



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, JEL

CJCSI 6610.01E
10 April 2014

TACTICAL DATA LINK STANDARDIZATION AND INTEROPERABILITY

References: See Enclosure D.

1. Purpose. In accordance with (IAW) references a through s, this instruction establishes policy to achieve and maintain interoperability among those Department of Defense (DoD) information technology (IT) and national security systems (NSS) that implement tactical data links (TDL). Policies outlined in this instruction are focused on achieving interoperability through the standardization of message protocols, format, content, implementation, and documentation. IAW reference a, this instruction establishes procedures for the development, review, and validation of IT and NSS TDL message standards based on compatibility, interoperability, and integration requirements. It also establishes procedures for ensuring compliance through joint interoperability certification and program review. As directed by reference b, it establishes procedures for the validation of interface standards and compatibility requirements for TDL message protocol format and content. Applicable TDL-related standards are found in Enclosure B.

2. Superseded/Cancellation. CJCSI 6610.01D, "Tactical Data Link Standardization Implementation Plan," 30 December 2010, is superseded.

3. Applicability. This instruction applies to the Joint Staff (JS), Combatant Commands (CCMDs), Military Departments, and DoD Agencies and activities. It is also recommended for other Federal Departments implementing TDLs. The Joint Multi-Tactical Data Link Standards Working Group (JMSWG) Terms of Reference (reference c) and the Joint Multi-Tactical Data Link Configuration Control Board (JMTCCB) Terms of Reference (reference d) establish TDL configuration management procedures.

4. Policy. See Enclosure A.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Summary of Changes

a. Clarifies that JS J6 has assumed the responsibilities of the disestablished U.S. Joint Forces Command.

b. Adds MADL and CoT MIL-STDs to the CM responsibilities of the JMTCCB.

c. Replaces references to the Joint TDES Migration Plan with the Joint TDL Migration Plan (JTMP).

d. Harmonizes instruction with various related administrative changes (newer references, name changes to groups and/or organizations, etc.).

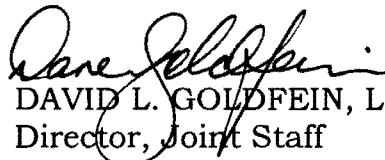
e. Defines the requirement for C/S/As to use the Interoperability Enhancement Process (IEP), which pursues bit-level interoperability and defines implementation documentation requirements.

f. Changes the name of CJCSI 6610 from "Tactical Data Link Standardization Implementation Plan" to "Tactical Data Link Standardization and Interoperability" for clarification and better alignment with document focus.

8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNET. DoD Components (to include the Combatant Commands), other Federal Agencies, and the public, may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at http://www.dtic.mil/cjcs_directives. JS activities may also obtain access via the SIPR directives Electronic Library websites.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joints Chiefs of Staff:


DAVID L. GOLDFEIN, Lt Gen, USAF
Director, Joint Staff

Enclosures

- A - Policy
- B - Responsibilities
- C - TDL Standards Publications
- D - References
- GL - Glossary

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY

DoD IT and NSS implementing TDLs will comply with applicable TDL message standards and their associated documentation (Enclosure B). Compliance with TDL message standards is fundamental to achieving and maintaining joint and coalition compatibility and interoperability.

a. Documentation. TDL message standards are defined in U.S. Military Standard (MIL-STD) documents and North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAG). Joint Multi-Tactical Data Link Operating Procedures are contained in reference f. For NATO, the equivalent document is Allied Data Publication 33.

b. Certification. Joint Interoperability, Implementation Requirement Exceptions, Interim Certificate to Operate, National and Service Difference Documents, and Platform Implementation

(1) Joint Interoperability Test Certification. Joint Interoperability certification is required for all IT and NSS that implement TDLs prior to operating in joint or multinational arenas. The Interoperability Steering Group (ISG) will review systems that are placed in operation without joint certification for consideration and possible inclusion on the Operating at Risk List as defined in reference r. CCMDs will notify the ISG, through the JS J6, of any operational system within their area of responsibility that does not have a joint certification and of any interoperability issues associated with data link operations.

(2) Implementation Requirement Exceptions. Compliance with implementation requirements specified in TDL message standards is essential for ensuring joint and coalition interoperability. In some instances, however, an IT and NSS may support a mission so narrowly defined it would be inefficient and disadvantageous to comply with all message standard implementation requirements. In these cases, the JMTCCB may approve requests for exceptions to implementation requirements. IAW its responsibility as Joint Force Integrator, the JS J6 representative to the JMTCCB must concur in any implementation requests for exceptions by evaluating user requirements and weighing the interoperability impact. Normally, exceptions will be approved in advance of IT and NSS joint interoperability certification. Exceptions are intended to be permanent or temporary (shall not exceed 4 years, with no renewal) and will be included in all Service/Agency and

system-level description documentation. Exceptions do not constitute a waiver of the requirement for IT and NSS certification testing IAW references g and s. However, the Joint Interoperability Test Command and Joint Analysis Review Panels shall consider the approved requests for exceptions to requirements when making a determination on whether to certify TDL systems.

(3) Interim Certificate to Operate (ICTO). An ICTO, as outlined in reference r, is approved by the ISG. It is temporary (may not exceed 1 year in duration) and is approved only in exceptional cases where an IT and NSS is required to be used operationally prior to completion of joint interoperability certification. An ICTO does not waive the requirement to complete certification testing IAW reference r.

(4) National Difference Document (NDD). The national requirements documentation defines a specific nation's requirements in terms of message transmission and reception protocols and message formats, field coding and data (Data Field Identifiers, Data Use Identifiers and Data Items). These requirements can be viewed either in the form of an NDD or National Requirements Specification. An NDD will document the differences between a MIL-STD (e.g., MIL-STD-6016) and another, higher-level standard (in this example, STANAG 5516). However, an NDD is not always necessary; for some of the MIL-STDs, there may not be a corresponding, higher-level, multinational standard.

(5) Service Difference Document (SDD). An SDD, once approved and/or developed, will define the differences between MIL-STD requirements and a specific Service's TDL requirements to fulfill that Service's national data link philosophy and operational needs. Each Service's SDD shall be reviewed and approved by the JMTCCB. Approved SDD requirements shall become part of the current MIL-STD baseline and shall be considered in developing certification requirements and analyzing test results for the platforms of that Service. Joint Interoperability Test Command and Joint Analysis Review Panels shall consider the approved SDD requirements when making a determination on whether to certify TDL systems.

(6) Message Implementation Plan (MIP). The MIP defines a program's platform's implementation development plan; through a two part process initially outlining the high-level (Message and Word level) implementation requirements to support identified mission areas and TDL capabilities.

(a) The initial MIP supports high-level analysis of the TDL functions areas, and Mission Area interoperability assessments to develop a recommendation for approval or disapproval by the Service-level authority in order to proceed with development of the supporting implementation artifacts.

(b) The final MIP is the template to develop and mature the technical solution, which shall include the Platform Requirements Specification (PRS), and Platform Requirements Difference Document (PRDD) to satisfy a platform's Information Exchange Requirements.

(c) To support the requirement of reference g for TDL participants to provide the final MIP prior to Milestone C, JS J6 will review the MIP during the Joint Capabilities Integration Development System (JCIDS) process to conduct initial Joint Mission Area interoperability assessments.

(7) Platform Requirements Specification (PRS). The PRS defines the baseline of a platform's subset of the requirements from the MIL-STD and does not change. The PRDD format is used to explain the differences between the MIL-STD and the PRS. Deviations from a platform's TDL implementation requirements shall be approved by the JMTCCB.

(8) Platform Implementation Difference Document (PIDD). The PIDD format is used to explain the implementation differences from the development baseline standard, which is initially transitioned from the PRDD. Each PIDD entry defines the rationale for the deviation and, if applicable, a workaround. All fielded or actual deviations from the baseline standard after the platform implementation has been tested are documented.

(9) Actual Platform Implementation Specifications (APIS). The APIS are created following the development and testing of a platform's implementation. They document the fielded (actual) implementation data of the platform and define the program's actual performance. The APIS can change often as problems are identified and corrected. The APIS/PIDD support interoperability evaluations to identify capability gaps against functional requirements and interoperability assessments of data exchange between TDL capable platforms.

(10) Platform Bit-Level Implementation. The TDL bit-level implementation contained in the APIS identifies the data item details—Data Field Identifiers (DFIs) and Data Use Identifiers (DUIs)—for transmission and reception. The deviations from the required implementation plan detailed in the PRS/PRDD and implementation differences documented in the PIDD. The TDL bit-level implementation should be provided after the platform's program has been developed and tested but before it is submitted for joint certification testing. The procedures governing the development of the required implementation are the same as that of the actual implementations.

c. Configuration Management. The Defense Information Systems Agency (DISA) Enterprise Engineering Directorate (EE), Systems Engineering Division

(EE2), Tactical Standards Branch (EE21), Tactical Data Link Standards Section (EE211), is responsible for configuration management of TDL MIL-STDs (reference f) and other associated documents. DISA is the U.S. custodian for applicable U.S. and NATO TDL documents.

(1) The JMSWG is the forum for resolving interoperability issues related to TDL message standards format, structure, and development. The JMTCCB is the configuration management authority for TDL, Multifunction Advanced Data Link (MADL), and Cursor on Target (CoT) MIL-STDs, applicable NATO STANAGs, CJCSM 6120.01, and other associated U.S. and NATO TDL documents. Action officer review of these documents will be accomplished within the JMTCCB. JS J6 will represent the CCMDs during the JMSWG and JMTCCB and will staff critical issues with the CCMDs prior to these meetings. Recommended changes to reference f may be submitted to appropriate JMSWG and JMTCCB representatives, the JS J6, or DISA at any time. Interoperability issues beyond the scope of the JMTCCB and JMSWG will be referred to the ISG for resolution.

(2) Each CCMD, Service, or DoD Agency (C/S/A) will participate in the information technology standards process. IAW references c and d, JS J6 will represent Combatant Commanders at the JMSWG and JMTCCB. Representatives are responsible for providing their respective organization's position on all issues. Representatives will be empowered to commit their organization's assistance in matters requiring coordination. C/S/As that fail to participate in either the JMSWG or JMTCCB will automatically abstain from any decision or vote that occurs at either forum.

(3) In the event a C/S/A's position is substantive and cannot be resolved at the JMSWG or JMTCCB, the issue will be taken to the Military Communications-Electronics Board (MCEB)¹ for adjudication.

d. Migration Strategy. IAW the Joint TDL Migration Plan (JTMP) (reference h), one method for achieving TDL interoperability is through migration of non-interoperable legacy TDL message standards to the joint family of TDL message standards described in that document. Adherence to JTMP policy will be a factor in consideration of ICTO requests, interoperability certification, and joint message standard development.

¹ An update to DoD Directive 5100.35, Military Command, Control, Communications, and Computers (C4) Executive Board (MC4EB), is currently in staffing and will replace the current MCEB structure when complete.

e. Joint Interoperability of Tactical Command and Control Systems (JINTACCS) Transformation. The C/S/As will continue building on DoD, JS, and Service/Agency initiatives to transform the JINTACCS program.

(1) These initiatives include, but are not limited to, improving interoperability planning; interoperability systems management and documentation; and requirements identification and prioritization. C/S/As will also continue to develop standardized procedures and processes for analyzing and documenting information exchange requirements and defining, managing, and assessing system-specific bit-level information-processing and display functions.

(2) The DoD CIO adoption of the National Information Exchange Model (NIEM) as the basis for a significant portion of its data exchange strategy facilitates the ability to share information among multinational, interagency and Service entities. DoD's strategy includes the creation of a Military Operations (MilOps) domain, which leverages the maturity of NIEM with a common interoperability approach. The MilOps domain provides a migration path for multiple formats and standards and allows the tactical community the advantage of shared data definitions, methods, and tools for building data components and requisite Information Exchange Package Documentation. Additionally, the MilOps domain increases its content and viability by leveraging operationally mature tactical information exchanges. Initial transformation intent is to incrementally capture and re-use data items from MIL-STDs, providing participants with benefits from DoD's interoperability advances.

(INTENTIONALLY BLANK)

ENCLOSURE B

RESPONSIBILITIES

1. The Chairman of the Joint Chiefs of Staff will establish procedures during the JCIDS process for the development, coordination, and review of joint TDL message standards, NATO STANAGs, and other associated documentation for DoD IT and NSS.
2. C/S/A will:
 - a. Ensure TDL systems conform to joint TDL message standards.
 - b. Ensure that JCIDS documents identifying TDL systems (e.g., Information Support Plans) contain directives to implement Joint TDL standards and/or STANAGs, as appropriate.
 - c. Identify and provide required corrections and improvements to TDL message standards and/or STANAGs and interface operating procedures, and fully participate in the configuration management of these documents IAW references c through e.
 - d. Ensure fielding plans conform to approved joint TDL migration plans.
 - e. Ensure all system- and platform-specific TDL implementations comply with the approved requirements, documents, and operational and system views of approved integrated architectures. If the user community becomes aware of a significant IT and NSS compliance deficiency, report this deficiency, as appropriate, to the JS, Service Chief Information Officer (CIO), or DoD CIO for corrective action.
 - f. The C/S/As will continue building on DoD, JS, and Service/agency initiatives to transform the JINTACCS program.
 - (1) These initiatives include, but are not limited to, improving interoperability planning, interoperability systems management and documentation, and requirements identification and prioritization. C/S/As will also continue to develop standardized procedures and processes for analyzing and documenting information exchange requirements and defining, managing, and assessing system-specific bit-level information-processing and display functions.

(2) Capability developers who are implementing tactical data standards within their IT and NSS solutions will leverage the IEP. IEP is an effort, co-chaired by JS J6 and DISA, which pursues bit-level interoperability and defines implementation documentation requirements. IEP consists of the Interoperable Systems Management and Requirements Transformation (iSMART) processes, the Enhanced Systems Management and Requirements Transformation (eSMART) tool set, and the Joint Capabilities and Limitations (JC&L) interoperability tool. The development process for platform-level TDL requirements implementation, including formats, is addressed in the iSMART Military Handbook (MIL-HDBK-524) (reference q). IEP improves tactical data and sensor interoperability, and provides joint planners and operational users information on how systems interact in joint networks. Standards management will take into account the requirements of DoD Instruction (DoDI) 4120.24, Defense Standardization Program (DSP), and DoDI 4120.24-M, DSP Policies and Procedures.

3. CCMDs will:

a. Identify and provide required corrections and improvements to joint TDL message standards and interface operating procedures. In coordination with JS J6, fully participate in the configuration management of these documents IAW references c through e.

b. Identify, through Integrated Priority List submissions, the highest priority TDL issues within their area of responsibility, to include data link management, fielded systems that are either not interoperable or not supported, and warfighting capability shortfalls related to TDLs.

c. Advocate TDL standardization through appropriate Command and Control Interoperability or Interoperability Management Boards (CCIB/IMB) with coalition countries.

4. Directors of the National Security Agency, National Reconnaissance Office, and Defense Intelligence Agency will:

a. Ensure TDL systems implement joint TDL message standards as defined by and IAW the procedures found in references a through s, as appropriate.

b. Identify and provide required corrections and improvements to joint TDL message standards and interface operating procedures, and fully participate in the configuration management of these documents IAW references c through e.

5. DISA is executive agent for the JINTACCS program, including Link-11, Link-11B, Link-16, Link-22, Variable Message Format (VMF), MADL, CoT, Joint

Range Extension Applications Protocol (JREAP), and Integrated Broadcast Service (IBS) Common Message Format (CMF). In this capacity, DISA will:

- a. Serve as DoD single point of contact for development and configuration management of joint TDL message standards. DISA will execute the responsibilities of the Lead Standardization Activity and Preparing Activity for designated TDL message standards.
- b. In collaboration with other DoD Components, identify information exchange requirements and develop standardized procedures and formats for information flow and implementation documentation within and between TDLs and between IT and NSS systems and common data sources.
- c. Maintain a list of approved TDL interface standards against which IT and NSS must be certified.
- d. Convene and chair the JMSWG. The JMSWG is the authority for development of U.S. TDL message standards and the focal point for resolving standards issues related to U.S. and coalition TDL interoperability IAW reference c.
- e. Convene and chair the JMTCCB. The JMTCCB approves all changes to U.S. TDL message standards and associated documentation IAW reference d, and establishes U.S. positions regarding allied or NATO TDL interoperability, including all changes to TDL STANAGs and associated documentation.
- f. Identify, program, and provide resources to accomplish DISA responsibilities for TDL message standard management.
- g. IAW reference i, act as classification authority for TDL message standards.
- h. Act as U.S. Representative during applicable CCMD C2 CCIBs or IMBs to advocate TDL standardization with coalition countries.
- i. Distribute the TDL MIL-STDS and NATO STANAGS using ASSIST for distribution within the U.S. and other appropriate means for coalition partners.

6. DoD Responsibilities

a. The DoD CIO (responsibilities outlined in references j through m) will review Service compliance with TDL interoperability policies established by this instruction and references a through s (including reference n, DoD Information Technology Standards Registry). Based on this review and evaluation, the DoD

CIO will make recommendations to the Defense Acquisition Executive (DAE) (reference o) regarding program funding.

b. The DAE will take appropriate action, either independently or based on recommendations from the DoD CIO and Military Department CIOs, to enforce program compliance with interoperability policy.

c. The DAE may direct the DoD Chief Financial Officer (reference p) and the heads of Military Departments to withhold acquisition program funds based on failure to comply with TDL interoperability policies, migration plans, or interoperability shortfalls.

d. Office of the Assistant Secretary of Defense for Production and Logistics, Economic Security Division, will manage and produce MIL-STDs and military bulletins for the TDL program.

ENCLOSURE C

TDL STANDARDS PUBLICATIONS

<u>TDL</u>	<u>Associated Publications</u>
Link-4A	MIL-STD-6004
Link-11/11B	MIL-STD-6011
Link-16	MIL-STD-6016 & STANAG 5516
Link-16 terminal (MIDS)	STANAG 4175 (no U.S. MIL-STD equivalent)
VMF	MIL-STD-6017
IBS CMF	MIL-STD-6018
JREAP	MIL-STD-3011 & STANAG 5518
Link-22	STANAG 5522 (no U.S. MIL-STD equivalent)
TDL Data Forwarding	MIL-STD-6020
MADL	TIDP/TE In development
CoT	TIDP/TE In development

(INTENTIONALLY BLANK)

ENCLOSURE D

REFERENCES

- a. DoD Directive 4630.05, 5 May 2004, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”²
- b. DoD Instruction 4630.8, 30 June 2004, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”²
- c. Defense Information Systems Agency, Tactical Standards Management Branch (EE21), 1 December 2012 “Terms of Reference Joint Multi-Tactical Data Link Standards Working Group (JMSWG)”
- d. Defense Information Systems Agency, Tactical Standards Management Branch (EE21), 14 February 2012, “Terms of Reference for the Joint Multi-TDL Configuration Control Board (JMTCCB)”
- e. DoD Directive 5105.19, 25 July 2006, “DoD Executive Agent for Information Technology Standards”
- f. CJCSM 6120.01 Series, “Joint Multi-Tactical Data Link (TDL) Operating Procedures (JMTOP)”
- g. CJCSI 3170.01 Series, “Joint Capabilities Integration and Development System (JMTCCB)”
- h. Department of Defense Chief Information Officer (DoD CIO), “Joint TDL Migration Plan (JTMP)”, 7 February 2014
- i. DoD 5200.1-R, 14 January 1997, “Information Security Program”
- j. Title 10, U.S.C., Chapter 131, “Planning and Coordination”
- k. Title 40, U.S.C., Subtitle III, “Information Technology Management”
- l. Title 44, U.S.C., Chapter 35, “Coordination of Federal Information Policy”

² DoDI 8330.xx, which is under development, will update policy and procedures for interoperability of IT and NSS and incorporate and cancel DoDD 4630.05 and DoDI 4630.8 (references a and b).

- m. DoD Directive 5144.02, 22 April 2013, “Department of Defense Chief Information Officer (DoD CIO)”
- n. DoD Information Technology Standards Registry
- o. DoD Directive 5134.01, 9 December 2005, “Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))”
- p. DoD Directive 5118.03, 20 April 2012, “Under Secretary of Defense (Comptroller) (USD(C)/Chief Financial Officer (CFO), Department of Defense”
- q. Interoperable Systems Management and Requirements Transformation (iSMART) Military Handbook (MIL-HDBK-524), 26 June 2012.
- r. Joint Interoperability Test Command, “Interoperability Process Guide Version 1.0,” 11 September 2012.
- s. JCIDS Manual, 19 January 2012, “Manual for the Operation of the Joint Capabilities Integration and Development System”

GLOSSARY

PART I-ABBREVIATIONS AND ACRONYMS

Items marked with an asterisk () have definitions in PART II*

APIS	Actual Platform Implementation Specification
C/S/A	Combatant Command/Service/agency
CCIB	Command and Control Interoperability Board
CCMD	Combatant Command
CI*	Configuration item
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CM*	Configuration management
CMF	Common Message Format
CoT	Cursor on Target
DAE	Defense Acquisition Executive
DISA*	Defense Information Systems Agency
DoD	Department of Defense
DSP	Defense Standardization Program
eSMART	Enhanced Systems Management and Requirements Transformation
IAW	In accordance with
IBS	Integrated Broadcast Service
ICTO*	interim certificate to operate
IEP	interoperability enhancement process
IMB	Interoperability Management Board
IOP*	interface operating procedure
iSMART	Interoperable Systems Management and Requirements Transformation
ISG	Interoperability Steering Group

IT	information technology
ITS*	information technology system
JCIDS	Joint Capabilities Integration Development System
JC&L	Joint Capabilities and Limitations
JINTACCS*	Joint Interoperability of Tactical Command and Control Systems
JITC*	Joint Interoperability Test Command
JMSWG*	Joint Multi-Tactical Data Link Standards Working Group
JMTCCB*	Joint Multi-Tactical Data Link Configuration Control Board
JREAP	Joint Range Extension Application Protocol
JTMP	Joint Tactical Data Link Migration Plan
MADL	Multifunction Advanced Data Link
MCEB	Military Communications-Electronics Board
MIDS	Multifunction Information Distribution System
MilOps	Military Operations
MIL-STD	military standard
MIP	Message Implementation Plan
NATO	North Atlantic Treaty Organization
NDD	National Difference Document
NIEM	National Information Exchange Model
NSS*	national security systems
PIDD	Platform Implementation Difference Document
PRDD	Platform Requirements Difference Document
PRS	Platform Requirements Specification
SDD	Service Difference Document
STANAG	standardization agreement
TDES	Tactical Data Enterprise Services
TDL*	tactical data link
TIDP-TE*	Technical Interface Design Plan Test Edition
U.S.	United States
VMF*	variable message format

PART II-DEFINITIONS

Configuration Item (CI) -- An aggregation of hardware and software that satisfies an end use function and is designated by the government for separate configuration management.

Configuration Management (CM) -- As applied to configuration items, a discipline applying technical and administrative direction and surveillance over the life cycle of items. The Joint Multi-Tactical Data Link Configuration Control Board uses this management process to develop and maintain joint tactical data link standards, interface operating procedures and associated documents and to establish U.S. positions regarding allied or NATO interoperability.

Defense Information Systems Agency (DISA) Enterprise Engineering Directorate (EE), Systems Engineering Division (EE2), Tactical Standards Branch (EE21), Tactical Data Link Standards Section (EE211) -- Functions as lead standardization activity and preparing activity for TDL standards.

Exception -- An exception is a permanent or temporary (shall not exceed four years, with no renewal) deviation of a system's TDL implementation from the required TDL standard implementation. Exceptions are approved by the JMTCCB. Systems granted an exception are subject to joint certification testing.

Interim Certificate To Operate (ICTO) -- ICTO represents the authority to field a new system or capability for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO will be made by the Interoperability Steering Group based on the sponsoring component's initial laboratory test results and assessed impact, if any, on the operational network to be employed.

Interface Operating Procedures (IOP) -- TDL IOPs are published in CJCSM 6120.01 and provide doctrine, tactics, techniques, and procedures designed for Combatant Commands, joint task force commanders, Services, and agencies in planning, designing, and operating TDL networks.

Interoperability -- 1. (DoD, NATO) The ability to operate in synergy in the execution of assigned tasks. 2. (DoD only) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. Source: JP-3-32.

Information Technology System (ITS) -- ITS includes any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Information technology does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

Joint Interoperability of Tactical Command and Control Systems (JINTACCS) -- The JINTACCS program is managed in accordance with this and other referenced instructions and includes TDLs and U.S. message text formats.

Joint Interoperability Test Command (JITC) -- DISA (JITC) is responsible for IT and NSS interoperability certification.

Joint Multi-TDL Standards Working Group (JMSWG) -- The JMSWG is the joint body chaired by DISA tasked with resolving joint and coalition interoperability issues affecting the JINTACCS TDL program.

Joint Multi-TDL Configuration Control Board (JMTCCB) -- The JMTCCB is a joint board chaired, funded, and coordinated by DISA and is responsible for configuration management of the JINTACCS TDL message standards.

National Security Systems (NSS) -- NSS include telecommunications and information systems operated by the Department of Defense, the functions, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Tactical Data Link (TDL) -- A means of connecting one platform to another for the purpose of transporting and receiving data with a DoD approved standardized communications link suitable for transmission of digital information. A TDL is characterized by its standardized message format, protocols, and transmission characteristics. A TDL supports near-real-time tactical data exchange between participants using a variety of formatted messages.

TDL Message Standards -- TDL message standards are a set of technical and procedural parameters with which systems/equipment must comply to achieve compatibility and interoperability with other systems/equipment. This includes the data communications protocol and data item implementation specification.

Technical Interface Design Plan Test Edition (TIDP-TE) -- Under the joint publication CM process, interim TDL standards are developed as TIDP-TEs to conduct developmental certification testing.

Variable Message Format (VMF) -- VMF is a message format designed to support the exchange of digital data between combat units with diverse needs for volume and detail of information using various communications media. VMF is a bit-oriented message standard with limited character-oriented fields. Message length can vary with each use based on the information content of the message. VMF is intended to be the basis of the U.S. Army's digitization transformation.

(INTENTIONALLY BLANK)