CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6610.01F
DISTRIBUTION: A, B, C 8 January 2021

TACTICAL DATA LINK STANDARDIZATION AND INTEROPERABILITY

Reference:
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 C.

2. Superseded/Cancellation. CJCSI 6610.01E, “Tactical Data Link Standardization Implementation Plan,” 10 April 2014 is superseded.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 strongly recommended for other Federal Departments implementing TDLs. The Joint Multi-Tactical Data Link Standards Working Group (JMSWG) Terms of Reference (reference b), the Joint Multi-Tactical Data Link Configuration Control Board (JMTCCB) Terms of Reference (reference c), and the Combat Net Radio Working Group (CNRWG) Terms of Reference (reference f) establish detailed TDL configuration management procedures not included in this instruction.

4. Policy. See Enclosure A.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Summary of Changes

a. Clarifies JS J6 role with Tactical Data Links Standardization and Interoperability.

b. Adds CNRWG responsibilities and relationship.

c. Adds CNRWG Terms of Reference to references.

d. Refines JMTCCB roles and responsibilities.

e. Refines JMSWG roles and responsibilities.

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.jcs.mil/library>. JS activities may also obtain access via the SIPR directives Electronic Library websites.

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

For the Chairman of the Joint Chiefs of Staff:

ANDREW P. POPPAS, LTG, USA
Director, Joint Staff

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

ENCLOSURE A

POLICY

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

2. Documentation. TDL message standards are defined in U.S. Military Standard (MIL-STD) documents and North Atlantic Treaty Organization (NATO) Allied Tactical Data Link Publications (ATDLP). Joint Multi-Tactical Data Link Operating Procedures are contained in reference d. For NATO, the equivalent document is ATDLP 7.33.

3. Certification. Joint Interoperability, Implementation Requirement Exceptions, Interim Certificate to Operate, National and Service Difference Documents, and Platform Implementation, Platform Requirements Specification, Platform Implementation Difference Document, Actual Platform Implementation Specifications, and Platform Bit-Level Implementation.

a. 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 J-6, 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.

b. 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 (RFEs) to implementation requirements. Normally, exceptions are approved in advance of IT and NSS joint interoperability certification. Exceptions granted may be permanent or temporary. A temporary RFE 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 Defense Information Systems Agency's (DISA) Joint Interoperability Test Command (JITC) and Joint Analysis Review Panels shall consider the approved requests for exceptions to requirements when making a determination on whether to certify TDL systems.

c. Interim Certificate to Operate. An Interim Certificate to Operate (ICTO), as outlined in reference r, approved by the ISG is temporary (may not exceed 1 year in duration). It 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.

d. National Difference Document. National Requirements Documentation define 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 a National Difference Document (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, ATDLP-5.16). However, an NDD is not always necessary; for some of the MIL-STDs, there may not be a corresponding, higher-level, multinational standard.

e. Service Difference Document. A Service Difference Document (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.

f. Message Implementation Plan. The Message Implementation Plan (MIP) defines a program 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.

(1) 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.

(2) 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.

(3) To support the requirement of reference g for TDL participants to provide the final MIP prior to Milestone C, while JS J-6 will review the MIP during the Joint Capabilities Integration Development System (JCIDS) process to conduct initial joint mission rea interoperability assessments.

g. Platform Requirements Specification. 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.

h. Platform Implementation Difference Document. Programs use the Platform Implementation Difference Document (PIDD) format to explain the implementation differences from the development baseline standard, which transitions 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 platform implementation testing completes, require documentation.

i. Actual Platform Implementation Specifications. Creation of the Actual Platform Implementation Specifications (APIS) follows 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. When identified problems receive correction, APIS can change. The APIS/PIDD support interoperability evaluations to identify capability gaps against functional requirements and interoperability assessments of data exchange between TDL capable platforms.

j. Platform Bit-Level Implementation. The TDL bit-level implementation contained in the APIS identifies the data item details—Data Field Identifiers and Data Use Identifiers—for transmission and reception. The deviations from the required implementation plan are detailed in the PRS/PRDD and implementation differences are 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.

k. Configuration Management

(1) The DISA Development and Business Center Innovations, Systems Engineering, and Architecture Office (BDE) Tactical Data Link Standards Branch (BDE3) is the U.S. custodian for applicable U.S. and NATO TDL documents. BDE3 is responsible for configuration management of TDL MIL-STDs (Enclosure C) and other associated documents. BDE3 is also the U.S. custodian for applicable U.S. and NATO TDL documents.

(2) The DoD Executive Agent for TDL Standards shall establish and execute the JMTCCB on an ongoing basis. The JMTCCB is the DoD's principle forum for the configuration management of the TDL-related standards identified in Enclosure B as well as for resolving interoperability issues related to TDL message standards format, structure, and development.

l. The JMTCCB is the forum for resolving interoperability issues related to TDL message standards format, structure, and development.

(1) The JMTCCB is the configuration management authority for TDL Military Standards (TDL MIL-STD), Multifunction Advanced Data Link (MADL), and Cursor on Target (CoT) MIL-STD, applicable NATO standardization agreement (STANAGs), Chairman of the Joint Chiefs of Staff (CJCS) Manual (CJCSM) 6120.01, and other associated U.S. and NATO TDL documents.

(2) Combatant Command/Service/Agency (C/S/A) Action Officer review of MIL-STDs, applicable NATO STANAGs, CJCSM 6120.01, and other associated U.S. and NATO TDL documents will be accomplished within the JMTCCB and/or the CNRWG, as appropriate.

(3) The CNRWG is the configuration management authority for the Header and Data Transfer Layer MIL-STDs generally associated with the Variable Message Format MIL-STD. The CNRWG is chaired by the U.S. Army.

(4) Recommended changes to the applicable TDL-related standards and operational procedures found in Enclosure B may be submitted to a cognizant JMTCCB or CNRWG principal representative at any time.

(5) Substantive TDL interoperability and standards issues that cannot be resolved at the JMSWG, JMTCCB, or CNRWG will be referred to the Military

Command, Control, Communications and Computers (C4) Executive Board (MC4EB) for resolution.

m. The JMSWG is the principal forum for the application of policy and discussion of doctrinal, operational, tactical, and procedural issues concerning the TDLs used in joint and combined operations. Tasked to advance TDL interoperability as it relates to TDL message standards format, structure, and development.

(1) DISA's Systems Engineering Division shall chair the JMSWG as an information technology standards working group tasked to achieve and maintain communication interoperability through the standardization of message protocols, format, content, implementation, and documentation.

(2) The JMSWG principal representatives consists of the JS J-6; Army; Marine Corps; Navy; Air Force; the National Security Agency/Air Force Intelligence Agency, Surveillance and Reconnaissance Agency; the Integrated Broadcast Service (IBS) Executive Agent; and DISA's JITC. JMSWG associate membership consists of the Navy's joint program office (PMW-101). In addition to its JS role, JS J-6 will represent the CCMDs and provide their vote during the JMSWG.

(3) The JMSWG and its subgroups are responsible for the development of joint operational procedures, network design, planning, and network management. The JMSWG develops policy recommendations on joint standards development, testing, classification issues, and U.S. and NATO configuration management.

(4) The JMSWG and its subgroups provide policy guidance to the U.S. Delegate to the NATO TDL Capability Team and its Syndicates.

(5) The JMSWG provides policy recommendations to the MC4EB for adjudication, and guidance to Command and Control Interoperability Boards (CCIB), Interoperability Management (IMB), CSG, etc., and other decision making bodies that impact U.S. TDL standards. 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 MC4EB for adjudication.

n. The CNRWG is the configuration management authority for the Header and Data Transfer Layer MIL-STDs generally associated with the Variable Message Format MIL-STD. Interoperability issues beyond the scope of the CNRWG will be referred to the JMSWG for resolution.

(1) The U.S. Army shall establish and execute the CNRWG on an ongoing basis. The CNRWG is the configuration management authority for MIL-STD-188-220 and MIL-STD-2045-47001, two of the principal header and bearer standards associated with Variable Message Format (VMF). Combat Net Radio interoperability issues exceeding the scope of the CNRWG charter will be referred to the JMSWG or MC4EB, as required for resolution.

(2) The CNRWG will conduct action officer review of the Header and Data Transfer Layer MIL-STDs generally associated with the Variable Message Format MIL-STD.

o. 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.

p. Joint Interoperability of Tactical Command and Control Systems Transformation. The C/S/As will continue building on DoD, JS, and Service/Agency initiatives to transform the Joint Interoperability of Tactical Command and Control Systems (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 adoption of the National Information Exchange Model (NIEM) will serve as the basis for a significant portion of its data exchange strategy, and may facilitate the ability to share information among multinational, interagency, and Service entities. DoD programs will consider and apply NIEM for XML-based message exchanges where it's application is determined to be useful and practical. DOD's strategy includes the Military Operations (MilOps) domain. The MilOps domain which provides shared data definitions, methods, and tools which may be used in multiple formats and standards.

ENCLOSURE B

RESPONSIBILITIES

1. The CJCS 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.

a. JS J-6 will provide guidance and direction as necessary ensure JMSWG, JMTCCB, and the CNRWG development, coordination, and review of joint TDL message standards, NATO STANAGs, and other associated documentation support DoD and CJCS priorities.

b. IAW references c and d, JS J-6 will represent the CCMDs at the JMSWG, JMTCCB, and CNRWG. In addition to its oversight role to these meetings, JS J-6 will provide the CCMDs vote during these meetings and will staff critical issues with the CCMDs in order to establish a coordinated position.

2. Military Command, Control, Communications and Computers Executive Board

a. IAW reference w, the MC4EB will provide resolution on substantive issues forwarded from the JMSWG, JMTCCB, or the CNRWG that have an adverse effect on TDL interoperability and other information exchange standards if unresolved.

b. When requested, provide clarification guidance and direction on joint and allied policies affecting TDL standards, and interoperability.

c. Provide to the JMSWG, JMTCCB, and CNRWG, as necessary, results of technical and operational risk assessments, and recommendations to support changes/updates to joint and allied TDL standards.

3. CCMD, Service, or DoD Agency

a. Each C/S/A will identify and provide representatives to participate in the JMSWG, JMTCCB, and CNRWG in support of the IT standards process.

(1) Representatives are responsible for providing their respective organization's position on all issues.

(2) Representatives will be empowered to commit their organization's assistance in matters requiring coordination. C/S/As that fail to participate will automatically abstain from any decision or vote that occurs.

b. Ensure TDL systems conform to joint TDL message standards.

c. Ensure that JCIDS documents identifying TDL systems (e.g., Information Support Plans) contain directives to implement joint TDL standards and/or STANAGs, as appropriate.

d. 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 b, c, and e.

e. Ensure fielding plans conform to approve joint TDL migration plans.

f. 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.

g. 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 processing and display functions.

(2) Capability developers who are implementing tactical data standards within their IT and NSS solutions will leverage the Interoperability Enhancement Progress (IEP). IEP is an effort, co-chaired by JS J-6 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.

4. CCMDs will:

a. Identify and provide required corrections and improvements to joint TDL message standards and interface operating procedures. In coordination with JS J-6, fully participate in the configuration management of these documents IAW references b, c, and 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 CCIB or IMB with coalition countries.

5. Directors of the National Security Agencyand 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 b, c, and e.

6. DISA is the executive agent for the JINTACCS program. Standards within the scope of JINTACCS including Link-11, Link-11B, Link-16, Link-22, VMF, Header and Transfer Layer Protocols, MADL, CoT, Joint Range Extension Applications Protocol (JREAP), IBS Common Message Format (CMF), and the applicable corresponding NATO TDL Standards. 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 TDLs, 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. Under the authority of the Joint Staff J-6, the JMSWG is responsible for development of U.S. TDL message standards and the focal point for resolving standards, implementation, and testing issues related to U.S. and coalition TDL interoperability IAW reference b.

e. Convene and chair the JMTCCB. Under the authority of the Joint Staff J-6, 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. Provide 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 official source for DoD specifications and standards distribution within the U.S. Distribution to coalition partners will be conducted in coordination with the CCMDs to access releasability and meet theater requirements.

j. Maintain Link 11 standards in caretaker status until the established sunset date of 2025, at which time Link 11 Standards will be remove from ASSIST and retired from the DoD Information Technology Standards Registry.

7. <u>DoD Responsibilities</u>. 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.

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

b. 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.

c. 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.

INTENTIONALLY BLANK

ENCLOSURE C

TDL STANDARDS PUBLICATIONS

TDL	Associated Publications
Link-11/11B	MIL-STD-6011 and STANAG 5511
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 (US MIL-STD under development)
TDL Data Forwarding	MIL-STD-6020
MADL	TIDP/TE In development
CoT	MIL-STD 6090 TIDP/TE In development
NATO QUALIFICATION LEVELS FOR TDL PERSONNEL	STANAG 5555 (no U.S. MIL-STD equivalent)
CNR	
VMF Header	MIL STD 2045-47001
VMF Transfer Layer	MIL STD 188-220

INTENTIONALLY BLANK

ENCLOSURE D

REFERENCES

a. DoDI 8330.01, 11 December 2019, “Interoperability of Information Technology (IT), Including National Security Systems (NSS)”

b. DISA BDE3, 5 April 2016, “Terms of Reference Joint Multi-Tactical Data Link Standards Working Group (JMSWG)”

c. DISA BDE3, 28 August 2018, “Terms of Reference for the Joint Multi-TDL Configuration Control Board (JMTCCB)”

d. CJCSM 6120.01 Series, “Joint Multi-Tactical Data Link (TDL) Operating Procedures (JMTOP)”

e. DoDD 5105.19, 25 July 2016, “DoD Executive Agent for Information Technology Standards"

f. Combat Net Radio Working Group (CNRWG) Terms of Reference, 30 September 2020

g. CJCSI 3170.01 Series, “Joint Capabilities Integration and Development System"

h. DoD CIO, 7 February 2014, “Joint TDL Migration Plan (JTMP)”

i. DoD 5200.1-R, January 1997, “Information Security Program”

j. Title 10, U.S. Code, Chapter 131, “Planning and Coordination”

k. Title 40, U.S. Code, Subtitle III, “Information Technology Management”

l. Title 44, U.S. Code, Chapter 35, “Coordination of Federal Information Policy”

m. DoDD 5144.02, 19 September 2017, “Department of Defense Chief Information Officer (DoD CIO)”

n. DoD Information Technology Standards Registry <https://gtg.csd.disa.mil/disr/standards/search/simple.html>

o. DoDD 5134.01, 25 September 2007, “Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L))”

p. DoDD 5118.03, 20 April 2012, incorporating Change 1 29 May 2020, "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 2.0 Change 1, 30 October 2018."

s. DoD CIO and JS J-6 memorandum, 1 April 2019, "Primary Sponsorship of the National Information Exchange Model"

t. DoDD 8500.01, 14 March 2014, incorporating Change 1 7 October 2019, "Information Assurance (IA), ASD (NII) DoD CIO, Department of Defense"

u. DoDD 8510.01, 28 July 2017, "Risk Management Framework (RMF) for DoD Information Technology (IT), DoD CIO, Department of Defense"

v. JCIDS Manual, 12 February 2015, "Manual for the Operation of the Joint Capabilities Integration and Development System"

w. CJCSI 5116.05 Series, "Military Command, Control, Communications, and Computers Executive Board (MC4EB)

GLOSSARY

PART I — ABBREVIATIONS AND ACRONYMS

APIS	Actual Platform Implementation Specification
ATDLP	Allied Tactical Data Link Publication
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
CMF	Common Message Format
CNR	Combat Net Radio
CNRWG	Combat Net Radio Working Group
CoT	Cursor on Target
CSG	Communication Steering Group
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
MC4EB	Military Command, Control, Communications, and Computers Executive Board (MC4EB)
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
VMF*	Variable Message Format

GLOSSARY

PART II – DEFINITIONS

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

Configuration Management. 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. Functions as lead standardization activity and preparing activity for TDL stands comprising of Enterprise Engineering Directorate (EE), Systems Engineering Division (EE2), Tactical Standards Branch (EE21), Tactical Data Link Standards Section (EE211).

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 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. 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 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. 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. DISA (JITC) is responsible for IT and NSS interoperability certification.

Joint Multi-TDL Standards Working Group. 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. 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 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. 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. Under the joint publication CM process, interim TDL standards are developed as TIDP-TEs to conduct developmental certification testing.

Variable Message Format. 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