Annex A
Technical Standards Guidance
to
LandWarNet 2020 and Beyond
Enterprise Architecture

Version 2.0

As of: 1 August 2014

Table of Contents

Table of Contents....................i

List of Figures....................ii

Executive Summary....................iii

1. Purpose....................1

1.1 Scope....................1

1.2 Audience....................2

1.3 Roles and Responsibilities....................2

1.3.1 The CIO/G-6 (in coordination with TRADOC, G-3/5/7, and ASA (ALT)) shall: 3

1.3.2 Request ASA(ALT) perform the following actions:....................3

1.3.3 Request the DCS, G-3/5/7 perform the following actions:....................4

1.4 References....................4

2. Technical Standards & Technical Standards Maturity Model (TSMM)....................5

2.1 Technical Standards Selection....................5

2.2 Technical Standards Maturity Model (TSMM)....................6

2.2.1 The Standard Source Attribute....................7

2.2.2 The Backward Compatibility (BWC) Attribute....................8

2.2.3 The Industry Maturity Attribute....................8

2.2.4 The Adoption in Marketplace Attribute....................9

2.2.5 The EoIP-based Adaptability/Supportability Attribute....................9

3. Technical Standards Profiles (ATGR Profiles)....................10

3.1 Purpose....................10

3.2 A Technical Standards Profiles (ATGR Profiles) is defined by the following generalized criteria:....................10

3.3 Technical Standard Types....................11

3.4 Army Standards View – StdV-1 (Standards Profile) and StdV-2 (Standards Forecast) for the Common Operating Environment (COE)....................11

3.5 Value Proposition for an Army Standards View for COE:....................11

3.6 Approach....................12

4. Technical Architecture Processes....................13

4.1 Purpose....................13

4.2 Technical Guidance Development Process....................14

4.3 DISR Change Request Process....................14

4.4 Information Support Plan (ISP) Review Process....................16

4.5 Technical Architecture (TA) Process for Validation of Non-Programs of Record 17
4.6 DISR and Army Waiver Approval Process 18
Appendix A – Acronyms / Glossary 20
Appendix B – Glossary 21
Appendix C – Army Standards Profile Guidance in Support of COE v3, version 1.0 (To Be Published Separately) 23

List of Figures

Figure 1: Strategy and Architecuture Alignment. 2
Figure 2: Annual StdV-1/2 Process Flow for COIE 13
Figure 3: Technical Guidance Development Process 14
Figure 4: DISR Baseline Change Request (CR) Process 15
Figure 5: CIO/G-6 Army Input Process to DISR Change Request (CR) Process 16
Figure 6: ISP Review Process 17
Figure 7: TA Validation (Non-PoR) Process 18
Figure 8: DISR and Army Waiver Process 19

Executive Summary

The Chief Information Officer/G-6 (CIO/G-6) is responsible for providing the information technology (IT) Enterprise Architecture (EA) guidance for the Army. A major element of the Army's Enterprise Architecture is the IT technical standards guidance provided herein. IT standards are a critical forcing function for achieving interoperability across DoD and with Unified Action Partners. Where Joint solutions do not meet Army requirements, Army-built systems must align to DoD and Joint architectures to ensure interoperability with Unified Action Partners (UAPs). Alignment with DoD and Joint architectures is achieved through adherence to technical standards. Moreover, if IT capabilities are built on an approved, common set of technical standards baseline, then the Army has built interoperable solutions from the beginning that can be validated during the Army Interoperability Certification (AIC) Process.

A challenge the Army faces is maintaining and improving interoperability among its systems and solutions while keeping pace with technological advances that provide opportunities to improve current capabilities and fill critical capability gaps. Annex A describes the set of processes to align the Army Standards Profile with the DoD IT Standards Registry (DISR) and process DISR change and waiver requests. The Army must develop IT technical profiles that are re-usable, logical and useful categories to facilitate visibility of applicable standards guiding solutions development and procurement strategies.

Our way ahead is to continue to collaborate with the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA(ALT)) and other Army stakeholders to continuously improve our standards lifecycle processes. CIO/G-6 in coordination with other stakeholders will achieve improvement by aligning IT standards to Army-wide Network strategy and capability needs. These standards will guide the development of solution architectures, and the fielding of interoperable solutions.

The Army CIO/G-6 has worked collaboratively with the ASA(ALT) community and the Mission Areas to establish a standards development process that will produce an Army Annual Standards View (StdV-1) or an Army Technical Profile establishing a baseline of prescribed standards that will guide and inform the acquisition community to plan for and build Army IT capabilities to meet Army priorities. The Army approved standards profile is the start point for improving interoperability and cyber security, and for closing capability gaps in the Army. In addition, it will be the basis for Army AIC.

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 16:08:17 -04'00'

Gary W. Blohm
Director Army Architecture Integration Center

1. Purpose

This Annex applies to the development and lifecycle management of IT Technical Standards across the Army Enterprise. It establishes the enterprise guidance to manage IT standards to achieve interoperability and provide the acquisition community with the ability to rapidly develop solutions to fill prioritized capability gaps and new IT requirements.

The challenge the Army faces is maintaining and improving interoperability while keeping pace with technology advances that provide opportunities to improve current capabilities and fill critical capability gaps. Standards must serve a specific purpose, not be established for their own sake – they must add value to the Army in the areas of interoperability, maturity, improved capability and cybersecurity. The Army must develop IT technical profiles that are re-usable, logical and provide useful categories to facilitate visibility of applicable standards guiding solutions development and procurement strategies.

This update supersedes Appendix A (dated 30 August 2010, DISR Baseline 2010-2.0) in two ways:

a. It aligns with the DISR Baseline 2014-14.01 and with the End State by promoting the Army StdV 1.0 as the approved Army standards baseline.

b. It aligns with the Army Network Campaign Plan and with the LandWarNet 2020 and Beyond Enterprise Architecture. Figure 1 depicts the relation between Annex A and other documents.

1.1 Scope

This Annex applies to all IT Technical Standards across the Army Enterprise. The processes outlined support Technical Architecture (TA) development and validation; DISR Change Request (CR) and Waiver processes for all Programs of Record (PoRs) and non-PoRs. It is a major subordinate element of LandWarNet 2020 and Beyond Enterprise Architecture as depicted in Figure 1 below.

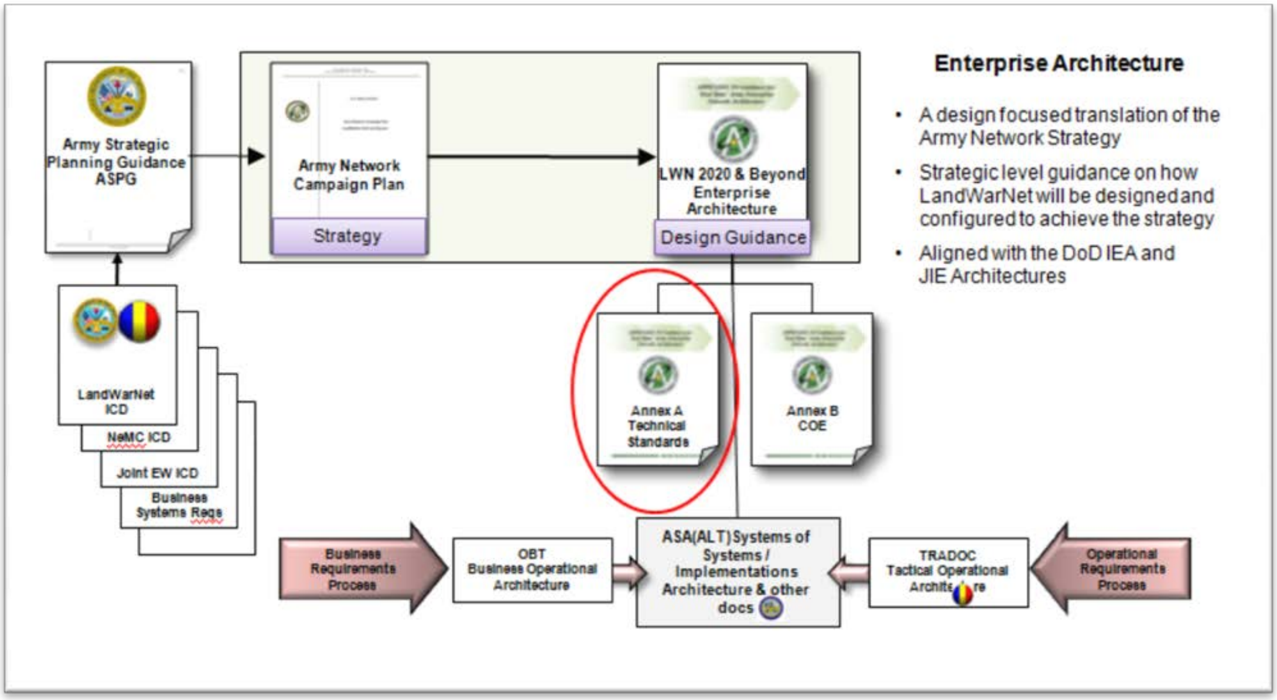

Army Strategic Planning Guidance ASPG
Army Network Campaign Plan
Strategy
LWN 2020 & Beyond Enterprise Architecture
Design Guidance
Enterprise Architecture
• A design focused translation of the Army Network Strategy
• Strategic level guidance on how LandWarNet will be designed and configured to achieve the strategy
• Aligned with the DoD IEA and JIE Architectures
LandWarNet ICD
NeMC ICD
Joint EW ICD
Business Systems Reqs
Annex A Technical Standards
Annex B COE
Business Requirements Process
OBT Business Operational Architecture
ASA(ALT) Systems of Systems / Implementations Architecture & other docs
TRADOC Tactical Operational Architecture
Operational Requirements Process

Figure 1: Strategy and Architecuture Alignment.

1.2 Audience

The audience for this document includes all LandWarNet stakeholders. The primary stakeholders (including Deputy Chief of Staff, G-3/5/7, CIO/G-6, G-8 FD,Training and Doctrine Command (TRADOC), Office of Business Transformation (OBT), and ASA(ALT)) will utilize the information contained in this document to directly inform:

- The development of materiel solutions and associated policy
- IT investment and acquisition decisions
- The development of LandWarNet architecture products

Other critical stakeholders including Combatant Commands (COCOM), Unified Action Partners (UAP) etc., may utilize this information to become acquainted with the LandWarNet information environment (IE) that will support and enable their mission and business processes. This technical standards guidance will help to inform Industry Partners to focus their technology and Research and Development (R&D) efforts to best support the future IT needs of the Army.

1.3 Roles and Responsibilities

In accordance with the authority in Section 2223 of Title 10, United States Code; Paragraphs 16d and 16j of Department of the Army General Order (DAGO) 2012-01; DoD Directive (DoDD) 5144.02, DoD Chief Information Officer (DoD CIO), 22 April

2013; DoD Directive 8000.01, Management of Department of Defense Information Enterprise, 10 February 2009; and Army Regulation 25-1, Army Information Technology, dated 25 June 2013 (currently under revision), and AR 71-9, Warfighter Capabilities Determination, dated 28 December 2009.

1.3.1 **The CIO/G-6 (in coordination with TRADOC, G-3/5/7, and ASA (ALT)) shall:**

a. Establish the architecture process, assign responsibilities and provide direction for identifying, developing and prescribing IT standards that share, exchange, and use information to enable the Army to operate in joint, multinational, and interagency operations.

b. Collaboratively develop IT standards and standardized profiles for use throughout the Army to promote interoperability, information sharing, reuse, portability and cybersecurity within the Army as well as within the Joint Information Environment (JIE) and the National Intelligence Community's Intelligence Community – Information Technology Enterprise (IC ITE).

c. Process and evaluate waivers for approval to use other than mandated DoD and Army IT standards (i.e., emerging standards) in accordance with DoD guidance.

d. Coordinate with the DoD CIO, Under Secretary of Defense (USD) (AT&L), the DoD EA for IT standards, and the Chairman of the Joint Chiefs of Staff (CJCS), as required, to establish processes and procedures for enforcing IT standards compliance.

e. Provide representatives to the Joint Enterprise Standards Council (JESC) in accordance with DoD guidance.

f. Validate that all Information Support Plans (ISP) submitted by program managers include a standards profile and a summary list of all system interfaces.

g. Review all capability documents ensuring all materiel solutions are compliant with DoD IT Standards Registry.

1.3.2 Request ASA(ALT) perform the following actions:

a. Require program managers for IT acquisitions and procurements to include a standards viewpoint (i.e., StdV-1 Standards Profile and StdV-2 Standards Forecast, formerly referred to as the Technical View (TV)) for inclusion in Capability Development Documents (CDDs) and Capability Production Documents (CPDs) that conforms to the DoD architecture framework and the Army's LandWarNet 2020 and Beyond Enterprise Architecture.

b. Require all IT implementations to comply with the IT standards in the DISR and Army approved standards with DISR waivers in the Army Technical Guidance Repository (ATGR), https://www.kc.army.mil/TRM_TOOL/default.aspx.

c. Require program managers to include DoD and Army approved standards conformance testing events and procedures in interoperability test plans.

d. Require Program Managers to demonstrate compliance with approved DoD and/or Army conformance to standards validation events.

e. Develop, validate and execute a standards compliance program to ensure that Program Managers are properly developing and implementing Army approved standards correctly.

f. Review requests for proposal (RFPs) and contract statements of work (SOWs) prepared by program managers to ensure DISR IT standards established in capability documents (ICDs, CDDs and CPDs) are translated into clearly contractual requirements.

g. Fully support the DoD Information Technology Service Management (ITSM) through planning, budgeting, and execution.

h. Use IT standards in the DISR for system development, acquisition, and procurement, considering impact of cost, schedule, performance, and cybersecurity.

1.3.3 Request the DCS, G-3/5/7 perform the following actions:

Ensure no CDD or CPD is staffed or is approved by Headquarters, Department of the Army that does not have properly identified IT standards.

1.4 References

- Title 10 United States Code (USC) Sections 2223 & 2224
- DoDD 5144.02, DoD Chief Information Officer (DoD CIO), dated 22 April, 2013
- DoDD 8000.0, Management of the Department of Defense Information Enterprise, dated 10 February 2009
- DoDI 8310.aa (Information Technology Standards in the DoD) Draft

- DoDI 8330-01, Interoperability of Information Technology (IT), including National Security Systems (NSS), dated 21 May 2014
- DoD Information Technology Service Management (ITSM)
- DoD Information Enterprise Architecture Volumes I, II Version 2.0 dated July 2012
- Army Regulation (AR) 25-1, Army Information Technology, dated 25 June 2013
- AR 71-9, Warfighter Capabilities Determination, dated 28 December 2009

2. Technical Standards & Technical Standards Maturity Model (TSMM)

The purpose of this section is to lay out broad principles and criterion related to selection of standards with a specific framework for analysis. The framework is called the TSMM. It should be noted that the Army also considers independent frameworks for identifying and evaluating technologies using a comprehensive approach that is not vendor driven. Such frameworks generate credible information that is helpful to the process of identifying and evaluating technologies that could make an impact on Army capabilities.

2.1 Technical Standards Selection

The selection of technical standards in standards profiles is a critical sub-component of the development of architecture. A standard (or technical standard) is a statement of how a particular function is to be implemented. Standards are established by Computing Environment (CE) leaders and designated working groups within DoD and the Army as described in section 2.2 and 2.3.

Standards limit design freedom, but mitigate the complexity and cost of the multiplicity of solutions. Within the context of Rules-based Reference Architecture, the methodology is to specify guidance to solutions architects in terms of principles that convey broad transformational objectives; rules that convey specific architectural concepts; and decisions that are derived from operational requirements documents such as Initial Capabilities Documents (ICDs) developed by TRADOC to meet Army requirements.

2.1.1 There are two overarching principles that drive decision criteria for selection of technical standards:

a. Optimum Enterprise Benefit – Benefit is measured in terms of the following criteria: accessibility, consistency, cost, flexibility, functionality, manageability, risk, scalability, security, supportability and value.
b. Technology Components – Army architecture supports leading edge technologies to meet mission differentiating needs and requires mature, proven interoperable technologies in support of the Joint Information Environment (JIE).

2.1.2 Decision Criteria for selection of standards are:

a. **Existing/mandatory standards**. Evaluates the Army's experience with the technology/standard and its current use across the enterprise.
b. **Fits with existing Army Enterprise standards, technologies and systems**. Evaluates the interoperability issues the standard might have with existing standards deployed across the enterprise.
c. **Maintainability/Supportability**. Evaluates the effort and specialized skill sets required to support a technology standard.
d. **Cost.** Evaluates the estimated total cost of ownership if the Army chooses to adopt a new standard.
e. **Strategic Value**. Evaluates the breadth of standard's potential capabilities that would offer more flexibility and scalability.
f. **Flexibility**. Evaluates the breadth of the standard's applicability to multiple stakeholders, for example, a technology standard that provides the Army with greater enterprise-wide implementation opportunities than do "niche" technologies that are adaptable to only a small segment of Army users.
g. **Security**. Evaluates the ability and/or effectiveness of the potential technology standard to meet the Army Cybersecurity policies or established standards. The standard with less known conflicts with security components such as firewalls or Demilitarized Zones (DMZs), and that are representing less risk than do standards that have yet to be proven and may have unknown issues, incompatibilities or risks are more likely to be selected.
h. **Vendor Viability**. Evaluates the health of the proprietary standard vendor/s in terms of its stability, projected longevity, and likelihood it will exist in the future to support the standard and associated products.
i. **Industrial Base**. Evaluates the use and adoption of the standard throughout industry in general (both industry and federal government).
j. **Associated Product Lifecycle.** Evaluates the expected time the standard will be in use and supported by the vendor/s and the ability to maintain currency and its functionality. A longer lifecycle is more desirable from a training and hardware investment perspective.
k. **Intuitive.** Evaluates the standard with an immediate apprehension or cognition without complex reasoning or inferring; and an ability to gain direct knowledge or cognition without excessive instruction.
l. **Mission Command Enablement.** Evaluates the standard in terms of the FM-6.0 concept generally defined as Command & Control, Situational Awareness, and Distributed Planning.

2.2 Technical Standards Maturity Model (TSMM)

The TSMM maturity assessment process provides analysis and information for use with other evaluation criteria to provide an assessment methodology 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 purpose of the TSMM is to consistently assess the maturity of standards within the Technical Guidance. The TSMM measures five 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 Source Attribute, Backward Compatibility (BWC) Attribute, Industry Maturity Attribute, Adoption in Marketplace Attribute, and Ethernet Over Internet Protocol (EoIP)-based Adaptability/Supportability Attribute. In applying the TSMM, the selected maturity level combined with each of the five attributes in the model combined result in a score to when comparing various standards under assessment. 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 attributes being assessed.

2.2.1 The Standard Source Attribute

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

Standard Source Attribute	
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 under development by organizations for a specific COI or WG, including commercial and military.
Level 3	Standard is developed and maintained by military standard organizations, e.g., MIL-STD (Military Standard) (DoD) and Standard Agreement (STANAG) (NATO).
Level 4	Standard is under development commercially by industry standard development organizations like Internet Engineering Task Force (IETF), American National Standards Institute (ANSI), International Telecommunications Union (ITU), Institute of Electrical and Electrical Engineers (IEEE), International Standards Organization (ISO), and World Wide Web Consortium (W3C).

Table 1 : Standard Source Attributes

2.2.2 The Backward Compatibility (BWC) Attribute

The BWC Attribute measures the degree to which the standard is BWC to its prior version.

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 BWC level.

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

Table 2: Backward Compatibility Attributes

2.2.3 The Industry Maturity Attribute

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, National Aeronautics and Space Administration (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. The most advanced or mature level 4 (on a 1 to 4 scale of the MM) is assigned when a technology has been qualified for usage in operational missions.

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

Table 3:Industry Maturity Attributes

2.2.4 The Adoption in Marketplace Attribute

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 Attribute	
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/Joint Information Environment (JIE) only.
Level 4	Standard is in wide use for its specific application by DoD and commercially.

Table 4: Marketplace Attributes

2.2.5 The EoIP-based Adaptability/Supportability Attribute

Everything over Internet Protocol (EoIP)-based Adaptability/Supportability measures the level to which this technology can be implemented to realize the EoIP approach for achieving the CIO/G-6 guidance.

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 Attribute	
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.

Table 5: EoIP-based Adaptability/Supportability Attributers

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.

3. Technical Standards Profiles (ATGR Profiles)

3.1 Purpose

The purpose of Technical Standard Profiles (ATGR Profiles) is to provide a minimum set of standards that are associated with a particular set of functionality or technology. The Technical Standard View is independent of any systems and particular requirements. However, it can be reusable and traceable to a particular capability and service/function. The use of Technical Standard Views can facilitate and standardize the selection of standards as part of the development of architectures.

3.2 A Technical Standards Profiles (ATGR Profiles) is defined by the following generalized criteria:

a. **Built at Atomic Level** - From a technology perspective, a Technical Standard Profile is built at an atomic level, meaning that:

1. Omitting any standards in the Technical Standard View would result in loss of function or capability supported by the profile as a whole; and
2. Addition of any standards would not add to the core function or capability supported by the profile.

b. **System Independent** - A Technical Standards Profile (ATGR Profile) is system independent, and thus is flexible to support any configuration of capabilities, such as Capability Sets (CS) or System of Systems (SoS).

c. **Capable of Supporting Frameworks** - A Technical Standard Profile is able to support, or be mapped to, various frameworks, such as:

1. Technical Reference Model (TRM) structure which includes Service Area, Service Category, Service Standard.
2. LandWarNet Capability Sets (LWN CS) taxonomy which includes Capability and Service/Function; and Joint Common System Function List (JCSFL) functions.

d. **Modified when Standards/Technologies Change** - There is a need to update a Technical Standard Profile only when the status of a standard or technology changes. This occurs when there is a new release of the DISR Baseline, or when a new technology is emerging.

3.3 Technical Standard Types

A technical standard may originate from various kinds of organizations, both public and private. Example organization types include a corporation, a consortium (a small group of corporations), a trade association (an industry-wide group of corporations), a national government (including its military, regulatory agencies, and national laboratories and institutes), a professional association (society), a purpose-made standards organization such as ISO, or vendor-neutral developed generic requirements. It is common for one organization to refer to (reference, call out, cite) the standards of another. Voluntary standards may become mandatory if adopted by a government or business contract.

3.4 Army Standards View – StdV-1 (Standards Profile) and StdV-2 (Standards Forecast) for the Common Operating Environment (COE)

3.5 Value Proposition for an Army Standards View for COE:

The Common Operating Environment (COE) is an approved set of computing technologies and standards that enable secure and interoperable applications to be developed and deployed rapidly across five defined computing environments (CE). The Army StdV-1 and StdV-2 provide the current and forecasted standards for the Army. The CIO/G-6 will collaboratively develop an Army Annual StdV-1/2 each year to provide planning guidance for COE beginning with COE 3.0. This document is the Army

Standards Profile Guidance Version 1.0 (In support of Common Operating Environment V3). Specific development guidance will be provided by ASA(ALT) to PMs and CE leads through the use of Army Annual Standards View 1/2. The Army Annual StdV-1 and StdV-2 encompass all five layers in the COE Technical Reference Model (TRM). The Army Standards Profile and Forecast:

a. Contribute to achieving agility on how we deliver capabilities across all mission areas.

b. Reduce the life cycle cost of development and sustainment of our IT systems by eliminating unnecessary duplication.

c. Help to promote an open architecture that is standards based that leverages industry's best practices and products while reserving government purpose rights.

d. Contribute to building on a foundation that is cyber hardened and secure.

e. Contribute to achieving simplification of the Network through ease of use and reduced number of systems.

3.6 Approach

a. Each year, the Army CIO/G-6, in close coordination with ASA(ALT), will develop an Annual Standards View StdV-1 (Standards Profile) in the May timeframe to provide ASA(ALT) with the enterprise level guidance in the June timeframe required to begin the planning process and inform the Program Objective Memorandum (POM) cycle.

b. Annually, Program Managers (PMs) will develop standards profiles and waiver requests for individual Programs of Record (PoR) using the Army StdV-1 as a baseline and adjust the profile based on requirements for their respective systems for the next year. (See Figure). PMs will submit their systems profiles to the Computing Environment (CE) leads to produce a CE StdV-1 and StdV-2 (Standards Forecast). ASA(ALT) System of Systems Engineering & Integration (SOSE&I) will do an analysis across CEs and build a COE profile that is based on the cumulative System Profiles for all systems in the CEs and Control Point Specifications (CPS). The COE StdV-1 and StdV-2 will highlight what migrates, what sunsets, what is new, and what are common implementations across the COE. The COE StdV-1 and StdV-2 will be developed in the June/July timeframe for submission to the Army Acquisition Executive (AAE) for programmatic guidance to the CEs. This timeline supports the Weapons Systems Reviews (WSR) and POM cycles.

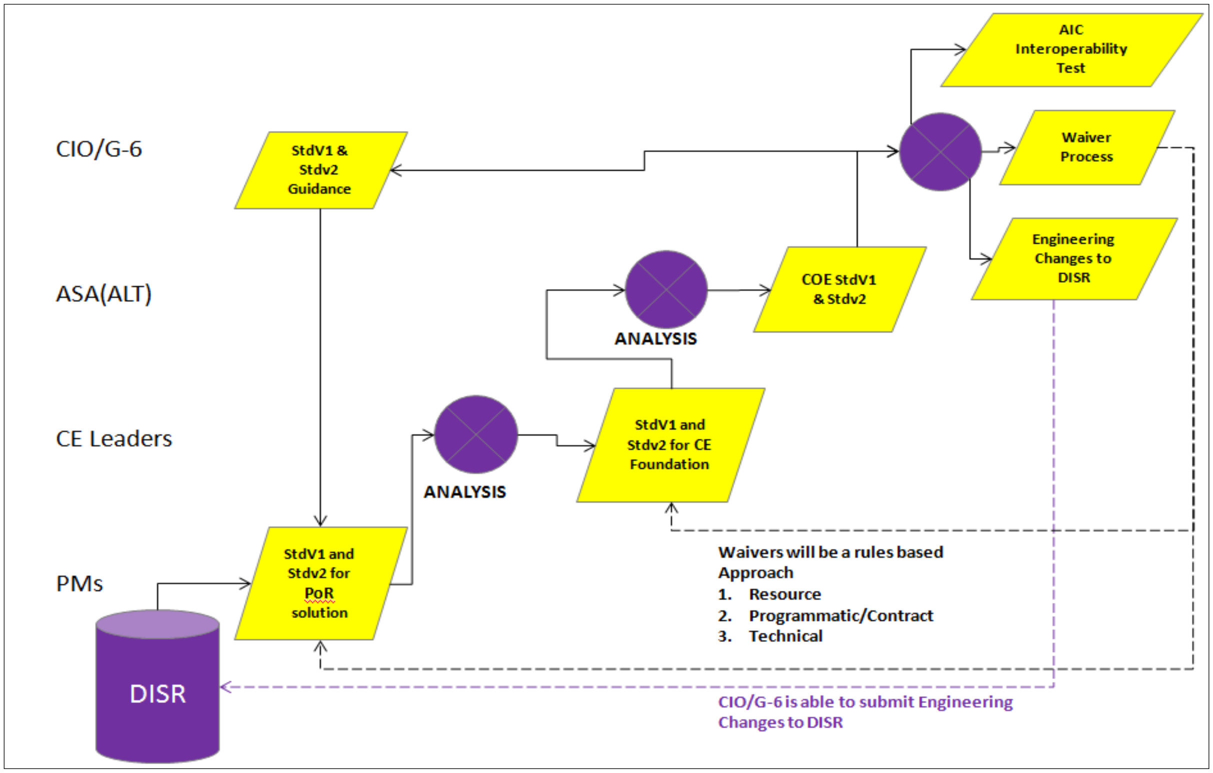

CIO/G-6
ASA(ALT)
CE Leaders
PMs
AIC Interoperability Test
Waiver Process
Engineering Changes to DISR
StdV1 & Stdv2 Guidance
COE StdV1 & Stdv2
ANALYSIS
StdV1 and Stdv2 for CE Foundation
ANALYSIS
StdV1 and Stdv2 for PoR solution
DISR
Waivers will be a rules based Approach
1. Resource
2. Programmatic/Contract
3. Technical
CIO/G-6 is able to submit Engineering Changes to DISR

Figure 2: Annual StdV-1/2 Process Flow for COE

4. Technical Architecture Processes

4.1 Purpose

The purpose of these process diagrams is to articulate the various processes used in support of the HQDA CIO/G-6 Technical Architecture development mission. These processes have been formalized in order to provide best practices, discipline, and consistency in the execution of this mission. In all cases, the operational drivers are used as input.

The use of these standards will be worked into the Business Capabilities Lifecycle (BCL) and/or Army Enterprise Network (AEN) solutions processes in the future. The Defense Information Systems Agency (DISA) has a well-established process for managing standards through the technology lifecycle by leveraging the official DISR statuses. Through the DISR process, standards are first published in emerging status, then raised to mandated, then moved to sunset, and finally retired. The DISR processes are available at the DISRonline GIG Technical Guidance Federation web site at https://gtg.csd.disa.mil/uam/login.do (CAC required). The processes and methodologies described below are the technical guidance development processes the CIO/G-6 uses.

4.2 Technical Guidance Development Process

The process and methodology described below in Figure 3 is the technical guidance development process. Based on various inputs, system engineering analysis is done to prescribe accurate technical standards to align with the Network Strategy and Capability Sets.

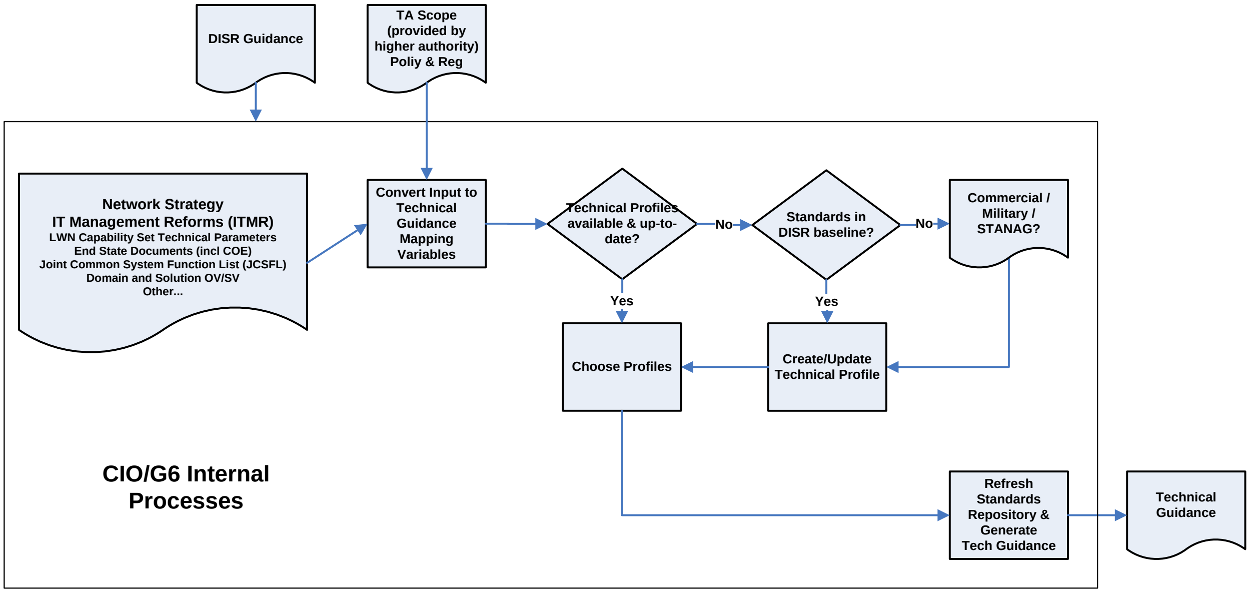

DISR Guidance
TA Scope (provided by higher authority) Poliy & Reg
Network Strategy
IT Management Reforms (ITMR)
LWN Capability Set Technical Parameters
End State Documents (incl COE)
Joint Common System Function List (JCSFL)
Domain and Solution OV/SV
Other...
Convert Input to Technical Guidance Mapping Variables
Technical Profiles available & up-to-date?
No
Standards in DISR baseline?
No
Commercial / Military / STANAG?
Yes
Yes
Choose Profiles
Create/Update Technical Profile
CIO/G6 Internal Processes
Refresh Standards Repository & Generate Tech Guidance
Technical Guidance

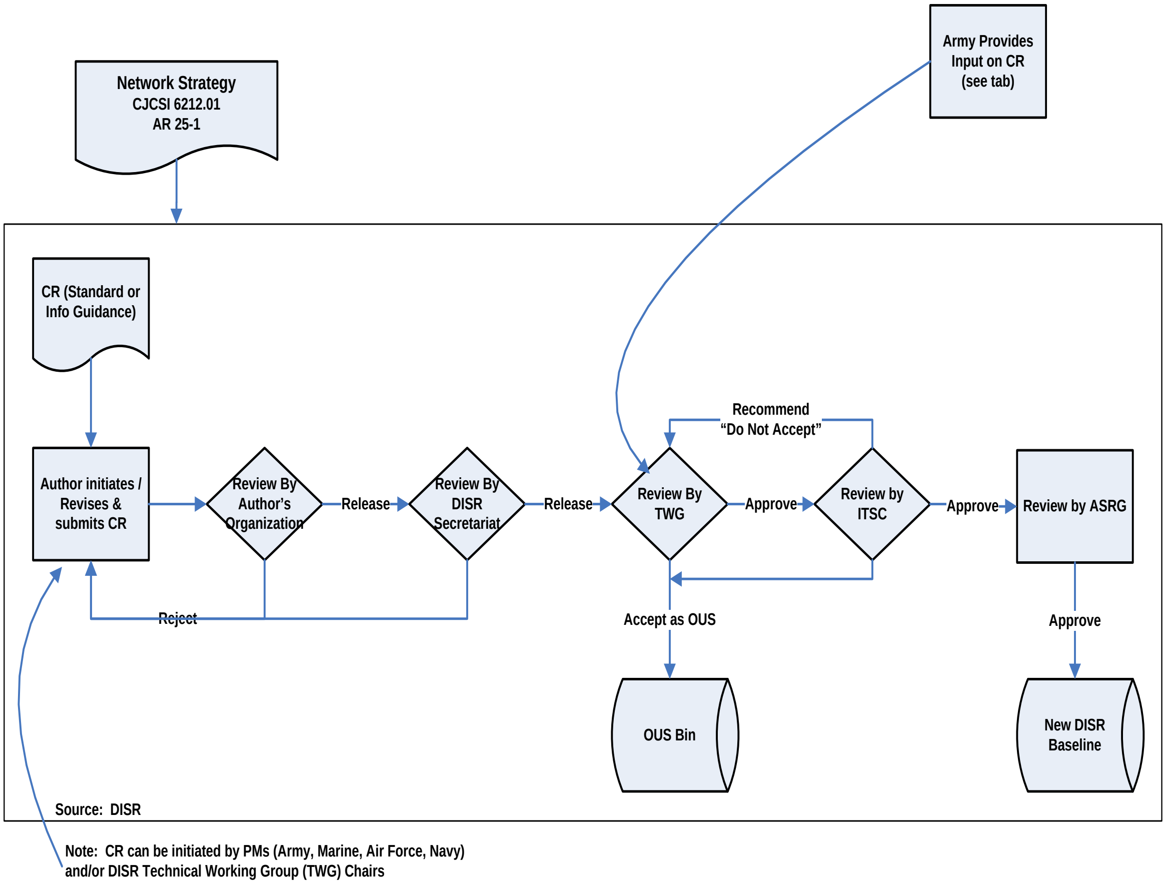
Figure 3: Technical Guidance Development Process

4.3 DISR Change Request Process

The Army change request process utilizes the DISR process that, by definition, relates to a DISR status change for a standard or information guidance. The DISR process is shown in Figure 4, and the CIO/G-6 role in this process is illustrated in Figure 5.

A PM initiates the CR. The author's immediate organization reviews the CR for release. Then the DISR Secretariat similarly reviews the CR prior to moving it 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 BWC and 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. 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.


Army Provides Input on CR (see tab)
Network Strategy
CJCSI 6212.01
AR 25-1
CR (Standard or Info Guidance)
Recommend "Do Not Accept"
Author initiates / Revises & submits CR
Review By Author's Organization
Release
Review By DISR Secretariat
Release
Review By TWG
Approve
Review by ITSC
Approve
Review by ASRG
Reject
Accept as OUS
Approve
OUS Bin
New DISR Baseline

Source: DISR

Note: CR can be initiated by PMs (Army, Marine, Air Force, Navy) and/or DISR Technical Working Group (TWG) Chairs

Figure 4: DISR Baseline Change Request (CR) Process

During execution of the DISR CR process, the CIO/G-6 performs further analysis of standards on behalf of the Army. This sub-process of the CR process includes application of the TSMM, outlined in greater detail in Section 2 of this document.

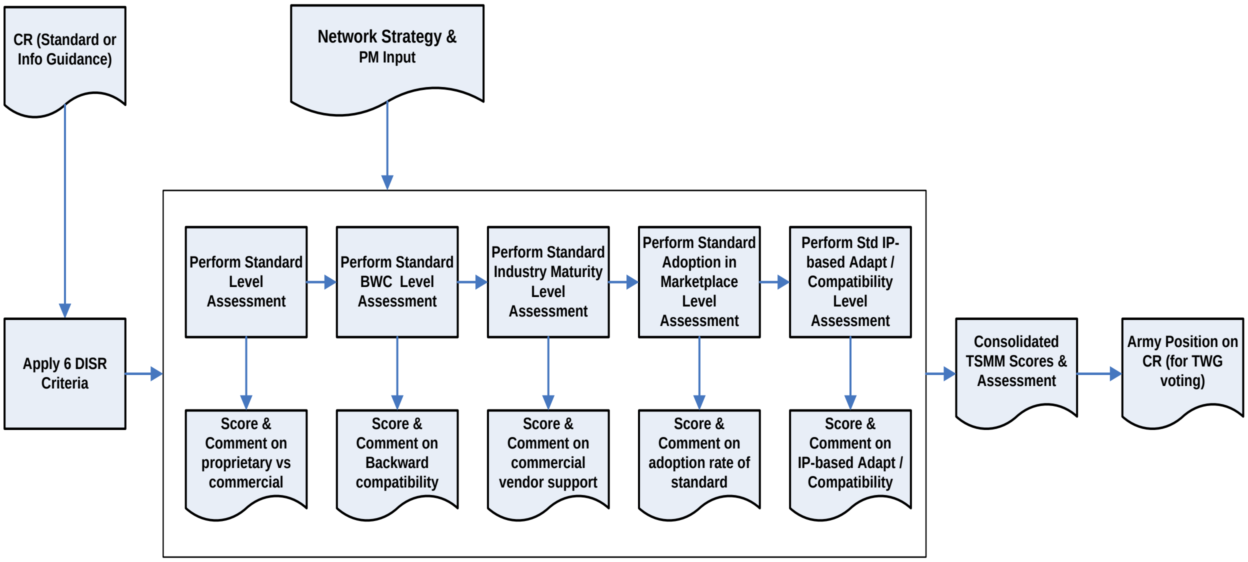

CR (Standard or Info Guidance)
Network Strategy & PM Input
Apply 6 DISR Criteria
Perform Standard Level Assessment
Perform Standard BWC Level Assessment
Perform Standard Industry Maturity Level Assessment
Perform Standard Adoption in Marketplace Level Assessment
Perform Std IP-based Adapt / Compatibility Level Assessment
Score & Comment on proprietary vs commercial
Score & Comment on Backward compatibility
Score & Comment on commercial vendor support
Score & Comment on adoption rate of standard
Score & Comment on IP-based Adapt / Compatibility
Consolidated TSMM Scores & Assessment
Army Position on CR (for TWG voting)

Figure 5: CIO/G-6 Army Input Process to DISR Change Request (CR) Process

4.4 Information Support Plan (ISP) Review Process

The primary DoD guidance for the ISP Review is DoDI 8330.01 Interoperability of Information Technology (IT) Including National Security Systems (NSS) dated 21 May 2014. Figure 6 depicts the internal ISP review process for systematic analysis of ISPs, with emphasis on StdV/TV (Technical View) validation, including checking compliance with CIO/G-6 technical guidance.

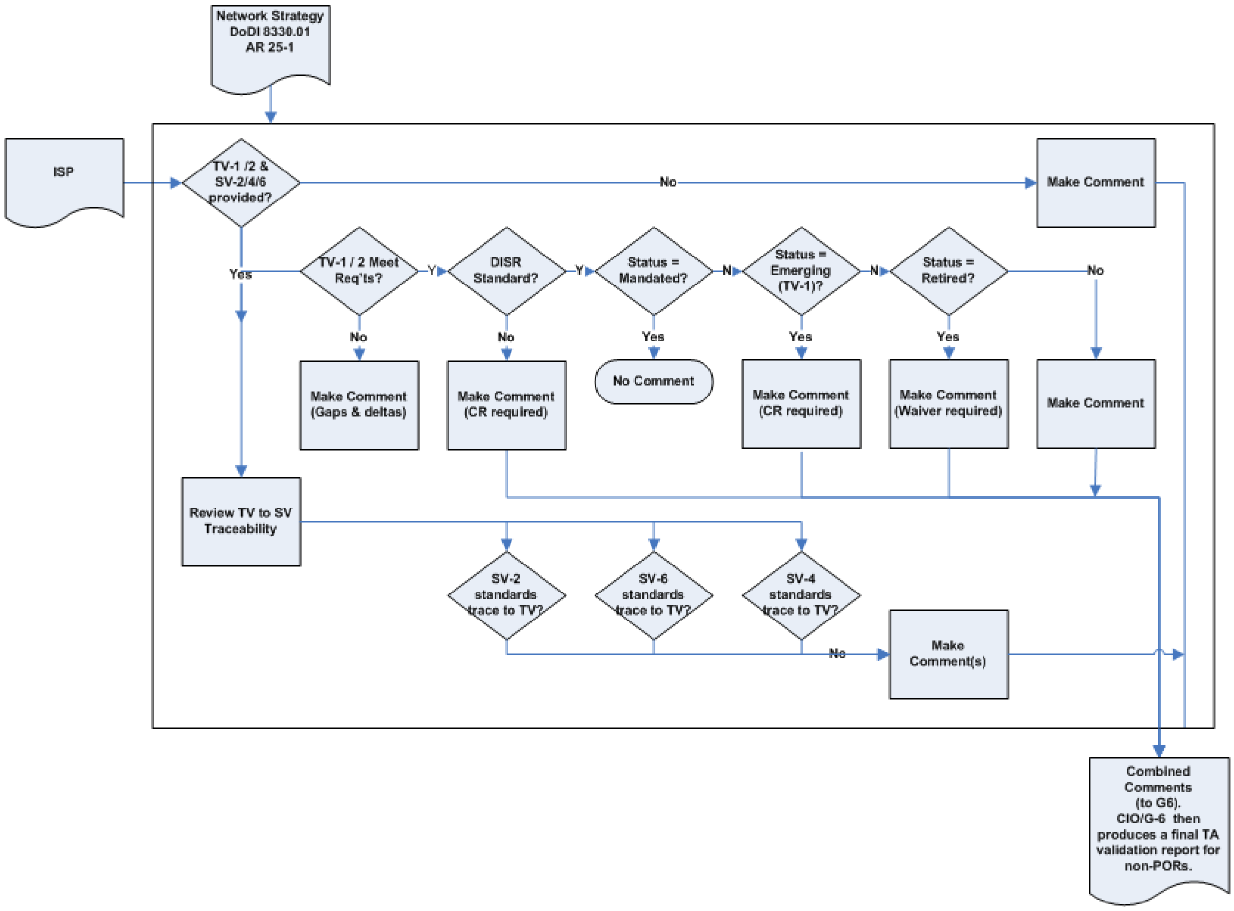

Network Strategy
DoDI 8330.01
AR 25-1
ISP
TV-1 /2 & SV-2/4/6 provided?
No
Make Comment
Yes
TV-1 / 2 Meet Req'ts?
Y
DISR Standard?
Y
Status = Mandated?
N
Status = Emerging (TV-1)?
N
Status = Retired?
No
No
No
Yes
Yes
Yes
Make Comment (Gaps & deltas)
Make Comment (CR required)
No Comment
Make Comment (CR required)
Make Comment (Waiver required)
Make Comment
Review TV to SV Traceability
SV-2 standards trace to TV?
SV-6 standards trace to TV?
SV-4 standards trace to TV?
No
Make Comment(s)
Combined Comments (to G6). CIO/G-6 then produces a final TA validation report for non-PORs.

Figure 6: ISP Review Process

4.5 Technical Architecture (TA) Process for Validation of Non-Programs of Record

Since non-programs of record are not subject to JCIDS analysis, TA validations are often performed. The TA validation is similar to the Infrastructure Support Plan Reviews 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 non-programs of record may be different than for a PoR, since non-programs of record are not subject to the JCIDS requirements. Some improvising and common sense logic consistent with principles found in guidance for PoRs needs to be applied. Figure 7 depicts this process below:

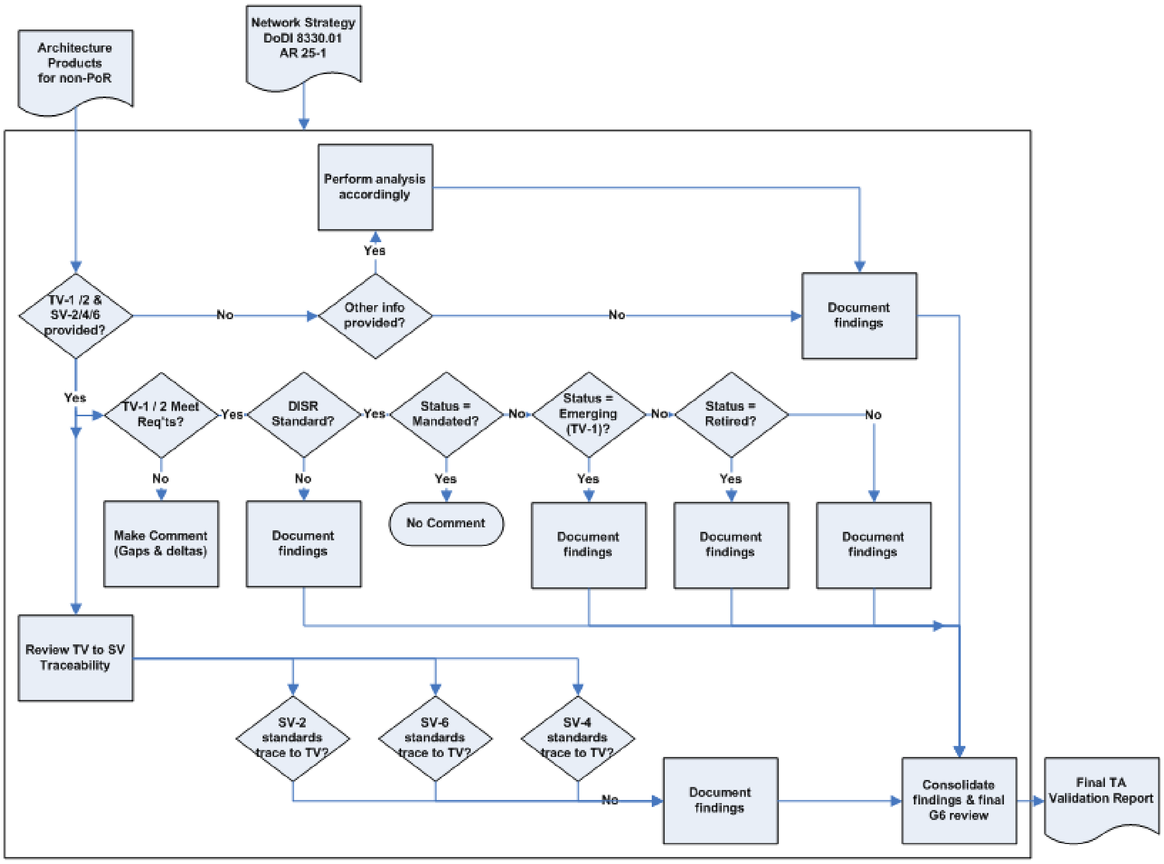

Architecture Products for non-PoR
Network Strategy DoDI 8330.01 AR 25-1
Perform analysis accordingly
Yes
TV-1 /2 & SV-2/4/6 provided?
No
Other info provided?
No
Document findings
Yes
TV-1 / 2 Meet Req'ts?
Yes
DISR Standard?
Yes
Status = Mandated?
No
Status = Emerging (TV-1)?
No
Status = Retired?
No
No
No
Yes
Yes
Yes
Make Comment (Gaps & deltas)
Document findings
No Comment
Document findings
Document findings
Document findings
Review TV to SV Traceability
SV-2 standards trace to TV?
SV-6 standards trace to TV?
SV-4 standards trace to TV?
No
Document findings
Consolidate findings & final G6 review
Final TA Validation Report

Figure 7: TA Validation (Non-PoR) Process

4.6 DISR and Army Waiver Approval Process

The DISR waiver process applies to emerging and retired standards. 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:

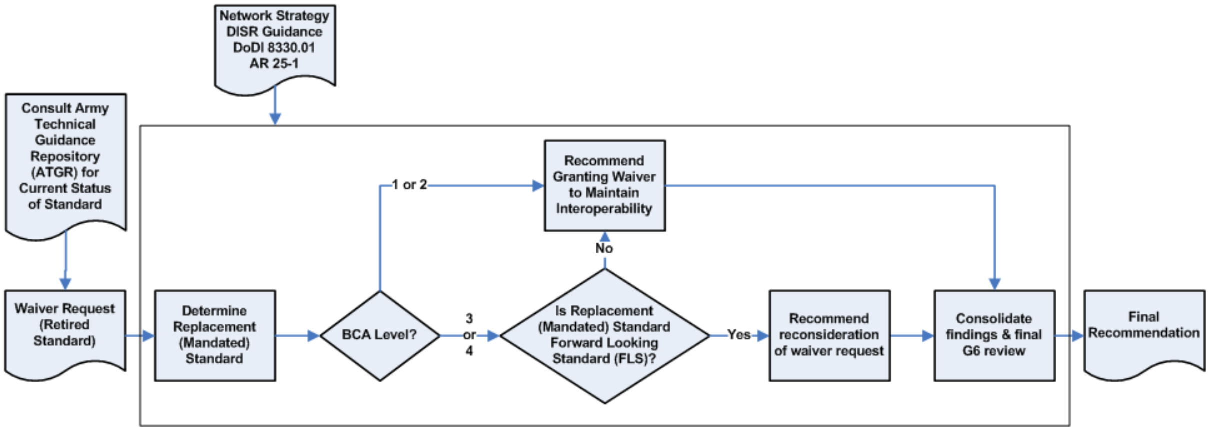

Network Strategy
DISR Guidance
DoDI 8330.01
AR 25-1
Consult Army Technical Guidance Repository (ATGR) for Current Status of Standard
Waiver Request (Retired Standard)
Determine Replacement (Mandated) Standard
BCA Level?
1 or 2
3 or 4
Recommend Granting Waiver to Maintain Interoperability
No
Is Replacement (Mandated) Standard Forward Looking Standard (FLS)?
Yes
Recommend reconsideration of waiver request
Consolidate findings & final G6 review
Final Recommendation

Figure 8: DISR and Army Waiver Process

Appendix A – Acronyms / Glossary

Acronyms

Acronym	Term
ABC	Army Business Council
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
ATGR	Army Technical Guidance Repository
CAC	Common Access Card
COCOM	Combatant Command
COE	Common Operating Environment
DISA	Defense Information Systems Agency
DISR	DoD Information Standards Registry
DoD	Department of Defense
EA	Enterprise Architecture
EoIP	Everything over Internet Protocol
IA	Information Assurance
IE	Information Environment
IT	Information Technology
JIE	Joint Information Environment
LandWarNet / LWN	Land Warrior Network
NR	Network Roadmap
OBT	Office of Business Transformation
R&D	Research and Development
SWaP	Size, Weight, and Power
TA	Technical Architecture
TPN	Tactical Processing Node
TRADOC	Training and Doctrine Command
TRM	Technical Reference Model
UAP	Unified Action Partner

Appendix B – Glossary

Term	Definition
Backward Compatibility	The Backward Compatibility (BWC) Attribute measures the degree to which the standard is BWC to its prior version.
Change Request	A change request relates to a DISR status change for a Standard or Information Guidance.
DoD Information Systems Registry	The DoD IT Standards Registry (DISR), is an online repository of IT standards formerly captured in the Joint Technical Architecture (JTA), Version 6.0. DISR replaces JTA. DISR online supports the continuing evolution of the DISR and the automation of all its processes; it can be accessed at https://disronline.disr.mil. DISR online is the repository for information related to DOD IT and National Security Systems (NSS) standards.
Everything over Internet Protocol	For the intent of this architecture document EoIP refers to integrating voice, video and data collaboration services to Internet Protocol.
GIG Technical Guidance Federation (GTG-F)	The GIG Technical Guidance Federation (GTG-F) is a suite of software applications on the NIPRNet and SIPRNet (June 2012) that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. The GTG-F content provides the technical information to various users in addressing and resolving technical issues needed to meet functional requirements (i.e., features and capabilities) of the GIG. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications. In addition to other resources the GTG-F includes the DoD Information Technology Standards Registry – Online (DISROnline).
Mandated Standard	A mandated standard is approved for use by DISA through a governance process with participating from the Services.
Standards View (StdV-1) Standards Profile	A listing of standards that apply to the Information Enterprise solution elements.
Standards View (StdV-2) Standards Forecast	Describes emerging standards and potential impact on the Information Environment solution elements.

Waiver	The process of requesting an exception to use a non-DISR standard or technology that is not an OUS.

Appendix C – Army Standards Profile Guidance in Support of COE v3, version 1.0 (To Be Published Separately)