CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6610.01D
DISTRIBUTION: A, B, C, JS-LAN, S 30 December 2010

TACTICAL DATA LINK STANDARDIZATION IMPLEMENTATION PLAN

References: Enclosure C

1. Purpose. 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. In accordance with (IAW) reference a, this instruction establishes procedures for the development, review, 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. Cancellation. CJCSI 6610.01C, 15 July 2006, is canceled.

3. Applicability. This instruction applies to the Joint Staff, combatant commands, Military Departments, and DOD agencies and activities. It is also recommended for other federal departments implementing TDLs. The Joint Multi-Tactical Data Link Configuration Control Board (JMTCCB) Terms of Reference (reference d), and Joint Multi-Tactical Data Link Standards Working Group (JMSWG) Terms of Reference (reference c) establish TDL configuration management procedures.

4. Policy. DOD IT and NSS implementing TDLs will comply with applicable TDL message standards (Enclosure B) and their associated documentation. 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 US military standards (MIL-STD) documents and North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAG). Joint Multi-Tactical Data Link Operating Procedures (JMTOP) are contained in reference f. For NATO, the equivalent document is Allied Data Publication 33 (ADatP-33).

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

(1) Joint Certification. IAW reference g, all IT and NSS that implement TDLs are considered for joint use. Joint certification is required prior to operating in joint or multinational arenas. The Military Communications-Electronics Board (MCEB) Interoperability Test Panel (ITP) will review systems that are placed in operation without joint certification for consideration and possible inclusion on the Interoperability Test Watch List (ITWL). Combatant commands will notify the ITP, through USJFCOM, 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 USJFCOM 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 testing. Exceptions are intended to be permanent 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 reference g. 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) Implementation Requirement Exceptions, Interim Certificate to Operate (ICTO). An ICTO, as outlined in reference g, is approved by the MCEB ITP. They are temporary (may not exceed one year in duration) and are approved only in exceptional cases where an IT and NSS is required to be used operationally prior to completion of a joint certification test. An ICTO does not waive the requirement to complete certification testing IAW reference g.

(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 a NDD or National Requirements Specification (NRS). 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 and 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. The 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) Platform Requirements Specification (PRS). The PRS consists of two parts, a Platform Requirements Difference Document (PRDD) and detailed TDL bit-level data (Data Field Identifier, Data Field Use, Data Item) implementation required by the platform. The PRDD documents the planned deviation from higher level requirements documents (i.e., deviations to requirements listed in a MIL-STD) and provides justification for the deviations. Deviations from a platform's TDL implementation requirements by function should be approved by the JMTCCB. The detailed TDL bit-level required implementation identifies the data (Data Field Identifier, Data Field Use, Data Item) transmission and reception required to be implemented by the platform. To support the requirement of reference g for TDL participants to provide the PRS prior to Milestone C, USJFCOM will review the PRS during the Joint Capabilities Integration Development System (JCIDS) process to conduct initial Joint Mission Area interoperability assessments.

(7) Actual Platform Implementation Specifications (APIS). The APIS consists of two parts, a Platform's Implementation Difference Document (PIDD) and a detailed TDL bit-level data (Data Field Identifier, Data Field Use, Data Item) implementation of the fielded platform. The PIDD's differences from a requirements specification (e.g., deviations to requirements listed in a PRS or in a MIL-STD). Each PIDD also contains the rationale defining the reason for the deviation and, if applicable, a work-around. The detailed TDL bit-level implementation identifies the data (Data Field Identifier, Data Field Use, Data Item) transmissions and receptions implemented by the platform. The APIS are

used for interoperability evaluations to identify capability gaps against functional requirements and interoperability assessments of data exchange between platforms.

c. Configuration Management. The Defense Information Systems Agency (DISA) Systems Engineering Center GE3, Interface Standards Division GE33 is responsible for configuration management of TDL MIL-STDs, reference f, and other associated documents. DISA is the US custodian for applicable US 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 MIL-STDs, applicable NATO STANAGs, CJCSM 6120.01, and other associated US and NATO TDL documents. Action officer review of these documents will be accomplished within the JMTCCB. Following JMTCCB review, updates to reference f will be provided to combatant commands, Services and Defense agencies (C/S/A) for concurrence or nonconcurrence only. This staffing procedure is established in order to maintain the rigor of the configuration management process. Recommended changes to reference f may be submitted to appropriate JMSWG and JMTCCB representatives, the Joint Staff Command, Control, Communications and Computer Systems, Information Transport Division (J-65A) or DISA at any time. Interoperability issues beyond the scope of the JMTCCB and JMSWG will be referred to the appropriate MCEB panel for resolution.

(2) Each C/S/A will participate in the information technology standards process. IAW references c and d, USJFCOM 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.

d. Migration Strategy. IAW the Joint Tactical Data Enterprise Services (TDES) 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.

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

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes.

a. Clarify that ADatP-33 is the NATO counterpart to CJCSM 6120.01, JMTOP.

b. Incorporate guidance on National Difference Documents, and the purposes of the APIS and PIDD.

c. Replace references to the Joint TDL Management Plan (JTDLMP) with the JTMP.

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

e. Interoperability Enhancement Process (IEP) is an effort, co-chaired by USJFCOM and DISA, that pursues bit-level interoperability and defines implementation documentation requirements.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--
http://www.dtic.mil/cjcs_directives.

9. Effective Date. This document is effective immediately.

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

Enclosures:
A – Responsibilities
B – TDL Standards Publications
C – References

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Office of the Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer	1
Office of the Under Secretary of Defense for Acquisition, Technology and Logistics	1
Office of the Secretary of Defense for Production and Logistics	1
National Defense University	1
Joint Forces Staff College	1
Headquarters Global Cyberspace Integration Center (GCIC)	1
Air Force Doctrine Center	1
Secretary of the Air Force, Warfighting Integration and Information Officer	1
Commander Joint Forces Command (USJFCOM),	1
Commander Forces Command (FORSCOM), Joint Interoperability Division	1
Chief of Naval Operations	1
Defense Information Systems Agency	1
Defense Information Systems Agency Joint Interoperability Test Command	1
Joint Doctrine Center	1
Joint Spectrum Center	1
Industrial College of the Armed Forces	1
Joint Command and Control Warfare Center	1
Joint Warfighting Center	1

Military Communications – Electronics Board	1
National War College	1
U.S. Forces Japan	1
U.S. Forces Korea	1
Space and Naval Warfare Systems Center Pacific	1
Naval Network Warfare Command	1
U.S. Army Communications and Electronics Command	1
U.S. Army Missile Command (AMCOM)	1
USMC Tactical Systems Support Activity	1
Missile Defense Agency	1

ENCLOSURE A

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. Combatant commands, Services, and DOD agencies (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 Information Technology (IT) and NSS compliance deficiency, report this deficiency, as appropriate, to USJFCOM, the Joint Staff, Service Chief Information Officer (CIO) or DOD CIO for corrective action.

f. The C/S/As will continue building on DOD, OASD, Joint Staff, and Service/agency initiatives to transform the JINTACCS program. 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. Capability developers who are implementing tactical data standards within their IT and NSS solutions, are encouraged to leverage the USJFCOM and DISA led Interoperability Enhancement Process (IEP). 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. 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 Department of Defense Instruction (DODI) 4120.25, Defense Standardization Program (DSP), and DODI 4120.24-M, DSP Policies and Procedures.

3. Combatant commands will:

a. Identify and provide required corrections and improvements to joint TDL message standards and interface operating procedures. In coordination with USJFCOM, 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 p 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 Joint Interoperability of Tactical Command and Control Systems program including Link-11, Link-11B, Link-16, Link-22, Variable Message Format (VMF), 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 (LSA) and Preparing Activity (PA) for 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 US TDL message standards and the focal point for resolving standards issues related to U.S. and coalition TDL interoperability.

e. Convene and chair the JMTCCB. The JMTCCB approves all changes to US TDL message standards and associated documentation IAW reference d, and establishes US 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 US Representative during applicable combatant command C2 CCIB or IMB to advocate TDL standardization with coalition countries.

6. DOD Responsibilities

a. The DOD CIO (responsibilities outlined in references j through l) will review Service compliance with TDL interoperability policies established by this instruction and references a through q (including reference m DOD Information Technology Standards Registry (DISR)). Based on this review and evaluation, the DOD CIO will make recommendations to the Defense Acquisition Executive (DAE) (reference n) regarding program funding.

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

c. The DAE may direct the DOD Chief Financial Officer (reference o) 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 (OASD), Production and Logistics, Economic Security Division will manage and produce MIL-STDs and military bulletins (MIL-BUL) for the TDL program.

e. The Defense Printing Service is responsible for printing and distributing TDL CJCSIs, CJCSMs, MIL-STDs, and MIL-BULs.

ENCLOSURE B

TDL STANDARDS PUBLICATIONS

TDL	Associated Publications
Link-11/11B	MIL-STD-6011
Link-16	MIL-STD-6016
Link 16 terminal (MIDS)	STANAG 4175 (no US MIL-STD equivalent)
VMF	MIL-STD-6017
IBS CMF	TIDP/MIL-STD-6018
JRE	MIL-STD-3011
Link-22	STANAG 5522 (no US MIL-STD equivalent)
TDL Data Forwarding	MIL-STD-6020

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

a. DOD Directive 4630.05, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

b. DOD Instruction 4630.8, 30 June 2004, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

c. Defense Information Systems Agency, 25 January 2002 "Center for Standards, Joint Multi-Tactical Data Link Standards Working Group (JMSWG) Terms of Reference"

d. Defense Information Systems Agency, Standards Management Branch (GE332), "Terms of Reference for the Joint Multi-TDL Configuration Control Board"

e. DOD Directive 5101.7, 21 July 2004, "DOD Executive Agent for Information Technology Standards"

f. CJCSM 6120.01 Series "Joint Multi-Tactical Data Link (TDL) Operating Procedures (JMTOP)"

g. CJCSI 6212.01 Series, "Interoperability and Supportability of Information Technology and National Security Systems"

h. Office of the Assistant Secretary of Defense, Networks and Information Integration/Department of Defense Chief Information Officer (OASD(NII))/DoD CIO), "Joint Tactical Data Enterprise Services Migration Plan (JTMP)," dated October 31, 2008

i. DOD 5200.1-R, January 1997, "Information Security Program"

j. Title 10, USC, Chapter 131, "Planning and Coordination"

k. Title 40, USC, Subtitle III, "Information Technology Management"

l. Title 44, USC, Chapter 35, "Coordination of Federal Information Policy"

m. DOD Directive 5144.1, 2 May 2005, "Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD(NII)/DOD CIO)"

n. DOD Information Technology Standards Registry (DISR)

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, 6 January 1997, "Under Secretary of Defense (Comptroller) (USD(C))/Chief Financial Officer (CFO), Department of Defense"

q. Global Information Grid (GIG) Capstone Requirements Document (CRD), 4 March 2003, JROCM 134-01

r. DOD Directive 8320.02, December 2, 2004, "Data sharing in a Net-Centric Department of Defense"

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
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
DAE	Defense Acquisition Executive
DISA*	Defense Information Systems Agency
DISR	DOD Information Technology Standards Registry
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
IT	information technology
ITP	Interoperability Test Panel

ITS*	information technology system
ITWL	interoperability Test Watch list
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
JRE	Joint Range Extension
JTDLMP	Joint Tactical Data Link Management Plan
JTMP	Joint Tactical Data Enterprise Services Migration Plan
LSA	lead standardization activity
MCEB	Military Communications-Electronics Board
MIDS	Multifunction Information Distribution System
MIL-BUL	military bulletin
MIL-STD	military standard
NATO	North Atlantic Treaty Organization
NRS	National Requirements Specification
NSS*	national security systems
NDD	National Difference Document
OASD	Office of the Assistant Secretary of Defense
PA	preparing activity
PIDD	Platform Implementation Difference Document
PRDD	Platform Requirements Difference Document
PRS	Platform Requirements Specification
SDD	Service difference document
STANAG	standardization agreement
TDES	Joint Tactical Data Enterprise Services
TDL*	tactical data link
TIDP-TE*	Technical Interface Design Plan Test Edition

USJFCOM	US Joint Forces Command
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 US positions regarding allied or NATO interoperability.

Defense Information Systems Agency (DISA) Systems Engineering Center GE3, Interface Standards Division GE33 -- Functions as lead standardization activity and preparing activity for TDL standards.

Exception -- An exception is the permanent 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.

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.

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 Military Communications-Electronics Board Interoperability Test Panel 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.

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 US 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).

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.

Tactical Data Link (TDL) -- A TDL is a standardized communications link suitable for transmission and receipt of tactical digital information. TDLs interface two or more command and control or weapons systems via single network architecture and multiple communication media. Current practice is to characterize a TDL by its standardized message formats and transmission characteristics.

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 US Army's digitization transformation.