standard supports the EoIP in the path toward the Network Vision & Strategy.

The EoIP-based Adaptability/Supportability attribute has some additional complexities as compared with the others. For example, some standards – such as an image format standard – fall under Level 1, but it does not really matter, as another standard provides the transport and communications capabilities needed to share the file – whether over IP or otherwise. In addition, any judgments based on level of investment required are very general, and not backed up with detailed information.

4.0 Acronym List

AMN	Afghanistan Mission Network
ADatP	Allied Data Publication
APC	Area Processing Center
AAE	Army Acquisition Executive
ASRG	Architecture and Standards Review Group
ATEC	Army Test & Evaluation Command
BCA	Backward Compatibility Assessment
BCEC	Battle Command Essential Capabilities
BWC	Backward Compatibility
CR	Change Request
CIAV	Coalition Interoperability Assurance & Validation
COE	Common Operating Environment
COTS	Commercial "off-the-shelf"
COP	Common Operational Picture
CONOPS	Concept of Operations
CONUS	Continental United States
CP	Control Point
DoD	Department of Defense
DISR	DoD IT Standards Registry
EoIP	Everything Over IP
FRAGO	Fragmentary Order
GIG	Global Information Grid
GNEC	Global Network Enterprise Construct
IAW	in accordance with
ISP	Information Support Plan
ITMR	IT Management Reforms
ITSC	Information Technology Standards Committee
JCIDS	Joint Capabilities Integration and Development Process
JCSFL	Joint Common System Function List
JIIM	Joint, Interagency, Intergovernmental/non-governmental organizations and Multinational
MATDEVs	Materiel Developers
MNC	Multinational Coalition
NGA	National Geospatial-Intelligence Agency
NW	Network
NATO	North Atlantic Treaty Organization
OUS	Organization-Unique Standards
OCONUS	Outside of Continental United States
PoR	Program of Record
STEP	Standardized Tactical Entry Point
StdV	Standards Viewpoint
StdV-1	Standards Profile
StdV-2	Standards Forecast
SoS	System-of-Systems
TOC	Tactical Operations Center
TA	Technical Architecture
TSMM	Technical Standards Maturity Model
TV	Technical View
TV-1	Technical Standards Profile

TV-2	Technical Standards Forecast
TWG	Technical Working Group
TRL	Technology Readiness Level
TNOSCs	Theater Network Operations Centers
UDOP	User Defined Operation Picture

5.0 References:

- a) Memorandum, Vice Chief of Staff of the Army (VCSA), subject: Achieving Army Network and Battle Command Modernization Objectives, dated 28 December 2009.
- b) Army Network Architecture Strategy-tactical Ver 1.1 Dated 06 April 2010 (unsigned version)
- c) Appendix C, The common Operating Environment (COE) Oct 20, 2010
- d) DoD Instruction 8410.02, NetOps for the Global Information Grid (GIG) 19 December 2008
- e) CJCSI 6212.01E Interoperability and Supportability of Information Technology and National Security Systems, 15 Dec 2008
- f) CJCSI 3170.01G Joint Capabilities Integration and Development System, 01 Mar 2009.
- g) DoDI 4630.8 Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), June 30, 2004
- h) DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 5, 2004
- i) DoD Directive 8100.1, Global Information Grid (GIG) Overarching Policy, September 19, 2002
- j) DoDD 5000.01 The Defense Acquisition System, November 2007