NOT MEASUREMENT SENSITIVE

MIL-STD-2045-47001C
22 March 2002
SUPERSEDING
MIL-STD-2045-47001B
20 January 1998
MIL-STD-2045-47001A
31 December 1997
MIL-STD-2045-47001
27 July 1995

DEPARTMENT OF DEFENSE INTERFACE STANDARD

CONNECTIONLESS DATA TRANSFER APPLICATION LAYER STANDARD

AMSC N/A

AREA DCPS

FOREWORD

This military standard is approved for use by all Departments and Agencies of the Department of Defense (DoD).

This military standard is produced by the Information Transfer Management Panel (IXMP). The MIL-STD-2045 document series was established within the Data Communication Protocol Standards (DCPS) Standardization Area to allow for the enhancement of commercial standards or the development of standards that are unique to DoD.

Specific details and instructions for establishing a MIL-STD-2045 document, as well as profile development guidelines, are documented in the IXMP Management Plan. IXMP Working Groups (WGs) are responsible for standard development, formal service and agency coordination, and approval.

This military standard does not supersede the scope of Allied Communication Publication (ACP) 123 with US SUPP-1. ACP 123 with US SUPP-1 addresses message handling communications protocol and procedures for the exchange of military messages.

The Preparing Activity (PA) for this standard is USACECOM, ATTN: AMSEL-SE-CD (Mr. R. Menell), Fort Monmouth, NJ 07703. The custodians for the document are identified in the Defense Standardization Program, "Standardization Directory (SD-1)" under Standardization Area DCPS.

Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this military standard should be addressed to the PA at the above address by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

TABLES

FIGURES

1 SCOPE

1.1 Purpose.

This military standard presents the minimum essential technical parameters in the form of a mandatory system standard and optional design objectives for interoperability and compatibility among digital message transfer devices (DMTDs), between DMTDs and applicable command, control, communications, computers, and intelligence (C4I) systems and among C4I systems using digital data for information transfer over limited bandwidth communication channels.

1.2 Scope.

This military standard addresses part of the communications protocol and procedures for the exchange of digital data among DMTDs, between DMTDs and C4I systems, and among C4I systems participating in inter- and intra-Service tactical networks. The material is presented in the context of the Open Systems Interconnection (OSI), as documented in national and international standards.

1.3 Application guidance.

This military standard applies to the design, construction, and development of new equipment and systems, and to the retrofit of existing equipment and systems.

1.4 System standards and design.

The parameters and other requirements specified in this military standard are mandatory if the word *shall* is used in connection with the parameter value or requirement under consideration. Non-mandatory objectives are indicated in parentheses after a standardized parameter value or by the word *should* in connection with the parameter value or requirement under consideration.

2 APPLICABLE DOCUMENTS

2.1 General.

The documents listed in this section are specified in sections 3, 4, and 5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they will meet all specified requirements documents cited in sections 3, 4, and 5 of this standard, whether or not they are listed.

2.2 Government documents.

2.3 Specifications, standards, and handbooks.

The following specifications, standards, and handbooks form a part of this military standard to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the current issue of the DoD Index of Specifications and Standards (DoDISS) and supplements thereto, cited in the solicitation (see 6.2).

STANDARDS:

FEDERAL:

FED-STD-1037	*Glossary of Telecommunication Terms*
FIPS 180-1	*Secure Hash Standard (SHS)*
FIPS 186-2	*Digital Signature Standard (DSS)*
FIPS 10-4	*Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions*

MILITARY:

MIL-STD-188-220	*DoD Interface Standard, Digital Message Transfer Device Subsystems*
Joint Pub (JP) 1-02	*DoD Dictionary of Military and Associated Terms*

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE:

DOI-103	*Defense Special Security Communications System (DSSCS) Operating Instructions System - Data Procedures DOI-103*

[Unless otherwise indicated, copies of federal and military standards are available from the Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094.]

2.3.1 Other Government documents, drawings, and publications.

The following other Government documents, drawings, and publications form a part of this military standard to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

VMF TIDP-TE	*DoD Interface Standard, Variable Message Format Technical Interface Design Plan-Test Edition*
MIL-STD-6016	*DoD Interface Standard, Tactical Digital Information Link (TADIL) J Message Standard*
MIL-STD-6040	*United States Message Text Format (USMTF)*

[Director, Defense Information System Agency (DISA), Interoperability Directorate, ATTN: IN51, 5600 Columbia Pike, Falls Church, VA 22041-2717.]

Approved Standard Change Catalog (SCC) modifications to this document form a part of the document as of the SCC approval date. Approved SCCs are posted to the "Documents" section of the CNRWG web page, http://www-cnrwg.itsi.disa.mil.

2.4 Non-Government publications.

The following documents form a part of this military standard to the extent specified herein. Unless otherwise specified, the issues of the documents that are DoD- adopted are those listed in the issue of the DoDISS cited in the solicitation. Unless otherwise specified, the issues of documents not listed in the DoDISS are the issues of the documents cited in the solicitation (see 6.2).

INTERNATIONAL ORGANIZATION for STANDARDIZATION (ISO):

ISO 7498-1	*Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model.*

[ISO standards are available from the American National Standards Institute (ANSI), Inc., 1430 Broadway, New York, NY 10018.]

OTHER:

Lempel-Ziv-Welch	*"A technique for high performance data compression"*, Terry A. Welch, IEEE Computer, Vol. 17, No. 6, pp. 8-19, June 1984
Lempel-Ziv 1977	*"A universal algorithm for sequential data compression"*, J. Ziv and A. Lempel, IEEE Transactions on Information Theory, Vol IT-23, No. 3, pp 337-343, May 1977.
RFC 1951	*"DEFLATE Compressed Data Format Specification version 1.3"*, L. Peter Deutsch, May 1996.
RFC 1952	*"GZIP file format specification, version 4.3"*, L. Peter Deutsch, May 1996.

2.5 Order of precedence.

In the event of a conflict between the text of this military standard and the references cited herein, the text of this military standard takes precedence. Nothing in this MIL-STD, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3 DEFINITIONS

3.1 Definitions of terms.

Definitions of terms used in this military standard are specified in FED-STD-1037.

3.2 Abbreviations and acronyms.

Abbreviations and acronyms used in this military standard are defined below. In addition, those listed in the current edition of FED-STD-1037 that are pertinent to standards referenced by this document have been included for the convenience of the reader.

ACP	Allied Communication Publication
ALP	Application Layer Protocol
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
C	Conditional
C4I	Command, Control, Communications, Computers, and Intelligence
CANTCO	Cannot Comply
CANTPRO	Cannot Process
CAT	Category
CNR	Combat Network Radio
DARPA	Defense Advanced Research Projects Agency
DCPS	Data Communication Protocol Standards
DISA	Defense Information Systems Agency
DMTD	Digital Message Transfer Device
DoD	Department of Defense
DoDISS	Department of Defense Index of Specifications and Standards
DOI	DSSCS Operating Instruction
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DSSCS	Defense Special Security Communications System
DTG	Date-Time Group
FAD	Functional Area Designator
FED-STD	Federal Standard
FIPS	Federal Information Processing Standard
FPI	Field Presence Indicator
FRI	Field Recurrence Indicator
GPI	Group Presence Indicator
GRI	Group Recurrence Indicator
HAVCO	Have Complied
HLEN	Header Length
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
ISO	International Organization for Standardization
IXMP	Information Transfer Management Panel
LRA	Least Recently Active

LSB	Least Significant Bit
LZ	Lempel-Ziv
LZW	Lempel-Ziv-Welch
M	Mandatory
MIL-STD	Military Standard
MR	Machine Receipt
MSB	Most Significant Bit
MSS	Maximum Segment Size
NA	Not Applicable
NCA	National Command Authority
ND	Not Determined
NITFS	National Imagery Transmission Format System
OPRACK	Operator Acknowledge
OSI	Open Systems Interconnection
P/F	Poll/Final
PA	Preparing Activity
PDU	Protocol Data Unit
QOS	Quality Of Service
R/C	Receipt/Compliance
S/R	Segmentation/Reassembly
SD-1	Standardization Directory
SHA-1	Secure Hash Algorithm
SHS	Secure Hash Standard
SPI	Security Parameters Information
TADIL	Tactical Digital Information Link
TBD	To Be Determined
TCP	Transmission Control Protocol
TE	Test Edition
TIDP-TE	Technical Interface Design Plan-Test Edition
UDP	User Datagram Protocol
UMF	User Message Format
URN	Unit Reference Number
USMTF	United States Message Text Format
VMF	Variable Message Format
WG	Working Group
WILCO	Will Comply
XML	eXtensible Markup Language
XOR	Exclusive OR

4 GENERAL REQUIREMENTS

4.1 Application layer users.

In the context of this MIL-STD, the user of the application layer is the application process that requires the communications services to effect information exchange (the transfer of digital data) between end systems.

4.2 Interoperability.

Interoperability of the application entity between end systems shall be achieved by implementing the application layer protocol (ALP) specified in this MIL-STD. This standard defines the minimum essential data communications parameters and protocol conventions that are necessary to support the handling and exchange of single messages or concatenated messages [a series of messages that are combined together in a single user data block for delivery to the same destination(s)] over subnetworks and point-to-point links.

4.3 Application-layer services provided.

The ALP shall provide the following services to the application process in order to facilitate the reliable exchange and distribution of messages of data between end user systems:

a. identification of intended communications partners by name;

b. identification of privacy/security mechanisms required;

c. passing of quality-of-service parameters (performance and non-performance parameters);

d. synchronization of cooperating application processes;

e. message handling (distribution, receipting, and monitoring);

f. identification of constraints on data syntax (character sets, data structure);

g. message or data transfer via connectionless operation; and

h. optional security services.

5 SPECIFIC REQUIREMENTS

5.1 Application layer.

The application layer shall provide the simplified message-handling protocol.

5.2 Application protocol data unit (PDU).

The application PDU shall be composed of an application header and user data, as shown in Figure 1.

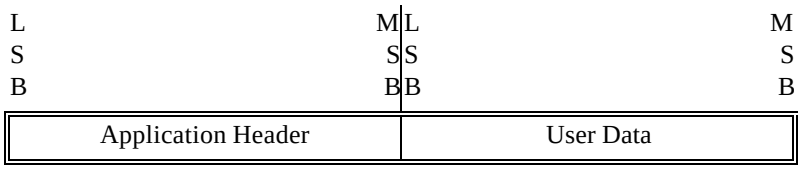

Figure 1. Application PDU structure

5.3 Application header.

The application header shall consist of the fields shown in TABLE I. The application header may contain two categories of fields, mandatory (M) and conditional (C). A conditional field is dependent upon the presence or absence of other fields. The order of fields shall follow that shown in TABLE I. The application header shall always be a multiple of 8 bits. If an application header is not a multiple of 8 bits, it shall be zero-filled so that it becomes a multiple of 8 bits.

TABLE I. Application header

Field Name	CAT	Group Code	Repeat Code	Description/ Resolution	Maximum Field Size (bits)
VERSION	M			MIL-STD-2045-47001 VERSION NUMBER	4
FPI	M			COMPRESSION TYPE	1
DATA COMPRESSION TYPE					2
GPI	M			ORIGINATOR ADDRESS GROUP	1
FPI		G1			1
URN		G1			24
FPI		G1			1
UNIT NAME		G1			448

TABLE I. Application header (Continued)

Field Name	CAT	Group Code	Repeat Code	Description/ Resolution	Maximum Field Size (bits)
GPI	M			RECIPIENT ADDRESS GROUP (See 5.6.3a)	1
GRI		G2	R1(N) 0<N<=16		1
FPI		G2	R1		1
URN		G2	R1		24
FPI		G2	R1		1
UNIT NAME		G2	R1		448
GPI	M			INFORMATION ADDRESS GROUP (See 5.6.3a)	1
GRI		G3	R2(16 - N)		1
FPI		G3	R2		1
URN		G3	R2		24
FPI		G3	R2		1
UNIT NAME		G3	R2		448
FPI	M				1
HEADER SIZE					16
GRI	M		R3(16)	MESSAGE HANDLING GROUP	1
UMF	M		R3		4
FPI	M		R3		1
MESSAGE STANDARD VERSION			R3		4
GPI	M		R3	MESSAGE IDENTIFICATION GROUP	1
FAD		G4	R3		4
MESSAGE NUMBER		G4	R3		7
FPI		G4	R3		1
MESSAGE SUBTYPE		G4	R3		7
FPI	M		R3		1
FILE NAME			R3		448
FPI	M		R3		1
MESSAGE SIZE			R3		20

TABLE I. Application header (Continued)

Field Name	CAT	Group Code	Repeat Code	Description/ Resolution	Maximum Field Size (bits)
OPERATION INDICATOR	M		R3		2
RETRANSMIT INDICATOR	M		R3		1
MESSAGE PRECEDENCE CODE	M		R3		3
SECURITY CLASSIFICATION	M		R3		2
FPI	M		R3		1
CONTROL/RELEASE MARKING			R3		224
GPI	M		R3	ORIGINATOR DTG	1
YEAR		G5	R3		7
MONTH		G5	R3		4
DAY		G5	R3		5
HOUR		G5	R3		5
MINUTE		G5	R3		6
SECOND		G5	R3		6
FPI		G5	R3	DTG EXTENSION	1
DTG EXTENSION		G5	R3		12
GPI	M		R3	PERISHABILITY DTG	1
YEAR		G6	R3		7
MONTH		G6	R3		4
DAY		G6	R3		5
HOUR		G6	R3		5
MINUTE		G6	R3		6
SECOND		G6	R3		6
GPI	M		R3	ACKNOWLEDGMENT REQUEST GROUP	1
MACHINE ACKNOWLEDGE REQUEST INDICATOR		G7	R3		1
OPERATOR ACKNOWLEDGE REQUEST INDICATOR		G7	R3		1
OPERATOR REPLY REQUEST INDICATOR		G7	R3		1
GPI	M		R3	RESPONSE DATA GROUP	1

TABLE I. Application header (Continued)

Field Name	CAT	Group Code	Repeat Code	Description/ Resolution	Maximum Field Size (bits)
YEAR		G8	R3	DTG OF MESSAGE BEING ACKNOWLEDGED	7
MONTH		G8	R3		4
DAY		G8	R3		5
HOUR		G8	R3		5
MINUTE		G8	R3		6
SECOND		G8	R3		6
FPI		G8	R3	DTG EXTENSION	1
DTG EXTENSION		G8	R3		12
R/C		G8	R3	RESPONSE TO ACKNOWLEDGE REQUEST	3
FPI		G8	R3		1
CANTCO REASON CODE		G8	R3		3
FPI		G8	R3		1
CANTPRO REASON CODE		G8	R3		6
FPI		G8	R3		1
REPLY AMPLIFICATION		G8	R3		350
GPI	M		R3	REFERENCE MESSAGE DATA GROUP	1
GRI		G9	R3/R4(4)		1
FPI		G9	R3/R4		1
URN		G9	R3/R4		24
FPI		G9	R3/R4		1
UNIT NAME		G9	R3/R4		448
YEAR		G9	R3/R4		7
MONTH		G9	R3/R4		4
DAY		G9	R3/R4		5
HOUR		G9	R3/R4		5
MINUTE		G9	R3/R4		6
SECOND		G9	R3/R4		6

TABLE I. Application header (Continued)

Field Name	CAT	Group Code	Repeat Code	Description/ Resolution	Maximum Field Size (bits)
FPI		G9	R3/R4	DTG EXTENSION	1
DTG EXTENSION		G9	R3/R4		12
GPI	M		R3	MESSAGE SECURITY GROUP	1
SECURITY PARAMETERS INFORMATION		G10	R3		4
GPI		G10	R3	KEYING MATERIAL GROUP	1
KEYING MATERIAL ID LENGTH		G10/G11	R3		3
KEYING MATERIAL ID		G10/G11	R3		64
GPI		G10	R3	CRYPTOGRAPHIC INITIALIZATION GROUP	1
CRYPTOGRAPHIC INITIALIZATION LENGTH		G10/G12	R3		4
CRYPTOGRAPHIC INITIALIZATION		G10/G12	R3		1024
GPI		G10	R3	KEY TOKEN GROUP	1
KEY TOKEN LENGTH		G10/G13	R3		8
FRI		G10/G13	R3/R5(N) 0<=N<=17		1
KEY TOKEN		G10/G13	R3/R5		16384
GPI		G10	R3	AUTHENTICATION (A) GROUP	1
AUTHENTICATION DATA (A) LENGTH		G10/G14	R3		7
AUTHENTICATION DATA (A)		G10/G14	R3	DIGITAL SIGNATURE	8192
GPI		G10	R3	AUTHENTICATION (B) GROUP	1
AUTHENTICATION DATA (B) LENGTH		G10/G15	R3		7
AUTHENTICATION DATA (B)		G10/G15	R3	DIGITAL SIGNATURE	8192
SIGNED ACKNOWLEDGE REQUEST INDICATOR		G10	R3		1
GPI		G10	R3	MESSAGE SECURITY PADDING GROUP	1
MESSAGE SECURITY PADDING LENGTH		G10/G16	R3		8
FPI		G10/G16	R3		1

TABLE I. Application header (Continued)

Field Name	CAT	Group Code	Repeat Code	Description/ Resolution	Maximum Field Size (bits)
MESSAGE SECURITY PADDING		G10/G16	R3		2040

5.4 Application header formatting.

The application header shall use a variable format syntax and format structure. The syntax and formatting procedures are defined below.

5.5 Syntax.

The application header consists of an ordered collection of bits (ones and zeros). A group is a combination of two or more related fields designated as a group. There are two types of groups, “G” groups and “R” groups. A “G” group is a combination of related fields. An “R” group is a repeatable combination of related fields. Presence and recurrence indicators as defined below shall be allowed in groups. The following syntax fields shall be used in the selection of fields to be transmitted:

a. Field Presence Indicators (FPIs). An FPI is a one-bit field used to indicate the presence or absence of the following field.

b. Field Recurrence Indicators (FRIs). An FRI is a one-bit field used to indicate the repeatability of a field.

c. Group Presence Indicators (GPIs). A GPI is a one-bit field used to indicate the presence or absence of the following group.

d. Group Recurrence Indicators (GRIs). A GRI is a one-bit field used to indicate the repeatability of a group.

5.5.1 Field presence indicator (FPI).

The FPIs are used to indicate the presence (FPI=1) or absence (FPI=0) of the following field and are not used for mandatory fields or single bit fields. These indicators are transparent to the user, allowing the user to send only those fields containing information when use of those fields is not mandatory.

5.5.2 Field recurrence indicator (FRI).

Fields may be designated as repeatable through a 1-bit FRI. If a field is preceded by an FPI, FPI=1 shall precede the first occurrence of the FRI and is not present for following repetitions. If the FPI=0, neither the FRI nor the field is present in the application header. An FRI=1 indicates the recurrence of the field after this iteration. An FRI=0 indicates the field will not occur after this iteration.

5.5.3 Group presence indicator (GPI).

A group is a combination of related fields. FPIs, FRIs, GPIs, and GRIs shall be allowed in groups. If a group is preceded by a GPI, then the GPI indicates the presence (GPI=1) or absence (GPI=0) of the group.

5.5.4 Group recurrence indicator (GRI).

An "R" group is repeatable and shall be preceded by a GRI. A "G" group is not repeatable and shall not be preceded by a GRI. If an "R" group is preceded by a GPI, GPI=1 shall precede the first occurrence of the GRI and is not present for following repetitions. If the GPI=0, neither the GRI nor the group is present in the application header. A GRI=1 indicates the recurrence of the group after this iteration. A GRI=0 indicates the group will not occur after this iteration.

5.5.5 End-of-literal field marker.

The end-of-literal field marker, a 7-bit ANSI ASCII DELETE character (1111111), is used to indicate the end of free-text, character-oriented, literal fields only. The maximum literal field size is specified for each such field in TABLE I. Either the end-of-literal field marker or the field maximum length shall signify the end of a text field. The application header processing software shall be capable of recognizing both conditions.

5.5.6 Data-field construction procedures.

The following construction procedures prescribe the sequence in which the application header fields are linearly joined before passing data to the next lower protocol layer. The header is constructed with elemental data fields ordered as specified in this standard. The data elements for the application header are as specified in this standard. There are two representations for data elements: 7-bit ANSI ASCII characters and binary numbers. All fields shall be joined least significant bit (LSB) first. The LSB of the first data field or field/group indicator shall be LSB-justified within the first byte of the message buffer. The LSB of each successive data field shall be concatenated to the most significant bit (MSB) of the preceding data field. The characters in a literal field are joined such that the LSB of the first character immediately follows the MSB of the previous field. The LSB of the second character immediately follows the MSB of the first character. This pattern is repeated until all characters of the field are joined. Figure 2 uses the first few fields of the application header (from TABLE I) as an example of the data field bit order. An example of a complete application header is provided in Appendix B. Bit No. 1 of Figure 2 maps to the LSB of the application header shown in Figure 1. Figure 2 is interpreted as follows:

BIT NO.	FIELD NAME	VALUE/CODE	MEANING
1 - 4	Version	1	MIL-STD-2045-47001B
5	FPI for Data Compression	0	NOT PRESENT
6	GPI for Originator Address Group	0	NOT PRESENT
7	GPI for Recipient Address Group	0	NOT PRESENT
8	GPI for Information Address Group	0	NOT PRESENT
9	GRI for Message Handling Group	0	NOT REPEATABLE
10 - 13	UMF	2	VMF K-Series
14	GPI for Message Identification Group	1	PRESENT
15 - 18	FAD	7	COMBAT SERVICE SUPPORT

	OCTET 1								OCTET 2									
	2^0	----	----	----	----	----	----	2^7	2^0	----	----	----	----	----	----	2^7	2^0	2^1
	LSB			MSB						LSB			MSB		LSB			MSB
FIELD	VERSION				FPI	GPI	GPI	GPI	GRI	UMF				GPI	FAD			
VALUE	1	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0

Figure 2. Application protocol data field bit order (example)

5.5.6.1 ASCII data element.

In a data element composed of a string of 7-bit ANSI ASCII characters, the left most character shall be stored in memory first.

5.5.6.2 Binary data element.

In a data element composed of a binary code, it shall be stored as a single data field.

5.5.6.3 Header format notations.

The header format is depicted in TABLE I; the notations used to describe the header format are as follows:

a. Category will display an “M” for those fields that are mandatory. All other fields are conditional.

b. Group Code The group codes in TABLE I represent a logical grouping of information that is implemented as a “G” group. “G” groups within a header will be notated as GN were N indicates that numbered grouping (i.e., G1 indicates the first “G” group within the header: etc.). Nested groups are indicated by “GN/GN” notation where the left-most group is the highest level of the nesting and the right-most group is the current, lowest level.

c. Repeat codes. The repeat codes in TABLE I denote group appearance, nesting of groups, and maximum repetitions. The following notations are used:

(1) R = Indicates this field is repeatable.

(2) RN = Indicates this field is part of a group that can be repeated, with N specifying the group number (that is, R1 indicates the first repeatable group in the message).

(3) (N) = Appears with the first field of a repeatable group, that is, R3(16), and indicates the maximum number of appearances of the group in the message. The example, R3(16), indicates the third repeatable group of the message that can appear a maximum of sixteen times.

(4) RN/RN = Nested repeating groups. Example R3/R4 R4 is nested in R3.

5.6 Application header fields.

5.6.1 Version.

This field shall be a 4-bit binary codeword representing the version of the MIL-STD-2045-47001 header being used for the message. TABLE II lists the MIL-STD-2045-47001 revision indicated by the Version code. The version code 15 shall be used in a response to indicate that the receiving system does not implement the MIL-STD-2045-47001 version originally sent. Only the Version field, data compression type FPI, originator address group and destination address group shall be required in this case.

TABLE II Version codes

Code MSB - LSB	**MIL-STD-47001 Revision**
0000 (0)	MIL-STD-2045-47001
0001 (1)	MIL-STD-2045-47001B
0010 (2)	MIL-STD-2045-47001C
0011-1110 (3-14)	Undefined
1111 (15)	Version Sent Not Implemented

5.6.2 Data compression type.

The absence of this field signifies data compression is not used. When present, this field shall be a 2-bit binary codeword representing whether the message or messages contained in the User Data portion of the Application PDU have been Unix compressed (LZW algorithm) or compressed using the gzip (LZ-77 algorithm) compression algorithm. TABLE III lists the Data Compression algorithm indicated by the Data Compression Type. When any type of optional data compression is indicated and multiple messages are present in the User Data portion of the Application PDU, all messages shall be compressed and each message shall be compressed independently of the other messages.

TABLE III. Data compression type codes

Code MSB-LSB	Compression Algorithm	Reference
00 (0)	LZW	Lempel-Ziv-Welch Compression Algorithm, Welch 1984
01 (1)	LZ-77	RFC 1951 and RFC 1952 (Lempel-Ziv Compression Algorithm, Lempel-Ziv 1977)
10-11 (2-3)	Undefined	

5.6.3 Originator, recipient, and information addressee fields.

These fields shall contain addresses that represent the names of the originating and receiving person(s) or process(es). The receiving application layer shall use the recipient and information fields to determine how the message shall be handled or delivered after the decoding process. The value in these fields depends on the person or process receiving the message. If a person is to be designated, the fields shall uniquely identify the individual so that the message may be routed to a specific mailbox or terminal. If a process is to be designated, these fields shall uniquely identify the process. The process shall be associated with an end system to define the address uniquely. The following requirements apply to recipient and information addressee fields:

a. The recipient and information addressee fields shall be extendible to a combined total of 16 addressees.

b. When the recipient address is not present (GPI = 0) and the information address group is not present (GPI = 0), the message shall be broadcast in accordance with lower layer broadcast rules.

5.6.3.1 Unit reference number (URN) field.

This field shall be a 24-bit binary code used by individuals, units and broadcast and multicast groups on an interface to uniquely identify friendly military entities. A URN that identifies a broadcast would be used to send a message to the local subnetwork. A URN that identifies a broadcast (16777215) would be used to send a message to the local subnetwork without routing (e.g., radio subnet, data link address of 127, IP broadcast without routing, or Local Area Network subnetwork broadcast without routing). The Broadcast URN shall not be acknowledged. A URN that identifies a multicast group would represent a sometimes large group of users, typically organized by echelon. The applicable codes for this field are specified in the VMF TIDP-TE. The URN field and the Unit Name field are mutually exclusive fields (one or the other, not both).

5.6.3.2 Unit name field.

This field shall be a variable size field up to a maximum of 448 bits. It shall be in a character-coded format and used to uniquely identify a friendly military individual, unit, broadcast group or multicast group. This field is divided into 64 groups of 7 bits each representing an ANSI ASCII character. Special characters are legal. ANSI ASCII Delete (1111111) shall be used as an end-of-text marker if the field is not at the maximum length. The Broadcast URN (16777215) shall have the corresponding unit name of Broadcast_URN.

5.6.4 User message format (UMF) field.

This field shall be a 4-bit binary codeword representing the message formats shown in TABLE IV. This field indicates the format of the message that is contained in the user data field and has association with the other message format-dependent fields, including, Functional Area Designator (FAD) (see 5.6.5), Message Number (see 5.6.6), Message Subtype (see 5.6.7), CANTCO Reason, (see 5.6.23), and CANTPRO Reason (see 5.6.24). The applicable codes for these fields are associated with the corresponding UMF in appendices to this document as shown in TABLE IV.

TABLE IV. UMF codes

Type of Message Format	**Code** MSB - LSB	**Message Format-Dependent Field/Code Reference**
Link 16 (J-series message)	0000 (0)	MIL-STD-6016
Binary File	0001 (1)	5.6.4.1
Variable Message Format (VMF) (K-series message)	0010 (2)	Appendix A
National Imagery Transmission Format System (NITFS)	0011 (3)	TBD
Forwarded Message (FWD MSG)	0100 (4)	5.6.4.2
United States Message Text Format (USMTF)	0101 (5)	5.6.4.3
(DOI-103)	0110 (6)	5.6.4.4
eXtensible Markup Language (XML) - Message Text Format (MTF)	0111 (7)	5.6.4.5
eXtensible Markup Language (XML) - Variable Message Format (VMF)	1000 (8)	5.6.4.6
Undefined	1011 – 1111 (9 - 15)	TBD

5.6.4.1 Binary file.

The transfer of a binary file or data block is indicated by setting the UMF field to “1” (0001). The block of data being transferred is a “logical binary file” whose format and content is not dictated by the file system or specific software application resident in the interfacing host processors. The binary file data is placed in the User Data portion of the application PDU. The file name is indicated in the File Name field (see 5.6.8) and the file size is indicated in the Message Size field (see 5.6.9). Except as indicated below, all other fields in the Message Handling Repeatable Group (R3) are used as defined in Appendix A (VMF). For file transfers, the GPI for the Message Identification Group (G4) shall be set to 0.

5.6.4.2 Forwarded message.

The forwarding of a message is indicated by setting the UMF field to “4” (0100). The forwarded message (including its application header) is placed in the User Data portion of the application PDU. When forwarding a message, all header and message body information of the forwarded message shall not be modified. Except as indicated below, all other fields in the Message Handling Repeatable Group (R3) are used as defined in Appendix A (VMF). For message forwarding, the GPI for the Message Identification Group (G4) shall be set to 0.

5.6.4.3 USMTF messages.

The format of USMTF messages is defined in MIL-STD-6040. The transfer of a USMTF file or data block is indicated by setting the code field to “5” (0101). The block of data being transferred is in USMTF format whose content is not dictated by the file system or software application resident in the interfacing host processors. For UMFs of this type the GPI for the Message Identification Group (G4) shall be set to 0.

5.6.4.4 DOI-103 messages.

The transfer of a DOI-103 file or data block is indicated by setting the code field to “6” (0110). The block of data being transferred is in USMTF format whose content is not dictated by the file system or software application resident in the interfacing host processors. For UMFs of this type the GPI for the Message Identification Group (G4) shall be set to 0.

5.6.4.5 XML-MTF.

The format of XML-MTF messages is defined in MIL-STD-6040, Annex A. The Transfer of an XML-MTF file or data block is indicated by setting the code field to binary "7" (0111). The block of data being transferred is in XML-MTF format whose content is not dictated by the file system or software application resident in the interfacing host processors. For UMF of this type the GPI for Message Identification Group (G4) shall be set to 0 (Not Present).

5.6.4.6 XML-VMF.

The format of XML-VMF messages is defined in VMF TIDP-TE, Appendix (TBD). The Transfer of an XML-VMF file or data block is indicated by setting the code field to binary "8" (1000). The block of data being transferred is in XML-VMF format whose content is not dictated by the file system or software application resident in the interfacing host processors. For UMF of this type the GPI for Message Identification Group (G4) shall be set to 1 (Present).

5.6.4.7 Message standard version.

This field shall be a 4-bit binary codeword (0 - 15) representing the message standard. This field indicates the version of the message standard that is contained in the user data field and has association with the UMF field. For those standards that do not support baseline implementation by the year, will be denoted by the Revision/Reissue. For the VMF, Link 16, USMTF, XML-MTF and XML-VMF bit codes 10 through 15 are reserved for those situations outside the current numbering scheme. As the VMF TIDP-TE matures it will eventually migrate to Military Standard (MIL-STD) 6017. The message standard versions for the supported UMF codes are shown in TABLE V.

TABLE V. Message standard version based on UMF codes

MSG STD Ver Bit Code	Link 16 (MIL-STD-6016) [0]	Binary File [1]	VMF Reissue [2]	NITFS [3]	FWD MSG [4]	USMTF (MIL-STD-6040) [5]	DOI-103 [6]	XML-MTF [7]	XML-VMF Reissue [8]
0	6016	Illegal	TIDP-TE R2	Undef	Illegal	1993	Undef	Undef	Undef
1	6016A	Illegal	TIDP-TE R3	Undef	Illegal	1995	Undef	Undef	Undef
2	6016B	Illegal	TIDP-TE R4	Undef	Illegal	1997	Undef	Undef	Undef
3	6016C	Illegal	TIDP-TE R5	Undef	Illegal	1998	Undef	Undef	TIDP-TE R5
4	6016D	Illegal	TIDP-TE R6	Undef	Illegal	1999	Undef	Undef	TIDP-TE R6
5	6016E	Illegal	TIDP-TE R7	Undef	Illegal	2000	Undef	Undef	TIDP-TE R7
6	6016F	Illegal	6017	Undef	Illegal	2001	Undef	2001	6017
7	6016G	Illegal	6017A	Undef	Illegal	2002	Undef	2002	6017A
8	6016H	Illegal	6017B	Undef	Illegal	2003	Undef	2003	6017B
9	6016I	Illegal	6017C	Undef	Illegal	2004	Undef	2004	6017C
10	Reserved	Illegal	Reserved	Undef	Illegal	Reserved	Undef	Reserved	Reserved
11	Reserved	Illegal	Reserved	Undef	Illegal	Reserved	Undef	Reserved	Reserved
12	Reserved	Illegal	Reserved	Undef	Illegal	Reserved	Undef	Reserved	Reserved
13	Reserved	Illegal	Reserved	Undef	Illegal	Reserved	Undef	Reserved	Reserved
14	Reserved	Illegal	Reserved	Undef	Illegal	Reserved	Undef	Reserved	Reserved
15	Reserved	Illegal	Reserved	Undef	Illegal	Reserved	Undef	Reserved	Reserved

5.6.5 Functional area designator (FAD) field.

This field shall contain a 4-bit binary codeword that identifies the functional area of a specific VMF message using codewords. The FAD combined with the Message Number field is used to define the applicable VMF message. The applicable codes for this field are specified in Appendix A as referenced TABLE XIV.

5.6.6 Message number field.

This field shall contain a 7-bit binary codeword that represents the number that identifies a specific VMF message within a functional area (see 5.6.5). The Message Number value shall range from 1 to 127.

5.6.7 Message subtype field.

This field shall contain a 7-bit binary codeword that represents the number that identifies a specific case (see A.3.4) within a VMF message. The case depends on the setting of the UMF field (see 5.6.4), Functional Area Designator field (see 5.6.5) and Message Number field (see 5.6.6) as is specified in Appendix A as referenced in TABLE IV and TABLE XV.

5.6.8 File name.

The File Name field shall be a character coded, variable length field of up to 64 7-bit ANSI ASCII characters (448 bits). It indicates the name of the computer file or data block contained in the User Data portion of the application PDU. The last four characters of the field may consist of a period followed by a three-character ending, indicative of

the file type (e.g., .txt, .doc, .exe, .bin). Special characters are legal. ANSI ASCII Delete (1111111) shall be used as an end-of-text marker if the field is not at the maximum length.

5.6.9 Message size field.

This field shall contain a 20-bit binary number indicating the size, in bytes, of the associated message. Within the user data, a message which is not a multiple of 8 bits, shall be zero-filled so that it becomes a multiple of 8 bits. When optional message compression is used, the message size field shall reflect the size of the message after it has been compressed. This field is required when there is more than one occurrence of the Message Handling Group (R3 in TABLE I) or, when there is a single occurrence of the Message Handling Group and a streaming/undelimited transport (such as TCP) is being used, but not when a delimited transport (such as UDP and S/R) is being used. If the transport protocol is unknown, a streaming/undelimited transport should be assumed when determining whether the message size field is required.

5.6.10 Operation indicator field.

This field shall be a 2-bit binary codeword, as shown in TABLE VI, indicating the operational function of the message used in support of either an operation, exercise, simulation or test.

5.6.11 Retransmit indicator field.

This shall be a one-bit field indicating whether a message is a retransmission. This field set to 1 shall affirm that the message is a retransmission. This field set to 0 shall indicate that the message is not a retransmission.

5.6.12 Message precedence field.

This field shall be a 3-bit binary codeword indicating the relative precedence of a message as shown in TABLE VII.

TABLE VI. Operation indicator codes

Operation indicator	Code MSB - LSB	Explanation
Operation	00 (0)	A military action or the carrying out of a strategic tactical, service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defense and maneuvers needed to gain the objectives of any battle or campaign. (JP 1-02)
Exercise	01 (1)	A military maneuver or simulated wartime operation involving planning preparation, and execution. It is carried out for the purpose of training and evaluation. It may be a combined, joint, or single-Service exercise, depending on participating organizations. (JP 1-02)
Simulation	10 (2)	Bogus message(s) initiated from simulated video, computer-generated or other input such as a scenario generator for training purposes.
Test	11 (3)	Message(s) inserted for the purpose of validating connectivity and interoperability of communications components and Command, Control, Communications, Computers and Intelligence (C4I) system(s).

TABLE VII. Message precedence codes

Precedence	Code MSB - LSB	Explanation
Undefined	000-001 (0 – 1)	
Emergency command	010 (2)	Reserved for only the NCA and certain designated commanders of Unified and Specified Commands, and then only for certain designated emergency action command and control messages. These messages shall be processed ahead of all other traffic and interrupt lower precedence traffic.
Undefined	011 (3)	
Flash	100 (4)	Reserved for initial enemy contact messages or operational combat messages of extreme urgency.
Immediate	101 (5)	Reserved for messages relating to situations that gravely affect the security of national/allied forces or populace and that require immediate delivery to the addressee(s).
Priority	110 (6)	Reserved for messages that requires expeditious action by the addressee(s) and/or furnishes essential information for the conduct of operations in progress when routine precedence will not suffice.
Routine	111 (7)	Used for all types of messages that justify transmission by rapid means unless of sufficient urgency to require a higher precedence

5.6.13 Security classification field.

This field shall be a 2-bit codeword indicating the security classification of the message as shown in TABLE VIII.

5.6.14 Control and release marking field.

This optional field, if present, shall be a variable size field up to a maximum of 224 bits. It shall be in a character-coded format and encoded as thirty-two 7-bit ANSI ASCII characters indicating the restrictions or requirements for special handling, access control, and releasability of the message. ANSI ASCII Delete (1111111) shall be used as an end-of-text marker if the field is not at the maximum length. Note: The field is intended to support the exchange of a list of up to 10 country codes (per FIPS 10-4) with which the message can be released or controlled.

TABLE VIII. Security classification codes

Classification	Code MSB - LSB
Unclassified	00 (0)
Confidential	01 (1)
Secret	10 (2)
Top secret	11 (3)

5.6.15 Originator date-time group (DTG).

These fields shall contain date and time information indicating the time, expressed in Zulu (Universal Time Coordinate) Time, that the message was prepared. This group combination shall be 33 bits long and shall contain data fields representing the year, month, day, hour, minute, and seconds of the message. Coding for each data field shall be as shown in TABLE IX.

TABLE IX. DTG codes

.

Element	Code MSB - LSB	Bits
Year	0000000 - 1100011 (0 - 99, where 00 - 94 equates to 2000 - 2094 95 - 99 equates to 1995 - 1999)	7
Month	0001 - 1100 (1 - 12)	4
Day	00001 - 11111 (1 - 31)	5
Hour (24 hour clock)	00000 - 10111 (0 - 23)	5
Minute	000000 - 111011 (0 - 59)	6
Second	000000 - 111011 (0 - 59)	6

5.6.16 DTG extension field.

This field shall be a 12-bit binary field containing a value that uniquely identifies each message. This field is mandatory if more than one message is sent with the same Originator DTG.

5.6.17 Time perishability DTG.

The fields in this group provide the latest time the message is still of value. These fields shall be encoded as specified in 5.6.15.

5.6.18 Machine acknowledge request indicator field.

This field shall be a 1-bit binary codeword indicating whether the originator of a message requires a machine acknowledge for the message. This field set to 1 shall affirm that a machine acknowledgment is required. This field set to 0 shall indicate that a machine acknowledgment is not required.

5.6.19 Operator acknowledge request indicator field.

This field shall be a 1-bit binary codeword indicating whether the originator of a message requires an operator acknowledgment for the message from the recipient. This field set to 1 shall affirm that an operator acknowledgment from the recipient is required. This field set to 0 shall indicate that an operator acknowledgement is not required.

5.6.20 Operator reply request indicator field.

This field shall be a 1-bit binary codeword indicating whether the originator of a message requires an operator reply to the message. This field set to 1 shall affirm that an operator reply to the message is required. This field set to 0 shall indicate that an operator reply is not required.

5.6.21 Message acknowledgment DTG.

The fields in this group provide the date and time of the original message that is being acknowledged. These fields shall be encoded as specified in 5.6.15.

5.6.22 Receipt/Compliance (R/C) field.

This field shall be a 3-bit binary codeword representing the R/C codes shown in TABLE X.

TABLE X. R/C codes

Type of R/C	Code MSB - LSB	Used by	Explanation
Undefined	000 (0)		
Machine Receipt [MR]	001 (1)	Recipient	Automatically generated in response to a machine acknowledge request from the originator to indicate that the original message can be successfully processed at the ultimate destination
Cannot Process [CANTPRO]	010 (2)	Recipient	Automatically generated to indicate that an original message cannot be successfully processed at the ultimate destination
Operator Acknowledge [OPRACK]	011 (3)	Recipient	A positive operator-generated acknowledgment to indicate receipt of a message at the ultimate destination
Will Comply [WILCO]	100 (4)	Recipient	An operator reply generated to indicate that received message is understood and that the ultimate destination will comply
Have Complied [HAVCO]	101 (5)	Recipient	An operator reply generated to indicate that received message is understood and that the ultimate destination has complied
Cannot Comply [CANTCO]	110 (6)	Recipient	An operator reply generated to indicate that a received message cannot or will not be carried out
Undefined	111 (7)		

5.6.23 Cannot comply (CANTCO) reason field.

This user-defined field shall be a 3-bit binary codeword indicating the reason that a recipient cannot comply with a particular message. The applicable codes for this field depend on the setting of the UMF field and are specified in Appendix A as referenced in TABLE IV.

5.6.24 Cannot process (CANTPRO) reason field.

This user-defined field shall be a 6-bit binary codeword indicating the reason that a particular message cannot be processed by a recipient or information addressee. It shall be used only in R/C messages. The applicable codes for this field depend on the setting of the UMF field and are specified in Appendix A as referenced in TABLE IV.

5.6.25 Reply amplification field.

This field shall be a variable size up to a maximum of 350 bits. It shall be a character-coded field to provide textual data for an amplification of the recipient's reply to a message, if necessary. This field is divided into 50 groups of 7

bits each representing an ANSI ASCII character. Special characters are legal. ANSI ASCII Delete (1111111) shall be used as an end-of-text marker if the field is not at the maximum length.

5.6.26 Reference message data group.

This group is used to reference existing messages that are related to the subject message contained in the User Data portion of the application PDU. The elements of this group are used to uniquely identify a reference message by specifying the originator address group and DTG. For example, if the subject message is a response to a previously exchanged request message, then the Reference Message Data Group may contain the originator and DTG of the request message.

5.6.27 Header size field.

This field shall be a 16-bit binary number indicating the size, in octets, of the header. All fields contained in the header, including all header fields preceding the Header Size field, the Header Size field itself, and all header fields following the Header Size field, are included in the octet count. This optional field is required when sending multiple messages over a streaming transport mechanism, e.g. persistent TCP connection.

5.6.28 Security parameter information (SPI).

This field shall be a 4-bit binary field, as shown in TABLE XI, indicating the identities of the parameters and algorithms that enable unambiguous security processing. This provides for 16 unique security implementations. Security implementations will differ in that all implementation may not provide the same security services or use the same algorithms and parameters.

TABLE XI. Security parameter information type codes

Code MSB - LSB	**Reference**
0000 (0)	Authentication (using SHA-1 and DSA)/ No Encryption
0001 – 1111 (1 – 15)	Undefined

It should be noted that the maximum field sizes are quite large in order to support newer and future cryptographic algorithms and very large key sizes. TABLE XII provides guidance on current typical sizes. In addition Appendix D provides the actual field sizes used when the SPI value is 0.

TABLE XII. SPI typical field sizes

Field Name	Size
Keying Material ID	0 - 64
Cryptographic Initialization	0 - 128
Key Token	0 - 512
Authentication Data (A)	320 - 1024
Authentication Data (B)	320 - 1024
Message Security Padding	0 - 128

5.6.29 Keying material ID length.

This field shall be a 3-bit binary field that defines the size, in octets, of the Keying Material ID field. A value of zero (0) defines the length as one (1) octet and a value of seven (7) defines the length as eight (8) octets. The Keying Material ID Length value shall range from 0 to 7.

5.6.30 Keying material ID.

This field shall be a variable size up to a maximum of 64-bits. This binary field identifies the key, a unique value, which was used for encryption. The SPI shall specify the value used for this field.

5.6.31 Cryptographic initialization length.

This field shall be a 4-bit binary field that defines the size, in 64-bit blocks, of the Cryptographic Initialization field. A value of zero (0) defines the length as one (1) 64-bit block and a value of 15 defines the length as 16 64-bit blocks. The Cryptographic Initialization Length value shall range from 0 to 15.

5.6.32 Cryptographic initialization.

This field shall be a variable size up to a maximum of 1024-bits. This binary field identifies a sequence of bits used by the originator and recipient to initialize the encryption and decryption process. The mechanism that describes how Cryptographic Initialization is achieved and the format of initialization data is determined by the value of the SPI.

5.6.33 Key token length.

This field shall be an 8-bit binary field that defines the size, in 64-bit blocks, of the Key Token field. A value of zero (0) defines the length as one (1) 64-bit block and a value of 255 defines the length as 256 64-bit blocks. The Key Token Length value shall range from 0 to 255. A key token maybe required for each originator, recipient and information addressee. The FRI field allows for up to 17 key tokens per message.

5.6.34 Key token.

This field shall be a variable size up to a maximum of 16,384-bits. This binary field that contains information, which enables each member of each address group to decrypt the user data associated with this message header. The mechanism that describes how Key Tokens are generated, validated, and processed is specified by the value of the SPI.

5.6.35 Authentication data (A) length.

This field shall be a 7-bit binary field that defines the size, in 64-bit blocks, of the Authentication Data (A) field. A value of zero (0) defines the length as one (1) 64-bit block and a value of 127 defines the length as 128 64-bit blocks. The Authentication Data (A) Length value shall range from 0 to 127.

5.6.36 Authentication data (A).

This field shall be a variable size up to a maximum of 8192-bits. This binary field is created by the originator of the message. It provides both connectionless integrity and data origin authentication (proof of origin). The mechanism that describes how Authentication Data (A) is generated, validated, and processed is specified by the value of the SPI.

5.6.37 Authentication data (B) length.

This field shall be a 7-bit binary field that defines the size, in 64-bit blocks, of the Authentication Data (B) field. A value of zero (0) defines the length as one (1) 64-bit block and a value of 127 defines the length as 128 64-bit blocks. The Authentication Data (B) Length value shall range from 0 to 127.

5.6.38 Authentication data (B).

This field shall be a variable size up to a maximum of 8192-bits. This binary field is created by the party sending the response acknowledgment message. It consists of a digital signature (proof of receipt) of the message which is being acknowledged. The acknowledgment message itself shall also contain Authentication Data (A). The mechanism that describes how Authentication Data (B) is generated, validated, and processed is specified by the value of the SPI.

5.6.39 Signed acknowledge request indicator.

This field shall be a 1-bit binary field indicating whether the originator of a message requires a signed response from the recipient. This field set to 1 shall indicate that a signed response is required from the recipient. This field set to 0 shall indicate that a signed response is not required.

5.6.40 Message security padding length.

This field shall be an 8-bit binary field that defines the size, in octets, of the message security padding field. A value of zero (0) defines the length as zero (0) octets and a value of 255 defines the length as 255 octets. The Message Security Padding Length value shall range from 0 to 255.

5.6.41 Message security padding.

This field shall be a variable size up to a maximum of 2040-bits. This binary field is necessary for a block encryption algorithm so that the message content to be encrypted is a multiple of the encryption block length. The value of the SPI shall specify the message security padding rules.

5.7 Application header formatting rules and construction procedures.

The case and condition syntax and procedures tabulated below shall be applied in the formatting and construction of the application header.

5.7.1 Case and conditionality statement syntax.

The purpose of the case and conditionality statements is to rigorously and unambiguously define the construction rules for the application header so that it will be possible to achieve consistent construct implementations across multiple systems. They include cases for each use of the application header and the inter-element conditionalities within the application header for basic processing, defaults, legal entries, and special considerations.

5.7.1.1 Logical operators.

Natural language does not lend itself to rigorous and unambiguous expression, therefore it is necessary to use well established logical operators to establish precise, mathematical meaning for logical relationships. The logical operators that will be used in this document are:

AND - separates two discrete values and evaluates to true if both of the discrete values are true.
OR - inclusive OR separates two discrete values and evaluates to true if at least one of the discrete conditions is true.
XOR - exclusive OR separates two discrete values and evaluates to true if and only if one, not both, of the discrete conditions is true.
NOT - a simple negation of the condition so that if A is true the NOT A would yield false.

The following truth table (TABLE XIII) illustrates the meaning of the logical operator definitions given above. The table shows, for example, that given both “A” and “B” as true, then “NOT A” will yield false. “A AND B” will yield true, “A OR B” will yield true, and “A XOR B” will yield false. “A AND B” in this example represents names or action designators.

TABLE XIII. Logical operator definitions

A	B	NOT A	A AND B	A OR B	A XOR B
TRUE	TRUE	FALSE	TRUE	TRUE	FALSE
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
FALSE	TRUE	TRUE	FALSE	TRUE	TRUE
FALSE	FALSE	TRUE	FALSE	FALSE	FALSE

5.7.1.2 Application.

Case and conditionality statements are used only to restrict the structure of the application header to a well-defined subset of the possible legal configurations that are specified by the application rules of application header construction.

5.7.1.3 Reserved words.

Case statements reserved words that will be used in this document are:

CASE -	Identifies the title (purpose) under which the statement is defined.
END CASE -	Ends the case statement.
IF...THEN...ELSE -	Describes conditions under which statements are valid. The statement always starts with "IF" and shall end with "ENDIF". An "IF" statement selects for execution, one or none of the enclosed sequence of statements depending on the (truth) value of one or more corresponding conditions.
ELSIF -	This keyword is used to extend the flexibility of the "IF...THEN...ELSE" construct. It is used when multiple conditions need to be evaluated in order to determine a logic path. Multiple "ELSIF" conditions are permitted. The general form is: IF *condition* THEN *sequence of statements* ELSIF *condition* THEN *sequence of statements* ELSE *sequence of statements* ENDIF
ENDIF -	Ends condition statement.

5.7.1.4 Cases.

Case statements are a form of expressing a condition. The construct in this document indicates there shall be at least two alternatives, and only one alternative at a time shall be valid. Case statements are used when a condition statement becomes too complex. A case statement may include an "XOR" (Exclusive OR) operator when it is possible to accomplish the same purpose in one or more ways. A case statement may also include an "OR" operator when any, or all, of several data elements can be used.

5.7.1.5 Conditions.

Condition statements define the conditions under which a data group, data element, or value in a data element may be used. The condition statement is very structured in its use. The following is an example of the format of a conditional statement:

```
IF (condition)
  THEN  (Sequence of Statements)
  ELSIF (condition)
  THEN (Sequence of Statements)
  ELSE (Sequence of Statements)
ENDIF
```

For the execution of an "IF" statement, the condition specified after "IF", and any conditions specified after other keywords are evaluated in succession until one evaluates to "TRUE", or all conditions are evaluated and yield "FALSE". If one condition evaluates to "TRUE", then the corresponding sequence of statements are executed. If all conditions evaluate to "FALSE" and an "ELSE" statement is present, the sequence of statements associated with the "ELSE" are executed; otherwise, none of the sequence statements are executed.

5.7.1.6 Defaults.

Defaults will be defined only if the receiving system's default value is of concern to the interface.

5.7.1.7 Expected response.

The expected response by the system receiving an application header will depend on the content of the header fields and shall be stated as it relates to the case and conditionality statements for the header.

5.7.1.8 Special considerations.

Special considerations cover those exceptions that cannot be defined under the preceding paragraphs.

5.7.1.9 Application header receipt.

Upon receipt of an application header, a system shall validate the presence of all mandatory groups and fields, determine that all occurrence category conditions are satisfied, and validate the legality of all field entries to determine the legality of the header. This receipt processing is required for each header.

5.7.2 Cases and conditions for the application header.

5.7.2.1 Cases.

5.7.2.1.1 Case 1: Message is an original message.

THIS CASE REQUIRES
GPI for Group 8 [Response Data Group] shall be "0" (Not Present)
AND Message body shall be present
END CASE

5.7.2.1.2 Case 2: Message is an acknowledgment message.

THIS CASE REQUIRES
GPI for Group 8 [Response Data Group] shall be "1" (Present)
AND GPI for Group 6 [Perishability DTG Group] shall be "0" (Not Present)
AND GPI for Group 7 [Acknowledgment Request Group] shall be "0" (Not Present)
AND Message body shall not be present
END CASE

5.7.2.1.3 Case 3: Message is a Computer File/Data Block Transfer.

THIS CASE REQUIRES
UMF shall be "1" (Binary File)
AND GPI for Group 4 [Message Identification Group] shall be "0" (Not Present)
END CASE

5.7.2.1.4 Case 4: Message is a Forwarded Message.

THIS CASE REQUIRES
UMF shall be “4” (Forwarded Message)
AND GPI for Group 4 [Message Identification Group] shall be “0” (Not Present)
AND User Data shall be present
END CASE

5.7.2.1.5 Case 5: Message was compressed.

THIS CASE REQUIRES
FPI for Data Compression shall be “1” (Present)
AND GPI for Group 8 [Response Data Group] shall be “0” (Not Present)
AND User Data shall be present
END CASE

5.7.2.1.6 Case 6: Message has security services applied.

THIS CASE REQUIRES
GPI for Group 10 [Message Security Group] shall be “1” (Present)
END CASE

5.7.2.1.7 Case 7: Message is a signed acknowledgment.

THIS CASE REQUIRES
GPI for Group 8 [Response Data Group] shall be "1" (Present)
AND GPI for Group 6 [Perishability DTG Group] shall be "0" (Not Present)
AND GPI for Group 7 [Acknowledgment Request Group] shall be "0" (Not Present)
AND GPI for Group 14 [Authentication Data (A)] shall be "1" (Present)
AND GPI for Group 15 [Authentication Data (B)] shall be "1" (Present)
AND Signed Acknowledge Request Indicator shall be "0" (Signed Response Not Required)
AND User Data shall not be present
END CASE

5.7.2.2 Conditions.

5.7.2.2.1 Condition 1:

IF the Originator Address Group is not present, THEN an acknowledgment shall not be requested.

IF GPI for Group 1 [Originator Address Group] is set to “0” (Not Present)
THEN GPI for Group 7 [Acknowledgment Request Group] shall be set to “0” (Not Present)
ENDIF

5.7.2.2.2 Condition 2:

IF the Bit-coded URN is present, THEN the Character-coded Unit Name shall not be present in the same address group.

IF FPI for URN is set to “1” (Present)
THEN FPI for Unit Name shall be set to “0” (Not Present)
ENDIF

5.7.2.2.3 Condition 3:

IF the Bit-coded URN is not present, THEN the Character-coded Unit Name shall be present in the same address group.

IF FPI for URN is set to “0” (Not Present)
THEN FPI for Unit Name shall be set to “1” (Present)
ENDIF

5.7.2.2.4 Condition 4:

IF the Character-coded Unit Name is present, THEN the Bit-coded URN shall not be present in the same address group.

IF FPI for Unit Name is set to “1” (Present)
THEN FPI for URN shall be set to “0” (Not Present)
ENDIF

5.7.2.2.5 Condition 5:

IF the Character-coded Unit Name is not present, THEN the Bit-coded URN shall be present in the same address group.

IF FPI for Unit Name is set to “0” (Not Present)
THEN FPI for URN shall be set to “1” (Present)
ENDIF

5.7.2.2.6 Condition 6:

This paragraph is left blank to maintain paragraph conformity.

5.7.2.2.7 Condition 7:

IF Message Handling Group (R3) repeats, THEN Message Size and Header Size shall be present.

IF GRI of R3 [Message Handling Group] is set to “1” (Repeated)
THEN FPI for Message Size shall be set to “1” (Present)
AND FPI for Header Size shall be set to "1" (Present)
ENDIF

5.7.2.2.8 Condition 8:

IF the message is not a CANTCO, THEN CANTCO Reason Code cannot be present.

IF R/C is NOT set to “6” (CANTCO)
THEN FPI for CANTCO Reason Code shall be set to “0” (Not Present)
ENDIF

5.7.2.2.9 Condition 9:

IF the message is not a CANTPRO, THEN CANTPRO Reason Code cannot be present.

IF R/C is NOT set to “2” (CANTPRO)
THEN FPI for CANTPRO Reason Code shall be set to “0” (Not Present)
ENDIF

5.7.2.2.10 Condition 10:

This paragraph is left blank to maintain paragraph conformity.

5.7.2.2.11 Condition 11:

IF the Machine Acknowledge OR Operator Acknowledge OR Operator Reply Request Indicators are set to “1”, THEN the Originator DTG group shall be present.

IF Machine Acknowledge Request Indicator is set to “1” (Machine Acknowledgment Required)
OR Operator Acknowledge Request Indicator is set to “1” (Operator Acknowledgment Required)
OR Operator Reply Request Indicator is set to “1” (Operator Reply Required)
THEN GPI for Group 5 [Originator DTG] shall be set to “1” (Present)
ENDIF

5.7.2.2.12 Condition 12:

This paragraph is left blank to maintain paragraph conformity.

5.7.2.2.13 Condition 13:

IF the Security Parameters Information is “0” (Authentication (using SHA-1 and DSA)/ No Encryption) THEN GPI for Keying Material Group, GPI for Cryptographic Initialization Group, GPI for Key Token Group, AND GPI for Message

Security Padding Group shall all be set to “0” (Not Present), AND the GPI for Authentication Data (A) Group shall be set to “1” (Present).

IF Security Parameters Information is set to “0” (Authentication (using SHA-1 and DSA)/ No Encryption)
THEN GPI for Group 11 [Keying Material Group] shall be set to “0” (Not Present)
AND GPI for Group 12 [Cryptographic Initialization Group] shall be set to “0” (Not Present)
AND GPI for Group 13 [Key Token Group] shall be set to “0” (Not Present)
AND GPI for Group 14 [Authentication (A) Group] shall be set to “1” (Present)
AND GPI for Group 16 [Message Security Padding Group] shall be set to “0” (Not Present)
ENDIF

5.7.2.2.14 Condition 14:

IF the GPI for Acknowledgment Request Group is set to “0” (Not Present) THEN the Signed Acknowledge Request Indicator shall be set to “0” (Signed Acknowledgment Not Required).

IF GPI for Group 7 [Acknowledgment Request Group] is set to “0” (Not Present)
THEN Signed Acknowledge Request Indicator shall be set to “0” (Signed Acknowledgment Not Required).
ENDIF

5.7.2.2.15 Condition 15:

IF the Signed Acknowledge Request Indicator is set to “1” (Signed Acknowledgment Required) THEN the Acknowledgment Request Group shall be set to “1” (Present).

IF Signed Acknowledge Request Indicator is set to “1” (Signed Acknowledgment Required)
THEN GPI for Group 7 [Acknowledgment Request Group] shall be set to “1” (Present).
ENDIF

5.7.2.3 Defaults.

Default values for Message Precedence, Acknowledgments, and Message Classification shall be user defined.

5.7.3 Expected response.

5.7.3.1 Machine acknowledge requested:

IF Machine Acknowledge Requested Indicator is set to “1” (Machine Acknowledgment Required)
THEN Response shall have R/C set to “1” (Machine Receipt)
OR Response shall have R/C set to “2” (CANTPRO)
ENDIF

5.7.3.2 Operator acknowledge requested:

IF Operator Acknowledge Requested Indicator is set to “1” (Operator Acknowledgment Required)
THEN Response shall have R/C set to “3” (OPRACK)
OR Response shall have R/C set to “2” (CANTPRO)
ENDIF

5.7.3.3 Operator reply requested:

IF Operator Reply Requested Indicator is set to “1” (Operator Reply Required)
THEN Response shall have R/C set to “4” (WILCO)
OR Response shall have R/C set to “5” (HAVCO)
OR Response shall have R/C set to “6” (CANTCO)
OR Response shall have R/C set to “2” (CANTPRO)
ENDIF

5.7.3.4 Signed acknowledge requested:

IF Signed Acknowledge Request Indicator is set to “1” (Signed Acknowledgment Required)
THEN Response shall have GPI for Group 15 [Authentication (B) Group] set to “1” (Present)
OR {Response shall have R/C set to “2” (CANTPRO)
AND [CANTPRO Reason Code is specified “27” (Authentication Failure)
OR CANTPRO Reason Code is specified “28” (Certificate not found)
OR CANTPRO Reason Code is specified “29” (Certificate invalid)
OR CANTPRO Reason Code is specified “30” (Do not support this SPI value)
OR CANTPRO Reason Code is specified “31” (Can not generate a signed acknowledgment)]}
ENDIF

5.7.4 Special considerations.

5.7.4.1 Perishable data check. Discard messages that are too old:

IF GPI for Group 6 [Perishable Data DTG] is set to “1” (Present)
AND Group 6 [Perishable Data DTG] is earlier than current DTG
THEN Message data shall be ignored
AND
IF Machine Acknowledgment Request indicator is set to “1” (Machine Acknowledgment Required)
THEN Response shall have R/C set to “2” (CANTPRO)
AND a CANTPRO Reason Code set to “25” (Message too Old, Based On Perishability)
ENDIF
ENDIF

5.7.4.2 Response to version non-interoperability.

Version code is set to “15” (Version Sent Not Implemeneted) if recipient does not implement the MIL-STD-2045-47001 version sent.

IF Recipient does not implement Version sent
THEN Version shall be set to “15” (Version Sent Not Implemented)
AND FPI for Data Compression Type shall be set to “0” (Not Present)
AND GPI for Group 1 [Originator Address Group] shall be set to “1” (Present)
AND Originator Address specified is the Original Recipient
AND GPI for Group 2 [Recipient Address Group] shall be set to “1” (Present)
AND Recipient Address specified is the Originator of the original message
ENDIF

5.7.4.3 Broadcast transmission check.

IF the Recipient Address Group is not present, AND the Information Address Group is not present THEN the message shall be a broadcast transmission.

IF GPI for Group 2 [Recipient Address Group] is set to “0” (Not Present)
AND GPI for Group 3 [Information Address Group] is set to “0” (Not Present)
THEN the message shall be broadcast in accordance with lower layer broadcast protocols
ENDIF

5.7.4.4 Originator DTG check.

IF the Originator DTG is ambiguous, THEN the DTG Extension shall be present.

IF Originator DTG is equal to the Originator DTG of a previously sent message
THEN FPI for DTG Extension shall be set to “1” (Present)
AND DTG Extension shall be unique
ENDIF

5.7.4.5 Message sent via a streaming/undelimited transport protocol check.

If Message Handling Group (R3) only occurs once and the message is being sent via a streaming/undelimited transport protocol, such as TCP, then Message Size and Header Size shall be present.

IF GRI of R3 [Message Handling Group] is set to “0” (Not Repeated)
AND the message is being sent via a streaming/undelimited transport
THEN FPI for Message Size shall be set to “1” (Present)
AND FPI for Header Size shall be set to "1" (Present)
ENDIF

5.7.4.6 Message concatenation.

When concatenating messages, the Originator, Recipient and Information Address Groups shall be common for all concatenated messages and therefore will appear once in the Application Header. The Message Handling Group (R3) shall repeat to specify information about each concatenated message. Each occurrence of the Message Handling Group [R3] shall be matched to its respective message in the User Data portion. The total size of a concatenated message block shall not exceed 1 megabyte (1,048,575 bytes).

IF GPI for Group 1 [Originator Address Group] is set to “1” (Present)
OR GPI for Group 2 [Recipient Address Group] is set to “1” (Present)
OR GPI for Group 3 [Information Address Group] is set to “1” (Present)
THEN (Group 1 [Originator Address Group], Group 2 [Recipient Address Group], and Group 3 [Information Address Group] addresses are common to all concatenated messages)
AND GRI for R3 [Message Handling Group] shall be set to “1” (Repeated)
AND Each iteration shall match in sequence specifying information about its respective concatenated message
AND FPI for Message Size shall be set to “1” (Present)
AND FPI for Header Size shall be set to "1" (Present)
AND Message Size, including application header, shall not exceed 1,048,575 bytes
ENDIF

5.7.4.7 Message case and message subtype relationship.

IF Cases exist for transmitted VMF message
THEN FPI for Message Subtype is specified “1” (Present)
ENDIF

5.7.4.8 Sending response to a large message.

If the received message size is greater than the Maximum Segment Size AND Response(s) were requested AND the message was received via a reliable transport mechanism (e.g. S/R, TCP, etc.) THEN send the response(s) via a reliable transport mechanism.

IF The received message size is greater than Maximum Segment Size
AND GPI for G7 [Acknowledgment Request Group] is set to “1” (Present)
AND the message was received via a reliable transport mechanism
THEN Response(s) to the received message shall be sent via a reliable transport mechanism
ENDIF

5.7.4.9 DTG extension to DTG of message being acknowledged.

IF GPI for Group 8 [Response Data Group] is set to “1” (Present)
THEN
IF FPI for DTG Extension discriminating the Originator DTG is set to “1” (Present)
THEN Response message shall have GPI for Group 8 [Response Data Group] identifying the DTG of message being acknowledged is set to “1” (Present)
AND FPI for DTG Extension discriminating the DTG of message being acknowledged shall be set to “1” (Present)

ELSE

Response message shall have GPI for Group 8 [Response Data Group] identifying the DTG of message being acknowledged is set to “1” (Present)

AND FPI for DTG Extension discriminating the DTG of message being acknowledged is set to “0” (Not Present)

ENDIF

ENDIF

5.7.4.10 Decompression of messages prior to parsing.

IF FPI for Data Compression Type field is set to “1” (Present)
THEN Receiving system shall decompress the user data prior to parsing
ENDIF

5.7.4.11 Unit Name usage in a response message.

IF FPI for Unit Name identifying the originator is set to “1” (Present)
THEN Response message shall have the FPI for Unit Name identifying the recipient is set to “1” (Present)
AND FPI for URN is set to “0” (Not Present)
ENDIF

5.7.4.12 URN usage in a response message.

IF FPI for URN identifying the originator is set to “1” (Present)
THEN Response message shall have the FPI for URN identifying the recipient set to “1” (Present)
AND FPI for Unit Name shall be set to “0” (Not Present)
ENDIF

5.7.4.13 Addressee URN uniqueness.

A specified URN shall occur at most once as an addressee of a message, either as a recipient destination or as an information destination. A duplicate destination URN in the recipient address group and the information address group of a message is not permitted.

5.7.4.14 Message that uses segmentation/reassembly protocol.

IF Data transfer is greater than the Maximum Segment Size (MSS) permitted
THEN Message Segmentation/Reassembly protocol shall be used
ENDIF

5.7.5 User data.

This portion of the application PDU shall contain the application process messages or data.

5.7.5.1 Message acknowledgments.

A message acknowledgment is a report back to the originator on a receiving station's receipt of and intentions with respect to a received message. Acknowledgment requests are directed to message recipients only; they do not apply to information addressees. Acknowledgments are implemented in the acknowledgment header format.

5.7.5.2 Acknowledgment header format.

Machine and operator acknowledgment request indicators are used by the originator to request a specific response from the receiving station, or appropriate operator, for selective acknowledgment of message receipt and compliance with the message instructions. A receiving station shall respond to the originator by sending an acknowledgment header. Depending on the type of acknowledgment request from the originator or the type of system involved, the response may be machine-generated (automatic) or operator-generated (manual) or a combination of both. The acknowledgment header consists of the following groups and fields (see also 5.7.2.1.2):

a. Acknowledgment originator address group (G1)

b. Acknowledgment recipient address group (R1)

c. Message Handling Group (R3). Within Message Handling Group, the Response Data Group (G8), shall include the DTG of message being acknowledged and the R/C field.

5.7.5.3 Message accountability.

The application header shall be used for the detection of duplicate messages and to associate an acknowledgment header with the original requesting message. The received fields of originator address group, originator DTG, and DTG Extension are used to uniquely identify a message. The originator shall guarantee the uniqueness of this combination of fields by ensuring that no original message is transmitted having the same DTG and DTG Extension.

a. Duplicate message check. The originator address group, originator DTG, and DTG Extension fields of each received message are compared with the corresponding fields of previous messages. Any duplicate messages (including retransmitted messages) shall be acknowledged if required and shall otherwise be ignored (discarded).

b. Acknowledgment matching. The originator address group, DTG of message being acknowledged, and DTG Extension fields of each received acknowledgment header are compared with the recipient address group, Originator DTG, and DTG Extension fields of previously originated messages that require acknowledgment. The message handling application will maintain DTG, Originator Address, and DTG Extension information about previously received messages for a period of time long enough to exhaust the message originator's retransmission timers. Acknowledgment headers that match original messages shall be processed; unmatched Acknowledgment headers shall be ignored (discarded).

5.7.5.4 Message retransmission.

A retransmission capability shall be provided to enable the automatic retransmission of a message that has not received an acknowledgment when one was requested. Automatic Retransmissions shall only apply if a machine acknowledgment is requested. Any Application layer acknowledgment precludes message retransmission.

a. The number of automatic retransmissions shall be selectable with a range of 0 to 3. The parameter governing the number of retransmissions shall be separately selectable for each Originator DTG/DTG Extension combination.

b. A timer shall be provided to schedule the automatic retransmission. Expiration time shall be selectable with a range of 5 to 600 seconds. Upon expiration of the timer, provided an acknowledgment has not been received, the message shall be retransmitted by the originating system. If an acknowledgment is not received prior to expiration of the timer on the final retransmission, the operator shall be notified. Messages containing perishable data and requiring acknowledgment shall have the Perishability DTG set to a time later than the retransmit timeout.

5.7.5.5 Message concatenation.

This allows chaining of messages together, with abbreviated message headers, to decrease overhead and facilitate more efficient communications. When concatenating messages, the Originator, Recipient, and Information Address Groups shall be common for all concatenated messages and therefore will appear once in the Application Header. The Message Handling Group [R3] shall repeat to specify information about each concatenated message. Each occurrence of the Message Handling Group [R3] shall be matched to its respective message in the User Data portion. The total size of a concatenated message block shall not exceed 1 megabyte (1,048,575 bytes) unless n-layer pass through is being invoked. When n-layer pass through is invoked without S/R, the total size of a concatenated message block shall not exceed 3283 octets. Any message using n-layer pass through exceeding this limit shall be segmented using the S/R protocol.

5.8 Processing factors.

5.8.1 Application process.

The application process shall provide the application layer the bit-oriented or character-oriented messages that satisfy information exchange requirements.

5.8.2 Message formats.

The message formats shall be user-defined. The UMF field in the application layer header specifies the message format that is being used in the application process.

5.8.3 Lower layer interactions.

Several application layer fields are used to indicate a desire for special handling or quality of service (QOS) from the lower layer protocols. The lower layer protocols should use these indications as guidance for providing the requested service.

5.8.3.1 Security classification.

This application layer field as described in TABLE VIII provides the desired guidance to the lower layers for establishing security classification.

5.8.3.2 Message precedence.

This application layer field as described in TABLE VII provides the desired guidance to the lower layers for setting message transmission precedence.

5.8.3.3 Quality of service (QOS).

The QOS desired by the application layer is derived from multiple fields: Message Size, Message Precedence, Originator DTG, Time Perishability DTG, and Machine Acknowledgment Request Indicator. The following QOS parameters are mapped from these application layer fields:

a. Normal/High Throughput

b. Normal/Low Delay

c. Normal/High Reliability

These QOS parameters are based on the following conditions:

```
IF (Time Perishability DTG - Originator DTG) <= Perish
        AND Precedence <> Routine
THEN Delay = Low
ELSIF (Time Perishability DTG - Originator DTG) > Perish
        AND Message Acknowledgment Indicator = 1
        AND Message Size >= Message Size Threshold
THEN Reliability = High
ELSIF Message Size >= Message Size Threshold
        AND Delay = Normal
        AND Reliability = Normal
THEN Throughput = High
ELSE Delay = Normal
        AND Throughput = Normal
        AND Reliability = Normal
ENDIF
```

where:

Message Size Threshold has a default value of (3*480 = 1440) bytes. Message Size Threshold shall be a parameter with a range of 1 to 1,048,575 bytes.

Perish shall be a parameter with a range of 1 to 10800 seconds.

5.8.3.4 Originator address Group.

This application layer group as described in 5.6.3 provides guidance to the lower layers for the originator address.

5.8.3.5 Recipient address Group.

This application layer group as described in 5.6.3 provides guidance to the lower layers for the destination address.

5.8.3.6 Message broadcast indicators.

The absence of a Recipient Address group and the absence of an Information Address group as described in 5.6.3 provides guidance to the lower layers for broadcast options.

5.8.3.7 Destination port number.

The port named “mil-2045-47001” has been registered with the Internet Assigned Number Authority and has been assigned port number 1581 (decimal) to indicate the MIL-STD-2045-47001 ALP as defined by this standard. This “mil-2045-47001” port shall be passed as the destination port parameter value to the lower layer protocol (e.g., UDP, TCP, or S/R) when exchanging UMF defined in TABLE IV. If n-layer pass through is invoked without S/R, the next lower layer is the intranet layer and destination port number is not required.

6 NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Subject term (key word) listing.

The following key words and phrases apply to this MIL-STD.

Application Header
Application Layer
CANTCO
CANTPRO
CNR
Combat Network Radio
DOI-103
Link 16
Message
MIL-STD-2045-47001
MIL-STD-6016
NITFS
S/R
SEP
Security Extension Protocol
Segmentation/Reassembly
TADIL J
TIDP-TE
USMTF
VMF

6.2 Issue of the DoD index of specifications and standards (DODISS).

When this military standard is used in procurement, the applicable issue of the DoDISS will be cited in the solicitation.

6.3 Management of TCP Connections.

When TCP is used to transport the MIL-STD-2045-47001 ALP over low baud rate combat network radio (CNR) networks, the overhead for opening and closing connections can contribute substantially to the offered load presented to the CNR network. The following conventions for the management of TCP connections used to transport the ALP are offered to allow the amount of overhead generated as the result of opening and closing TCP connections to be controlled.

a. When a MIL-STD-2045-47001 message becomes available for transport, a TCP connection will be opened to the destination if a connection to the destination hasn't already been established.

b. An established TCP connection to a given destination will be gracefully closed if no activity (transmitted or received data) occurs on the connection within some configurable time period of the most recent activity on that connection.

c. If a connection already exists to a given destination and an additional connection offer is received from the same destination, the older connection will be closed at the end of the normal completion of any pending message transports such that only one connection is maintained and utilized for each destination.

d. MIL-STD-2045-47001 messages will be offered for transport over the TCP connection to the specified destination in the order established by the Message Precedence field of the MIL-STD-2045-47001 Application Header. If a higher priority message becomes available for transport to a destination while a lower priority message is in the process of being transported to the same destination, the transport of the higher priority message will begin immediately after the transport of the lower priority message is completed. Lower priority messages that have not already been offered for transport on the connection should not be offered for transport until after higher priority messages have been offered for transport on the connection.

e. The number of connections/destinations that can be utilized simultaneously by a single MIL-STD-2045-47001 application should be limited to a configurable number. Once this limit is reached there are two reasons additional connection might need to be established: either a message becomes available locally for transport to an additional destination, or a connection offer is received from a new remote source.

   (1) In the case of a locally generated message to an additional destination, the Least Recently Active (LRA) connection, that is not currently being used for the transport of messages, should be closed prior to the establishment of a connection to the new destination. If all connections are actively being used, then the new message transport request should be discarded and treated as a transport failure.

   (2) In the case that a connection offer is accepted from an additional remote source, the LRA connection that is not currently being used for the transport of messages should be closed. If all connections are actively being used, then the new recently accepted connection should be abruptly closed. Abruptly closing the newly accepted connection will terminate any pending transmissions from the remote source and inform the remote source that any pending messages were not transported successfully.

APPENDIX A.

APPLICATION HEADER FIELDS AND CODES FOR VMF

A.1 General.

A.1.1 Scope.

This appendix contains definition of the VMF codes and values for application header fields that are dependent on the setting of the UMF field.

A.1.2 Application.

This appendix is conditional based on the setting of the UMF field as indicated in 5.6.4 and TABLE IV of this standard. If the UMF field is set to "2" (VMF), this appendix is mandatory for application headers pertaining to VMF messages. For all other settings of UMF field, this appendix is optional.

A.2 Applicable Documents.

GOVERNMENT STANDARDS

None.

OTHER GOVERNMENT DOCUMENTS

VMF TIDP-TE	DoD Interface Standard, Variable Message Format Technical Interface Design Plan-Test Edition

A.3 Codeword tables.

A.3.1 Unit reference number codewords.

The VMF codes for the URN field shall be in accordance with the VMF TIDP-TE.

A.3.2 FAD codewords.

The VMF codes for the FAD field are defined in TABLE XIV. The FAD field is defined in 5.6.5 of this document. The combination of the FAD field and the Message Number field shall point to the message number that appears in the Message Descriptions of the VMF TIDP-TE. For example, if the UMF = 2 (VMF K-Series), FAD = 7 (Combat Service Support), and Message Number = 1 (Medical Evacuation Request), then this corresponds to message number K07.1, in the 'Message and Purpose Table' of the VMF TIDP-TE.

TABLE XIV. FAD codewords

Functional Area	Code MSB - LSB
Network Control	0000 (0)
General Information Exchange	0001 (1)
Fire Support Operations	0010 (2)
Air Operations	0011 (3)
Intelligence Operations	0100 (4)
Land Combat Operations	0101 (5)
Maritime Operations	0110 (6)
Combat Service Support	0111 (7)
Special Operations	1000 (8)
JTF Operations Control	1001 (9)
Air Defense/Air Space Control	1010 (10)
Undefined	1011-1111 (11–15)

A.3.3 Message number codewords.

The VMF codes for the Message number field are listed in the VMF TIDP-TE. The Message number field is defined in Message number field (see 5.6.6) of this document.

A.3.4 Message subtype codewords.

The VMF codes for the Message subtype field are listed in TABLE XV. The Message subtype field is defined in 5.6.7 of this document. The combination of the FAD field (see 5.6.5), the Message number field (see 5.6.6) and the Message subtype field (see 5.6.7) identifies a specific case within a multi-purpose message.

A.3.4.1 VMF TIDP-TE message cases as messages subtypes.

Case statements define the rules for the preparation of each message for transmission and/or reception. These statements include the specific function of a message, its purpose(s), and the conditions for the use of data groups and data elements within that message. Cases for each VMF message variant are found in the VMF TIDP-TE, K-Series Message Formats Message Processing section of the parent message.

TABLE XV. VMF TIDP-TE message subtypes

Message Subtype Case Number	**Code** MSB - LSB
No Cases	0000000 (0)
Case 1.1	0000001 (1)
Case 1.2	0000010 (2)
Case 1.3	0000011 (3)
Case 1.4	0000100 (4)
Case 1.5	0000101 (5)
Case 1.6	0000110 (6)
Case 1.7	0000111 (7)
Case 1.8	0001000 (8)
Case 1.9	0001001 (9)
Case 1.10	0001010 (10)
Case 1.11	0001011 (11)
Case 1.12	0001100 (12)
Case 1.13	0001101 (13)
Case 1.14	0001110 (14)
Case 1.15	0001111 (15)
Case 1.16	0010000 (16)
Case 1.17	0010001 (17)
Case 1.18	0010010 (18)
Case 1.19	0010011 (19)

TABLE XV. VMF TIDP-TE message subtypes (Continued)

Message Subtype Case Number	Code MSB - LSB
Case 1.20	0010100 (20)
Case 1.21	0010101 (21)
Case 1.22	0010110 (22)
Case 1.23	0010111 (23)
Case 1.24	0011000 (24)
Case 1.25	0011001 (25)
Undefined	0011010 – 1111111 (26 – 127)

A.3.5 CANTCO reason codewords.

The VMF codes for the CANTCO Reason field are defined in TABLE XVI. The CANTCO Reason field is defined in 5.6.23 of this document.

TABLE XVI. CANTCO reason codewords

CANTCO reason	Code MSB - LSB
Communications problem	000 (0)
Ammunition problem	001 (1)
Personnel problem	010 (2)
Fuel problem	011 (3)
Terrain/Environment problem	100 (4)
Equipment problem	101 (5)
Tactical Situation problem	110 (6)

TABLE XVI. CANTCO reason codewords
(Continued)

CANTCO reason	Code MSB - LSB
Other	111 (7)

A.3.6 CANTPRO reason codewords.

The VMF codes for the CANTPRO Reason field are defined in TABLE XVII. The CANTPRO Reason field is defined in 5.6.24 of this document.

TABLE XVII. CANTPRO reason codes

CANTPRO Reason	Code MSB - LSB
Undefined	000000 (0)
Field content invalid	000001 (1)
Message incorrectly routed	000010 (2)
Address inactive	000011 (3)
Reference point unknown to receiving agency	000100 (4)
Fire units shall be controlled by receiving agency	000101 (5)
Mission shall be controlled by receiving agency	000110 (6)
Mission number unknown by receiving agency	000111 (7)
Target number unknown by receiving agency	001000 (8)
Schedule number unknown by receiving agency	001001 (9)
Incorrect controlling address for a given track number	001010 (10)
Track number not in own track file	001011 (11)
Invalid according to given field	001100 (12)
Message cannot be converted	001101 (13)

TABLE XVII. CANTPRO reason codes (Continued)

CANTPRO Reason	Code MSB - LSB
Agency file full	001110 (14)
Agency does not recognize this message number	001111 (15)
Agency cannot correlate message to current file content	010000 (16)
Agency limit exceeded on repeated fields or groups	010001 (17)
Agency computer system inactive	010010 (18)
Addressee unknown	010011 (19)
Can't forward (agency failure)	010100 (20)
Can't forward (link failure)	010101 (21)
Illogical juxtaposition of header fields	010110 (22)
Cannot uncompress Unix (LZW) compressed data	010111 (23)
Cannot uncompress LZ-77 compressed data	011000 (24)
Message too old, based on Perishability	011001 (25)
Security level restriction	011010 (26)
Authentication Failure	011011 (27)
Certificate not found	011100 (28)
Certificate invalid	011101 (29)
Do not support this SPI value	011110 (30)
Can not generate a signed acknowledgement	011111 (31)
Undefined	100000-111111 (32 – 63)

A.3.7 Data field construction procedures for VMF messages/user Data.

The following construction procedures prescribe the sequence in which the message fields are linearly joined to create the user data. The message is constructed with elemental data fields ordered as specified in the message

descriptions provided in the VMF TIDP-TE. The data elements for the messages are also as specified in the VMF TIDP-TE. There are two representations for data elements: 7-bit ANSI ASCII characters and binary numbers. All fields shall be joined LSB first. The LSB of the first data field or field/group indicator shall be LSB-justified within the first byte of the message buffer. The LSB of each successive data field or field/group indicator shall be the LSB of the user data shown in Figure 2 of this document. The characters in a literal field are joined such that the LSB of the first character immediately follows the MSB of the previous field. The LSB of the second character immediately follows the MSB of the first character. This pattern is repeated until all characters of the field are joined.

APPENDIX B.

EXAMPLE OF APPLICATION LAYER PDU AND VMF MESSAGE CONSTRUCTION

B.1 General.

B.1.1 Scope.

This appendix provides examples illustrating the construction of the Application Layer PDU and VMF Message data buffers (or streams).

B.1.2 Application.

This appendix is not a mandatory part of MIL-STD-2045-47001. The information contained herein is preliminary and intended for guidance only.

B.2 Example application layer PDU construction.

This section provides an example illustrating the construction of the Application Layer PDU data buffer (or stream).

B.2.1 Application layer data exchange.

The relationship of the Application Layer to other communication layers is shown in Figure 3. A layered communication model is used in this example for consistency with the principles of the ISO OSI reference model. The model discussed here is tailored to focus attention specifically on the Application Layer, and the data it produces. A user of the Application Layer exchanges user data with its peer at another node by sending and receiving the User Data via the Application Layer. The Application Layer sends and receives the User Data transparently by producing and exchanging an Application Layer PDU with its peer at another node. The Application Layer PDU consists of the Application Header concatenated with the User Data, and is sent and received via lower communication layers. The lower communication layers send and receive the User Data transparently over a variety of communications media.

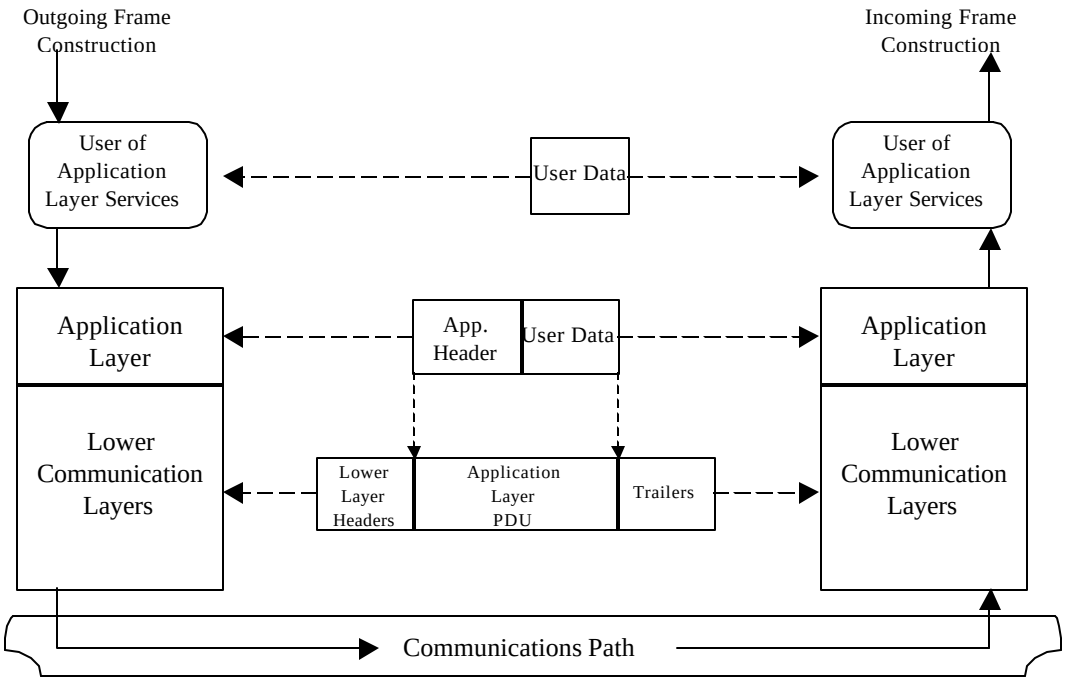

Figure 3. Application layer interaction with other communications layers

The format of the Application Layer PDU is defined in terms of the actual data buffer or data stream used to exchange the PDU between the Application Layer and the lower communication layers. The rationale for using the PDU's data buffer/stream to define the format is 1) for consistency with industry standard commercial communications hardware and software (e.g., UNIX implementations of TCP/IP), which exchange data with other software when sending or receiving as a buffer or stream of octets; 2) to provide a definition independent of the specifics of any other communication layer, consistent with the ISO OSI model principle of making communication layers independent; and 3) to avoid differences in the bit representations used to implement communications on different media. For example, on Ethernet LAN media each octet is sent LSB first, but on FDDI media each octet is sent MSB first. To achieve a universal definition of the PDU format, its representation is defined independent of the other communication layers. The relationship of the Application Layer PDU's data buffer/stream to the Application Layer is depicted in Figure 4. The Application Layer PDU is defined as a buffer or stream of octets. The rational for treating the PDU as a series of octets is for consistency with the way communications data is handled by industry standard commercial communications hardware and software and for independence from platform-dependent byte ordering issues. The Application Header and the User Data are each individually defined as a series of octets for the same reasons.

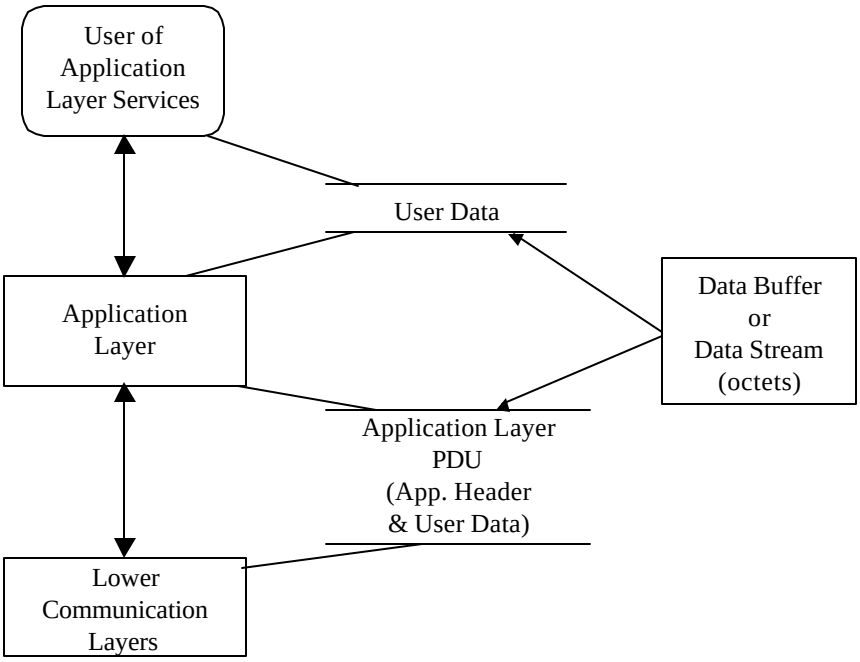

Figure 4. Exchange of application layer PDU between communications layers

B.2.2 Example.

The construction of an Application Layer PDU is illustrated by the example in TABLE XVIII. The first four columns of the table provide a description of each field in the example, the field length in bits, and the value of the field in both decimal and binary representations. The last four columns show the physical encoding of the Application Layer PDU. In the fifth column, Field Fragments, the bits of each field are placed in octets. The bit(s) of each field are positioned in an octet such that the LSB of the field is positioned in the least significant unencoded bit of the octet, the next LSB of the field is placed in the next least significant unencoded bit of the octet, and repeated until all of the bits of the field have been encoded. When an octet is filled before all the bits of a field are encoded, the process is continued encoding the next octet with the remaining bits of the field. This field/octet encoding procedure is performed starting with the first field and octet, and repeated for each successive field and individual octet, in order, until the encoding is completed. When a field has groups, the field encoding procedure is performed starting with the first group, and repeated for each successive group and individual octet, in order, until the encoding of the field is completed. The Unit Name field illustrates the encoding of a field with groups. Note the LSB of a field or octet is defined as the bit having the weight of 2^0 when the field or octet is represented as a numeric value. X's are used to identify bits that are not associated with the field being encoded. The sixth column, Octet Value - Binary, assembles the bits contributed by successive fields into complete octets, represented in binary. The seventh column, Octet Value - Hexadecimal, represents the octet value in hexadecimal. The last column, Octet Number, numbers the octets from first to last starting with 0.

When all fields have been encoded, any remaining unencoded bits in the last octet are filled with zeroes (zero padded). The Application Header is individually encoded and zero padded. The User Data is individually encoded and zero padded before it is passed to the Application Layer to have the Application Header added.

Unit Name is a variable length field. It can be terminated either with an end of text marker, or by using the maximum number of bits. In this example, the field is terminated with the Application Header end of text marker, the ANSI ASCII Delete character.

The Application Header is followed by the User Data. The User Data is shown as a single 10-octet message to complete the Application Layer PDU.

TABLE XVIII. Example construction of application layer PDU

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
Application Header							
Version	4	1	0001	XXXX0001			
FPI	1	0	0	XXX0XXXX			
Data Compression Type	2	NA					
GPI for Originator Address	1	1	1	XX1XXXXX			
FPI for URN	1	1	1	X1XXXXXX			
URN	24	207	000000000000000011001111	1XXXXXXX	11100001	E1	0
				01100111	01100111	67	1
				00000000	00000000	00	2
				X0000000			
FPI for Unit Name	1	1	1	1XXXXXXX	10000000	80	3
Unit Name (Note 1)	448 max	UNITA					
	7	85	1010101	X1010101			
	7	78	1001110	0XXXXXXX	01010101	55	4
				XX100111			
	7	73	1001001	01XXXXXX	01100111	67	5
				XXX10010			
	7	84	1010100	100XXXXX	10010010	92	6
				XXXX1010			
	7	65	1000001	0001XXXX	00011010	1A	7
				XXXXX100			
End of text marker (ANSI ASCII DEL)	7	127	1111111	11111XXX	11111100	FC	8
				XXXXXX11			
GPI for Recipient Address Group	1	1	1	XXXXX1XX			
GRI for R1	1	0	0	XXXX0XXX			
FPI for URN	1	1	1	XXX1XXXX			
URN	24	3	000000000000000000000011	011XXXXX	01110111	77	9
				00000000	00000000	00	10
				00000000	00000000	00	11
				XXX00000			
FPI for Unit Name	1	0	0	XX0XXXXX			
Unit Name	448	NA					
GPI for Information Address Group	1	0	0	X0XXXXXX			

TABLE XVIII. Example construction of application layer PDU (Continued)

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
GRI for R2	1	NA					
FPI for URN	1	NA					
URN	24	NA					
FPI for Unit Name	1	NA					
Unit Name	448	NA					
FPI for Header Size	1	0	0	0XXXXXXX	00000000	00	12
Header Size	16	NA					
GRI for R3	1	0	0	XXXXXXX0			
UMF	4	2	0010	XXX0010X			
FPI for Message Standard Version	1	NA					
Message Standard Version	4	NA					
GPI for Message Identification Group	1	1	1	XX1XXXXX			
FAD	4	2	0010	10XXXXXX	10100100	A4	13
				XXXXXX00			
Message Number	7	1	0000001	000001XX	00000100	04	14
				XXXXXXX0			
FPI for Message Subtype	1	0	0	XXXXXX0X			
Message Subtype	7	NA					
FPI for File Name	1	0	0	XXXXX0XX			
File Name	448	NA					
FPI for Message Size	1	0	0	XXXX0XXX			
Message Size	20	NA					
Operation Indicator	2	1	01	XX01XXXX			
Retransmit Indicator	1	0	0	X0XXXXXX			
Message Precedence Codes	3	2	010	0XXXXXXX	00010000	10	15
				XXXXXX01			
Security Classification	2	0	00	XXXX00XX			
FPI for Control/Release Marking	1	0	0	XXX0XXXX			
Control/Release Marking	224	NA					
GPI for Originator DTG	1	1	1	XX1XXXXX			
Year	7	96	1100000	00XXXXXX	00100001	21	16
				XXX11000			
Month	4	7	0111	111XXXXX	11111000	F8	17
				XXXXXXX0			
Day	5	3	00011	XX00011X			
Hour	5	16	10000	00XXXXXX	00000110	06	18

TABLE XVIII. Example construction of application layer PDU (Continued)

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
				XXXXX100			
Minute	6	27	011011	11011XXX	11011100	DC	19
				XXXXXXX0			
Second	6	55	110111	X110111X			
FPI for DTG Extension	1	0	0	0XXXXXXX	01101110	6E	20
DTG Extension	12	NA					
GPI for Perishability DTG	1	0	0	XXXXXXX0			
Year	7	NA					
Month	4	NA					
Day	5	NA					
Hour	5	NA					
Minute	6	NA					
Second	6	NA					
GPI for Acknowledgment Request Group	1	1	1	XXXXXX1X			
Machine Acknowledge Request Indicator	1	1	1	XXXXX1XX			
Operator Acknowledge Request Indicator	1	0	0	XXXX0XXX			
Operator Reply Request Indicator	1	0	0	XXX0XXXX			
GPI for Response Data Group	1	0	0	XX0XXXXX			
Year	7	NA					
Month	4	NA					
Day	5	NA					
Hour	5	NA					
Minute	6	NA					
Second	6	NA					
FPI for DTG Extension	1	NA					
DTG Extension	12	NA					
R/C	3	NA					
FPI for CANTCO Reason Code	1	NA					
CANTCO Reason Code	3	NA					
FPI for CANTPRO Reason Code	1	NA					
CANTPRO Reason Code	6	NA					
FPI for Reply Amplification	1	NA					

TABLE XVIII. Example construction of application layer PDU (Continued)

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
Reply Amplification	350	NA					
FPI for Reference Message Data Group	1	0	0	X0XXXXXX			
GRI	1	NA					
FPI for URN	1	NA					
URN	24	NA					
FPI for Unit Name	1	NA					
Unit Name	448	NA					
Year	7	NA					
Month	4	NA					
Day	5	NA					
Hour	6	NA					
Minute	6	NA					
Second	6	NA					
FPI for DTG Extension	1	NA					
DTG Extension	12	NA					
FAD	4	NA					
Message Number	7	NA					
GPI for Message Security Group	1	0	0 (If the GPI is zero you can't send the other GPI's)	0XXXXXXX	00000110	06	21
Security Parameters Information	4	NA	NA				
GPI for Keying Material Group	1	NA					
Keying Material ID Length	3	NA					
Keying Material ID	64	NA					
GPI for Cryptographic Initialization Group	1	NA					
Cryptographic Initialization Length	4	NA					
Cryptographic Initialization	1024	NA					
GPI for Key Token Group	1	NA					
Key Token Length	8	NA					
FRI	1	NA					
Key Token	16384	NA					
GPI for Authentication Data (A) Group	1	NA					

TABLE XVIII. Example construction of application layer PDU (Continued)

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
Authentication Data (A) Length	7	NA					
Authentication Data (A)	8192	NA					
GPI for Authentication Data (B) Group	1	NA					
Authentication Data (B) Length	7	NA					
Authentication Data (B)	8192	NA					
Signed Acknowledge Request Indicator	1	NA					
GPI for Message Security Padding Group	1	NA					
Message Security Padding Length	8	NA	NA				
FPI for Message Security Padding	1	NA	NA				
Message Security Padding	2040	NA	NA				
(Zero Padding)							21
User Data							
Message 1	10*8						22-31

Note 1: One and only one of the fields Unit Name and URN are to be present. Unit Name is shown present only for illustrative purposes, and is incorrectly shown with the URN also present.

B.3 Example VMF message construction.

This section provides an example illustrating the construction of the VMF Message data buffer (or stream).

B.3.1 VMF message data exchange.

The relationship of the VMF Messaging Services to other communication layers is shown in Figure 5. A layered communication model is used in this example for consistency with the principles of the ISO OSI reference model. The model discussed here is tailored to focus attention specifically on VMF Messaging Services, and the data it produces. A user of VMF Messaging Services exchanges Message Content with its peer at another node by sending and receiving the Message Content via the VMF Messaging Services. VMF Messaging Services sends and receives the Message Content by converting the Message Content to Message Data and exchanging the Message Data with its peer at another node. The VMF Message Data is sent and received via lower communication layers. The lower communication layers send and receive the VMF Message Data transparently over a variety of communications media. Note that VMF Messaging Services would ordinarily use Application Layer services from the lower communication layers to send and receive Message Data. The Message Data would then appear in the Application Layer PDU's User Data field.

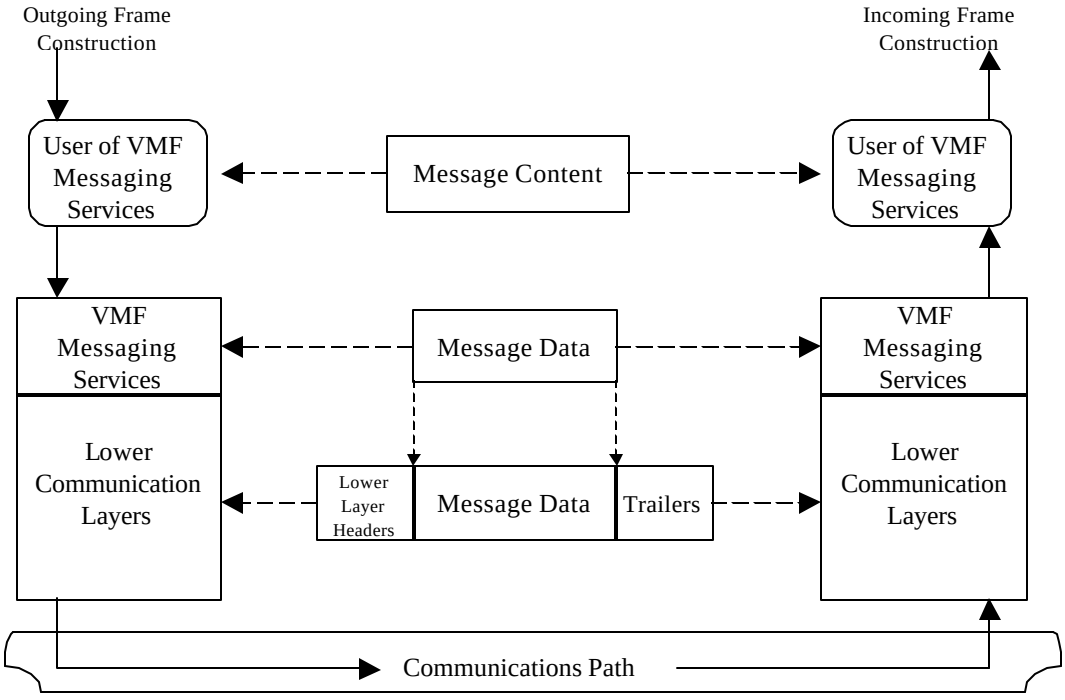

Figure 5. VMF message services interaction with other communications layers

The format of the Message Data is defined in terms of the actual data buffer or data stream used to exchange the Message Data between the VMF Messaging Services and the lower communication layers. The rationale for using the Message Data's data buffer/stream to define the format is 1) for consistency with industry standard commercial communications hardware and software (e.g., UNIX implementations of TCP/IP), which exchange data with other software when sending or receiving as a buffer or stream of octets;

2) to provide a definition independent of the specifics of any other communication layer, consis tent with the ISO OSI model principle of making communication layers independent; and 3) to avoid differences in the bit representations used to implement communications on different media. For example, on Ethernet LAN media each octet is sent LSB first, but on FDDI media each octet is sent MSB first. To achieve a universal definition of the Message Data format, its representation is defined independent of the other communication layers. The relationship of the Message Data's data buffer/stream to the VM F Messaging Services is depicted in Figure 6. The Message Data is defined as a buffer or stream of octets. The rational for treating the Message Data as a series of octets is for consistency with the way communications data is handled by industry standard commercial communications hardware and software and for independence from platform-dependent byte ordering issues.

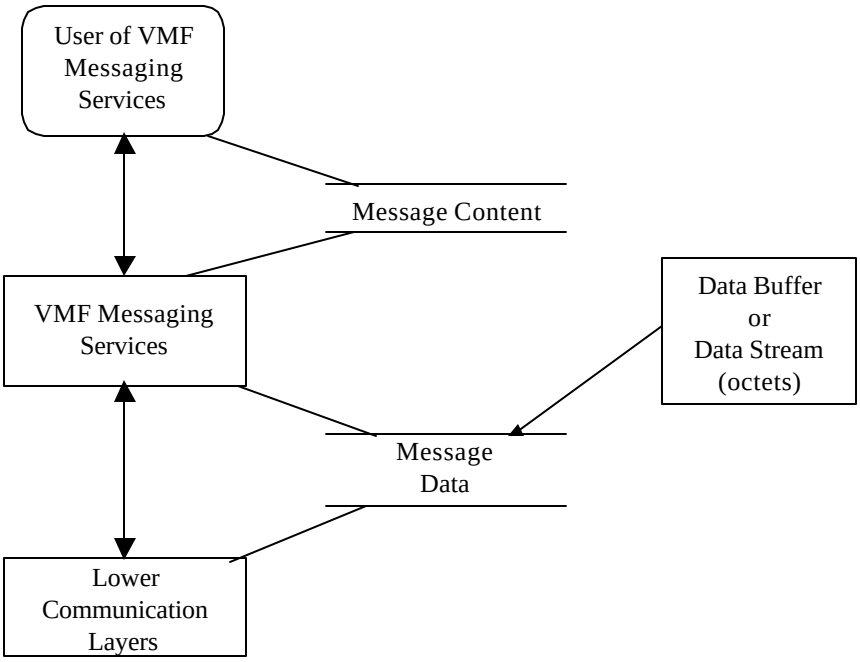

Figure 6. Exchange of message data between communications layers

B.3.2 Example.

The construction of VMF Message Data is illustrated by the example in TABLE XIX. The first four columns of the table provide a description of each field in the example, the field length in bits, and the value of the field in both decimal and binary representations. The last four columns show the physical encoding of the VMF Message Data. In the fifth column, Field Fragments, the bits of each field are placed in octets. The bit(s) of each field are positioned in an octet such that the LSB of the field is positioned in the least significant unencoded bit of the octet, the next LSB of the field is placed in the next least significant unencoded bit of the octet, and repeated until all of the bits of the field have been encoded. When an octet is filled before all the bits of a field are encoded, the process is continued encoding the next octet with the remaining bits of the field. This field/octet encoding procedure is performed starting with the first field and octet, and repeated for each successive field and individual octet, in order, until the encoding is completed. When a field has groups, the field encoding procedure is performed starting with the first group, and

repeated for each successive group and individual octet, in order, until the encoding of the field is completed. The Target Number field illustrates the encoding of a field with groups. Note the LSB of a field or octet is defined as the bit having the weight of 2^0 when the field or octet is represented as a numeric value. X's are used to identify bits that are not associated with the field being encoded. The sixth column, Octet Value - Binary, assembles the bits contributed by successive fields into complete octets, represented in binary. The seventh column, Octet Value - Hexadecimal, represents the octet value in hexadecimal. The last column, Octet Number, numbers the octets from first to last starting with 0.

When all fields have been encoded, any remaining unencoded bits in the last octet are filled with zeroes (zero padded). Each VMF Message is individually encoded and zero padded.

TABLE XIX. Example construction of VMF message data
(Sample message is from the VMF TIDP-TE, Reissue 4, July 2000)

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
Check Fire Type	3	0	000	XXXXX000			
Check Fire/Cancel Check Fire Command	3	1	001	XX001XXX			
FPI	1	1	1	X1XXXXXX			
Target Number (AB0031)	28						
		65 (A)	1000001	1XXXXXXX	11001000	C8	1
				XX100000			
		66 (B)	1000010	10XXXXXX	10100000	A0	2
				XXX10000			
		31	00000000011111	111XXXXX	11110000	F0	3
				00000011	00000011	03	4
				XXXXX000			
FPI (Observer ID)	1	0	0	XXXX0XXX			
URN (Observer ID)	24	NA					
GPI (Effective Time)	1	0	0	XXX0XXXX			
Effective Hour	5	NA					
Effective Minute	6	NA					
Effective Second	6	NA					
FPI	1	0	0	XX0XXXXX			
Launcher Message Sequencing Number	7	NA					
GPI (Entity ID Reference Group)	1	0	0	X0XXXXXX			
URN	24	NA					
Entity ID Serial Number	32	NA					
Day of Month	5	NA					
Hour	5	NA					
Minute	6	NA					
Second	6	NA					
(Zero Padding)	1	0	0	0XXXXXXX	00000000	00	5

APPENDIX C.

SEGMENTATION/REASSEMBLY PROTOCOL

C.1 General.

C.1.1 Scope.

Segmentation/reassembly (S/R) is a protocol intended for use with certain military applications. Data transfers larger than the maximum segment size (MSS) permitted shall be segmented and reassembled in accordance with the procedures set forth in the following paragraphs. Data transfers that are smaller than the MSS do not require S/R and do not carry the S/R header unless an end-to-end acknowledgment is required.

C.1.2 Application.

This appendix is a mandatory part of MIL-STD-2045-47001. The segmentation and reassembly protocol shall be supported within end systems.

C.2 Applicable Documents.

RFC 791	Internet Protocol -- DARPA Internet Protocol Specification
RFC 896	User Datagram Protocol
RFC 1122	Requirements for Internet Hosts -- Communication Layers

C.3 Overall operation.

The data transfers, which are larger than the designated MSS, shall be segmented by the source device prior to transmission, and reassembled at the destination device prior to delivery to the application. An end-to-end acknowledgment shall be employed to ensure reliable delivery of all segments in a connectionless transport environment.

C.3.1 Maximum segment size (MSS).

The MSS shall be calculated using the equation below with the following variables as defined.

MMTU	:	Maximum Message Transfer Unit size
SH	:	S/R header size
UDP	:	UDP header size
IP	:	IP header size
IL	:	Intranet layer header size

MSS = MMTU - (SH + UDP + IP) for IP datagrams; and

MSS = MMTU – (SH + IL + LL) for n-layer pass through

C.3.1.1 MSS for IP datagram exchanges.

It is desirable that IP datagrams, which will be transmitted across multiple subnetworks, do not exceed 576 octets. A MSS of 496 octets will assure that IP fragmentation will not occur at IP router/gateway devices. The following components take on maximized constant values based on the definitions provided within this appendix:

SH = 12 octets
UDP = 8 octets
IP = 60 octets

Thus: MSS = 576 – (12 + 8 + 60) = 496

C.3.1.2 MSS for n-layer pass through exchanges.

Since neither UDP nor IP are present with n-layer pass through, IP fragmentation is not a concern. Therefore the only limitation on size is based on maximum transmission size allowed by link layer. For n-layer pass through, the following components take on the maximized constant values provided below.

SH = 12 octets
IL = 50 octets

Thus: MSS = 3345 – (12 + 50) = 3283 octets

Although the MSS for n-layer pass through is 3283 octets, the recommended MSS value for n-layer pass through is 564 (576-12) octets. If a value larger than 564 is utilized, the assumptions made to help establish the MIL-STD-188-220 Protocol Parameter Values utilized to insure interoperability will be violated resulting in speed of service degradation and possible failure to communicate. The Protocol Parameter Values established are based on limiting the transmission times of each station. MSS values larger than 564 octets for MIL-STD-188-220 n-layer pass through would not be consistent with the Protocol Parameter Values because the maximum transmission times would be exceeded at some transmission bit rates.

Note: S/R should be used for messages being sent via MIL-STD-188-220 n-layer pass through that exceed 576 octets.

C.3.2 End-to-end acknowledgment.

A partial acknowledgment scheme shall be employed in which correctly received segments are acknowledged, even if all segments comprising a data transfer have not been received. Every data segment shall contain a last segment number from which the destination device may estimate the time required to receive all segments of a given data transfer. A receive timer is set during which the receiving unit is waiting for the expected segments of a data transfer to be arrived correctly. When this timer expires, all segments correctly received shall be acknowledged through a bit map in the S/R header. Upon successful receipt of all segments, the data transfer shall be reassembled and transferred

to the application layer. The source device shall only retransmit those segments that the receiver indicates are missing (via Partial Acknowledgment).

C.3.3 Interface with other layers.

The S/R protocol interfaces with the ALP and the protocol in the next layer down, which is either the UDP in the Transport Layer or the intranet layer header if n-layer pass through is invoked.

C.3.3.1 IP Datagram exchanges.

The parameters exchanged in the service interface between S/R and upper layer protocols that utilize S/R, are the same as the parameters exchanged in the service interface between UDP and the upper layer protocols that utilize UDP. Two of the interface parameters that the S/R service interface has in common with UDP are the source and destination ports. The source and destination port parameters provided in the S/R service interface shall be placed in corresponding Source Port and Destination Port fields of the S/R header. The port named “udp-sr-port” has been registered with the Internet Assigned Number Authority and assigned port number 1624 (decimal) to indicate S/R protocol as defined by this standard. When the S/R protocol layer invokes the UDP service interface the destination port parameter value should be set to “udp-sr-port” and the source port parameter value should be set to the same port number parameter value specified by the upper layer protocol when invoking S/R protocol service interface. Note that if an upper layer protocol were to invoke the UDP service interface directly, instead of utilizing the S/R service interface, the source and destination port number parameters would have the same values as the parameters provided by the upper layer when invoking the S/R protocol service interface.

C.3.3.2 N-layer pass through exchanges.

The parameters exchanged in the service interface between S/R and the upper layer protocols that utilize S/R are the same as the parameters that would have been exchanged if UDP and IP were utilized. The source and destination port parameters provided in the S/R service interface from the upper layer protocol shall be placed in the corresponding Source Port and Destination Port fields of the S/R header. Port 1581 as defined in paragraph 5.8.3.7 of this standard shall be used to indicate MIL-STD-2045-47001 as an ALP when S/R is used with n-layer pass through. If n-layer pass through with S/R is used with an ALP other than MIL-STD-2045-47001, use the respective port number for the ALP. The service parameters and values associated with the interface between S/R and the Intranet Header are described in MIL-STD-188-220C and include the Unitdata Request primitive parameters and the Unitdata Indications primitive parameters.

C.3.4 Source device procedures (segmentation).

All data transfers received from the application which exceed the MSS shall be segmented. The data transfer is segmented and a S/R header is appended to each segment. A serial number shall be assigned and copied into the header of each segment of that data transfer. Each information segment is then sequentially sent starting with segment number equal to 1. The originator shall indicate in the segmentation header whether the data transfer requires an end-to-end acknowledgment (Type field = 000) or does not require an end-to-end acknowledgment (Type field = 010). A retransmission timer shall be used for segment retransmission when end-to-end acknowledgment is invoked. If the retransmission timer expires without the receipt of at least a partial acknowledgment, an

Acknowledgment Request shall be issued to the recipient requesting for segments acknowledgment status. If no response to the Acknowledgment Request, the source device shall resend the Acknowledgment Request. If no response to the Acknowledgment Request after N number of tries, the data transfer shall be aborted and an error indication shall be returned to the upper layer process or application. If no end-to-end-acknowledgment is needed the originator shall assume the transmission completed successfully when the retransmission timer expires.

C.3.5 Destination device procedures (reassembly).

Upon receipt of a segment of a new data transfer, the recipient shall set an accumulation timer during which it expects to receive coming segments from the sender. If the accumulation timer expires before receiving all expected segments, a partial Acknowledgment (100) shall be sent to the sender indicating in the segment Acknowledgment bit map which segments of the data transfer have been received correctly. Otherwise, the timer shall be stopped. For a data transfer which requires an end-to-end acknowledgment, a Partial Acknowledgment or a Complete Acknowledgment shall be sent to the sender when all expected segments of the data transfer have been received correctly.

The recipient shall accumulate segments of a data transfer with the same serial number from the same source IP address and reassemble that data transfer when all segments have been successfully received, using segment numbers to indicate segment position relative to the whole data transfer. S/R headers shall be removed. The whole data transfer is then passed to the upper layer process indicated by the port number.

C.4 S/R PDU Format.

C.4.1 Common S/R Header.

Figure 7 depicts the S/R header that precedes all PDUs defined in this appendix.

C.4.1.1 Source port.

This 16-bit port number identifies the application process that is sending the Application PDU that is being transported by S/R. Its value is established by Source Port parameter passed in the S/R service interface send request at the sending system.

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td>Type</td><td>HLEN</td><td>P/F</td><td>Serial Number</td></tr>
</table>

Figure 7. Segmentation/Reassembly header

C.4.1.2 Destination port.

This 16-bit port number identifies the application process that will receive the Application PDU that is being transported by S/R. Its value is established by Destination Port parameter passed in the S/R service interface send request at the sending system.

C.4.1.3 Type.

This field identifies the type of header in use in accordance with the three-bit sequences below.

Bits	Decimal Value	Interpretation
000	0	End-to-end Acknowledgment required
010	2	End-to-end Acknowledgment not required
100	4	Partial Acknowledgment
110	6	Complete Acknowledgment
001	1	Abort Request
101	5	Abort Confirm
011	3	Acknowledgment request
111	7	Undefined

C.4.1.4 Header length (HLEN).

This 12-bit field indicates the total length of the S/R header in 32-bit words.

C.4.1.5 Poll/Final (P/F).

This 1-bit field is used to request an immediate response.

a. When a Data segment is received with the P/F bit set to “1”, the receiving unit shall immediately respond with a Partial Acknowledgment or a Complete Acknowledgment with P/F bit set to “1”.

b. When an Abort Request segment is received with the P/F bit set to “1”, the receiving unit shall immediately return an Abort Confirm segment with P/F bit set to “1”.

C.4.1.6 Serial number.

This 16-bit number is assigned by the originating device and uniquely identifies the data transfer of which this segment forms a part.

C.4.2 Data segment.

Data transfers that are larger than the MSS are segmented and sent to the destination addressee as the data portion of the Data segment. The length of the data portion shall be the same for all segments of a data transfer except for the last segment, which may be shorter. Two types of Data segments may be used by the source addressee to indicate whether end-to-end acknowledgment is required or not required. If end-to-end acknowledgment is used by the sending addressee, the destination addressee shall respond with a complete Acknowledgment after correctly receiving all segments of a data transfer. The format of the Data segment is shown in the Figure 8.

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td>Type</td><td>HLEN</td><td>P/F</td><td>Serial Number</td></tr>
<tr><td colspan="3">Segment Number</td><td>Last Segment Number</td></tr>
<tr><td colspan="4">Data Portion</td></tr>
</table>

Type = 000 or 010

Figure 8. Data segment

Where:

Source Port:	16 bits
Destination Port:	16 bits
Type:	03 bits
HLEN:	12 bits
P/F:	01 bit
Serial Number:	16 bits
Segment Number:	16 bits
Last Segment Number:	16 bits

C.4.2.1 Segment number.

This 16-bit number identifies the segment's position in the whole data transfer and is assigned by the originating device. It is used by the receiving unit in the reassembly process.

C.4.2.2 Last segment number.

This 16-bit number indicates the total number of segments in the data transfer identified by the serial number.

C.4.3 Partial acknowledgment.

A Partial Acknowledgment is used by the recipient to inform the originator of which segments have been received. The format of the Partial Acknowledgment segment is shown in Figure 9.

<table>
<tr><td colspan="3">Source Port</td><td colspan="2">Destination Port</td></tr>
<tr><td>Type</td><td>HLEN</td><td>P/F</td><td colspan="2">Serial Number</td></tr>
<tr><td colspan="3">Starting Segment No.</td><td>Bit Map</td><td>Padded</td></tr>
</table>

Type = 100

Figure 9. Partial acknowledgement segment

Where:

Source Port:	16 bits
Destination Port:	16 bits
Type:	03 bits
HLEN:	12 bits
P/F:	01 bit
Serial Number:	16 bits
Starting Segment Number:	16 bits
Bit Map:	1 - variable bits
Padded:	0 - 31 bits

C.4.3.1 Starting segment number.

This 16-bit number indicates that all segments prior to this number have been successfully received in sequence.

C.4.3.2 Acknowledgment segments bitmap.

The bits in this field are used to indicate which segments of a data transfer have been successfully received at the receiving unit. A bit set (binary 1) means the segment has been correctly received. Binary “0” indicates the segment was not correctly received. These bits are relative to the Starting Segment Number. The first (most-significant) bit of this field corresponds to the Starting Segment Number and will always set to “0”. The last (least significant) bit of this field shall set to binary “1” to indicate the last segment that has been received correctly. This field is extensible in 32-bit increments. Unused bits added to pad the field to a 32-bit boundary shall be set to “0”.

C.4.4 Complete acknowledgment segment.

The Complete Acknowledgment segment is used by the destination addressee to inform the source device that all segments of a data transfer associated with the serial number were received correctly. No data field shall be permitted with the Complete Acknowledgment. The format of the Complete Acknowledgment segment is shown in Figure 10 below.

Source Port			Destination Port
Type	HLEN	P/F	Serial Number

Type = 110

Figure 10. Complete acknowledgement segment

Where:

Source Port:	16 bits
Destination Port:	16 bits
Type:	03 bits
HLEN:	12 bits
P/F:	01 bit
Serial Number:	16 bits

C.4.5 Abort request.

The Abort Request shall be used to abort the transfer of a data transfer. Either the data transfer originator or its recipient may initiate the abort action. No data field shall be permitted with the Abort Request. All segments associated with the Serial Number shall be discarded. The format of the Abort Request / Confirm is shown in Figure 11.

Source Port			Destination Port
Type	HLEN	P/F	Serial Number

Type = 001 or 101

Figure 11. Abort request/confirm segment

Where:

Source Port:	16 bits
Destination Port:	16 bits
Type:	03 bits
HLEN:	12 bits
P/F:	01 bit
Serial Number:	16 bits

C.4.6 Abort confirm.

After receiving an Abort Request, the receiving addressee shall confirm its acceptance of the abort by transmitting an Abort Confirm. No data field shall be permitted with the Abort Confirm. All segments, which have the same Serial Number as identified in the Abort Request, previously received shall be discarded.

C.4.7 **Acknowledgment request.**

An Acknowledgment Request shall be used by the data transfer originator to request the acknowledgment status of all previous transmitted Data segments. Upon receiving an Acknowledgment Request, the receiver shall return a Partial Acknowledgment to the sender. The format of the Acknowledgment Request is shown in Figure 12.

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td>Type</td><td>HLEN</td><td>P/F</td><td>Serial Number</td></tr>
<tr><td colspan="3">Last Sent Segment No.</td><td>Padded</td></tr>
</table>

Type = 011

Figure 12. Acknowledgement request segment

Where:

Source Port:	16 bits
Destination Port:	16 bits
Type:	03 bits
HLEN:	12 bits
P/F:	01 bit
Serial Number:	16 bits
Last Sent Segment Number:	16 bits
Padded:	16 bits

C.4.7.1 Last sent segment number.

This 16-bit number is used in the Acknowledgment Request segment to indicate the highest segment number that had been sent at the time of the Acknowledgment Request segment is issued.

APPENDIX D.

SECURITY EXTENSION PROTOCOL

D.1 General.

D.1.1 Scope.

This appendix provides a description of the features and values associated with each SPI code currently defined in TABLE XI.

D.1.2 Application.

This appendix is a mandatory part of MIL-STD-2045-47001. The information contained herein is for conformance.

D.2 Applicable Documents.

GOVERNMENT STANDARDS

None.

D.3 Definitions.

Refer to Section 3 of this standard.

D.4 General Requirements.

D.4.1 SPI 0 authentication using SHA-1 and DSA/no encryption.

The SEP implementation, SPI field “0000”, is designed to provide message authentication for the MIL-STD-2045-47001 application header and associated user data. Security services provided by this SEP implementation include: 1) Data origin authentication; 2) Connectionless integrity; 3) Non-repudiation with proof of origin (message signature); and 4) Non-repudiation with proof of delivery (signed acknowledgment). This implementation does not provide confidentiality. Confidentiality is a security service that protects information from unauthorized disclosure through the use of data encryption.

D.4.1.1 Message security group.

The Message Security Group shall consist of the fields in TABLE XX when Case 6, condition 13 and expected response 5.7.3.4 apply. This example depicts the construction of a response message to an originator who requested a signed acknowledgement. The values of the Authentication Data (A) and Authentication Data (B) are values which are dependent upon the message content and signature keys of the sender and can not be specified in this example. Values which can not be determined are denoted with “ND”. For the sake of simplicity it was assumed that the portion of application header proceeding Group 10, was a multiple of 8 bits, so that G10 would start a new octet.

TABLE XX. Example construction of the SEP data

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
GPI for Message Security Group	1	1	1	XXXXXXX1			
Security Parameters Information	4	0	0000	XXX0000X			
GPI for Keying Material Group	1	0	0	XX0XXXXX			
Keying Material ID Length	3	NA					
Keying Material ID	64	NA					
GPI for Cryptographic Initialization Group	1	0	0	X0XXXXXX			
Cryptographic Initialization Length	4	NA					
Cryptographic Initialization	1024	NA					
GPI for Key Token Group	1	0	0	0XXXXXXX	00000001	01	1
Key Token Length	8	NA					
FRI	1	NA					
Key Token	16384	NA					
GPI for Authentication Data (A) Group	1	1	1	XXXXXXX1			
Authentication Data (A) Length	7	4	0000100	0000100X	00001001	09	2
Authentication Data (A) (Note 1)	320	ND	10001011	11001000	11001000	C8	3
			10101100	11011000	11011000	D8	4
			00011010	11011100	11011100	DC	5
			10110110	10110110	10110110	B6	6
			01100100	00101101	00101101	2D	7
			00010000	10111010	10111010	BA	8
			01000011	10110100	10110100	B4	9
			01011100	01010101	01010101	55	10
			10110111	11010001	11010001	D1	11
			00011000	00100110	00100110	26	12
			00011111	11110100	11110100	F4	13
			10010101	01011000	01011000	58	14
			10110001	00100100	00100100	24	15

TABLE XX. Example construction of the SEP data (Continued)

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
			01101010	11011111	11011111	DF	16
			10111001	01010110	01010110	56	17
			01111100	00011111	00011111	1F	18
			10010010	01011111	01011111	5F	19
			10110011	00110100	00110100	34	20
			01000001	11100010	11100010	E2	21
			11000000	01000001	01000001	41	22
			01000001	11000000	11000000	C0	23
			11100010	01000001	01000001	41	24
			00110100	10110011	10110011	B3	25
			01011111	10010010	10010010	92	26
			00011111	01111100	01111100	7C	27
			01010110	10111001	10111001	B9	28
			11011111	01101010	01101010	6A	29
			00100100	10110001	10110001	B1	30
			01011000	10010101	10010101	95	31
			11110100	00011111	00011111	1F	32
			00100110	00011000	00011000	18	33
			11010001	10110111	10110111	B7	34
			01010101	01011100	01011100	5C	35
			10110100	01000011	01000011	43	36
			10111010	00010000	00010000	10	37
			00101101	01100100	01100100	64	38
			10110110	10110110	10110110	B6	39
			11011100	00011010	00011010	1A	40
			11011000	10101100	10101100	AC	41
			11001000	10001011	10001011	8B	42
GPI for Authentication Data (B) Group	1	1	1	XXXXXXX1			
Authentication Data (B) Length	7	4	0000100	0000100X	00001001	09	43
Authentication Data (B) (Note 1)	320	ND	10001011	11001000	11001000	C8	44
			10101100	11011000	11011000	D8	45
			00011010	11011100	11011100	DC	46
			10110110	10110110	10110110	B6	47
			01100100	00101101	00101101	2D	48
			00010000	10111010	10111010	BA	49

TABLE XX. Example construction of the SEP data (Continued)

FIELD				OCTET BUFFER/STREAM			
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7 LSB 2^0	OCTET VALUE (Binary) MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET NO
			01000011	10110100	10110100	B4	50
			01011100	01010101	01010101	55	51
			10110111	11010001	11010001	D1	52
			00011000	00100110	00100110	26	53
			00011111	11110100	11110100	F4	54
			10010101	01011000	01011000	58	55
			10110001	00100100	00100100	24	56
			01101010	11011111	11011111	DF	57
			10111001	01010110	01010110	56	58
			01111100	00011111	00011111	1F	59
			10010010	01011111	01011111	5F	60
			10110011	00110100	00110100	34	61
			01000001	11100010	11100010	E2	62
			11000000	01000001	01000001	41	63
			01000001	11000000	11000000	C0	64
			11100010	01000001	01000001	41	65
			00110100	10110011	10110011	B3	66
			01011111	10010010	10010010	92	67
			00011111	01111100	01111100	7C	68
			01010110	10111001	10111001	B9	69
			11011111	01101010	01101010	6A	70
			00100100	10110001	10110001	B1	71
			01011000	10010101	10010101	95	72
			11110100	00011111	00011111	1F	73
			00100110	00011000	00011000	18	74
			11010001	10110111	10110111	B7	75
			01010101	01011100	01011100	5C	76
			10110100	01000011	01000011	43	77
			10111010	00010000	00010000	10	78
			00101101	01100100	01100100	64	79
			10110110	10110110	10110110	B6	80
			11011100	00011010	00011010	1A	81
			11011000	10101100	10101100	AC	82
			11001000	10001011	10001011	8B	83
Signed Acknowledge Request Indicator	1	1	1	XXXXXXX1			
GPI for Message Security Padding Group	1	0	0	XXXXXX0X			

TABLE XX. Example construction of the SEP data (Continued)

FIELD				OCTET BUFFER/STREAM					
TITLE	LENGTH (Bits)	VALUE (Dec)	VALUE (Binary) MSB 2^n LSB 2^0	FIELD FRAGMENTS MSB 2^7	LSB 2^0	OCTET VALUE (Binary) MSB 2^7	LSB 2^0	OCTET VALUE (Hex)	OCTET NO
Message Security Padding Length	8	NA	NA						
FPI for Message Security Padding	1	NA	NA						
Message Security Padding	2040	NA	NA						

Note 1 - The values in these fields are based upon random numbers generated at the time the signature is created. It is not therefore possible to determine the actual values which would be placed in these fields. For illustrative purposes, we have chosen the values (r and s) found in Appendix 5 of FIPS 186-2.

D.4.1.1.1 Security parameters information.

The Security Parameters Information (SPI) is set to “0” to identify the SEP-0 implementation.

D.4.1.1.2 Keying material ID length.

Confidentiality is not provided therefore Keying Material ID is not present.

D.4.1.1.3 Cryptographic initialization length.

Confidentiality is not provided therefore Cryptographic Initialization is not present.

D.4.1.1.4 Key token length.

Confidentiality is not provided therefore key tokens are not present.

D.4.1.1.5 Authentication data (A).

The Authentication Data (A) field provides for data origin authentication, connectionless integrity and non-repudiation with proof of origin. It is generated by digitally signing the hash of both the application header and user data. The signature algorithm is the DSA. The hashing algorithm is SHA-1. All values of the application header are hashed except for the 320-bit signature value. The input to the hash starts with the LSB of the first field of the application header. This corresponds with the header version field. It ends with the last byte of the uncompressed user message. When multiple user messages are present, a signature is calculated for each user message by digitally signing the hash of the application header and that particular instance of the user message.

D.4.1.1.6 Authentication data (B).

The Authentication Data (B) field provides for non-repudiation with proof of delivery (signed acknowledgment). It is generated by digitally signing the hash of both the application header and user data of the message being acknowledged. In this case the signature of the originator is included within the hash calculation. The signature algorithm is the DSA. The hashing algorithm is SHA-1. The input to the hash starts with the LSB of the first field of the original application header. This corresponds with the header version field. It ends with the last byte of the uncompressed original user data.

D.4.1.1.7 Signed acknowledge request indicator.

This field is set to “1” when the message originator is requesting a signed acknowledgment from the recipient.

D.4.1.1.8 Message security padding.

Confidentiality is not provided therefore GPI for message security padding is “0” (not present).

APPENDIX E.

DoD Standardized Profile Implementation Conformance Statements (DSPICS) Requirements List (DPRL) for MIL-STD-2045-47001C

E.1 General.

This appendix provides the DoD Standardized Profile Implementation Conformance Statements (DSPICS) Requirements List (DPRL) for MIL-STD-2045-47001C for implementations of Combat Net Radios. An implementation's completed DPRL is called the DSPICS. THE DSPICS states which capabilities and options have been implemented.

The main part of this appendix is a fixed-format questionnaire indexed into a number of major sub-clauses; these can be divided into further sub-clauses each containing a group of individual items. Answers to the questionnaire items are to be provided in the Support column by simply marking an answer (i.e., by check the applicable entry) to indicate a restricted choice (Yes, or No) or by entering a value or a range of values.

The structure of the DSPICS questionnaire consists of 7 main sections:

(1) Pre-Application Header Requirements
(2) MIL-STD-2045-47001C, Table I, Application Header
(3) Post Application Header Receipt Requirements
(4) Cases
(5) Conditions
(6) Expected Response Requirements
(7) Special Considerations
(8) Segmentation/Reassembly Protocol

An item number in the first column identifies each item. The second column contains the field name, statement of function, or the question to be answered. The third column contains the reference to the material that specifies the item in the main body of the standard. The fourth column records the status of the item – whether support is mandatory, optional, prohibited or conditional and fifth column for answers. The last column is to be used to list comments by their numerical endnote designator.

An implementer shows the extent of compliance by completing the DPRL. That is, compliance to all mandatory requirements and the options that are not supported are shown. If a conditional requirement is inapplicable, use the "No" choice. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference note in the Notes column, to an accompanying rationale for the noncompliance.

E.1.1 Scope.

This appendix contains the minimum set of MIL-STD-2045-47001 features required for joint interoperability. It is intended to guide system developers and users. The following can use the DSPICS:

a. The protocol implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight

b. The supplier and acquirer or potential acquirer of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard DSPICS performa

c. The user or potential user of the implementation, as a basis for initially checking the possibility of the inter-working with another implementation (note that, while inter-working can never be guaranteed, failure to inter-work can often be predicted from incompatible DSPICSs)

d. A protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

E.1.2 Application.

This appendix is a mandatory part of MIL-STD-2045-47001. This information contained herein is intended as guidance for system developers and users.

E.2 Applicable documents.

None.

E.3 Notation.

The following notations and symbols are used in the DPRL to indicate the status of features:

STATUS SYMBOL

M	Mandatory. A field which shall contain data with each transmission of the Application Header.
M.<n>	Support of every item of the group labeled by the same numeral <n> required, but only one is active at a time.
O	Optional. A field which is not designated as a mandatory field. An optional field shall be preceded by an FPI or be nested within a group which includes a GPI.
O.<n>	Optional, <n> is the number of optional selections.
P	Item Number
P:O.<n>	Parent item number of this option and number of options related to the parent when there is more than one.
C	Conditional. Condition statements defined the conditions under which a data group, data element, or value in a data element may be used. The condition statement is very structured in its use.
E	Mutually Exclusive. One or another field specified must occur, but not both.
-	***Not applicable (i.e., logically impossible in the scope of the profile.) (Not actually used yet. This code maybe deleted later.)***
X	Excluded or prohibited.
i	Out of scope of profile (left as an implementation choice)

The O.<n> notation is used to show a set of selectable options (i.e., one or more of the set must be implemented) with the same identifier <n>.

NOTATIONS FOR CONDITIONAL STATUS

<predicate>::	This notation introduces a group of items, all of which are conditional on <predicate>.
<predicate>:	This notation introduces a single item, which is conditional on <predicate>.
<index>:	This predicate symbol means that the status following it applies only when the DSPICS states that the features identified by the index are supported. In the simplest case, <index> is the identifying tag of a single DSPICS item. The symbol <index> also may be a Boolean expression composed of several indices.
<index>::	When this group predicate is true, the associated clause should be completed.

In each case, the predicate may identify a profile feature, or a Boolean combination of predicates. ("^" is the symbol for logical negation.)

SUPPORT COLUMN SYMBOLS

Yes	Supported by the implementation.
No	Not supported by the implementation.
-	Not applicable
The support of every item as claimed by the implementer is stated by checking the appropriate answer (Yes or No) in the support column.	

E.4 Implementation requirements.

This appendix categorizes requirements, identified by MIL-STD-2045-47001 paragraph numbers, as Mandatory, Conditional or Optional. Unless otherwise specified, the category assigned to a requirement applies to all subordinate subparagraphs for the requirement. Fully compliant systems shall implement all mandatory and conditional requirements. Minimally compliant systems shall implement all mandatory requirements and some conditional requirements as described in this appendix.

E.5 Detailed requirements.

TABLE XXI. Pre-Application header requirements

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
1.1	Application Layer	5.1	NA		
1.1.2	Application PDU in accordance with Figure 1.	5.2	M M	Yes ___ ___ No ___ ___	
1.1.3	Application Header in accordance with Table I.	5.3	M M	Yes ___ ___ No ___ ___	
1.1.3.1	Shall be in multiples of 8 bits. If necessary zero fill.	5.3	M M	Yes ___ ___ No ___ ___	
1.1.4	Application Header Formatting in	5.4	M M	Yes ___ ___ No ___ ___	

TABLE XXI. Pre-Application header requirements (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
	accordance with variable format syntax and format structure.				
1.1.5	Syntax, the following fields shall be used:	5.5	M M	Yes ___ ___ No ___ ___	
1.1.5.1	Field Presence Indicator (FPI)	5.5.1	1.1.5:M	Yes ___ ___ No ___ ___	
1.1.5.2	Field Recurrence Indicator (FRI)	5.5.2	1.1.5:M	Yes ___ ___ No ___ ___	
1.1.5.3	Group Presence Indicator (GPI)	5.5.3	1.1.5:M	Yes ___ ___ No ___ ___	
1.1.5.4	Group Recurrence Indicator (GRI)	5.5.4	1.1.5:M	Yes ___ ___ No ___ ___	
1.1.5.5	End-of-Literal Field Marker	5.5.5	M M	Yes ___ ___ No ___ ___	
1.1.5.6	Data-Field Construction Procedures	5.5.6	M M	Yes ___ ___ No ___ ___	
1.1.5.6.1	All fields shall be joined LSB first.	5.5.6	M M	Yes ___ ___ No ___ ___	
1.1.5.6.2	The LSB of each successive data field shall be concatenated to the MSB of the preceding data field.	5.5.6	M M	Yes ___ ___ No ___ ___	
1.1.5.6.3	ASCII Data Element	5.5.6.1	M M	Yes ___ ___ No ___ ___	
1.1.5.6.4	Binary Data Element	5.5.6.2	M M	Yes ___ ___ No ___ ___	
1.1.5.6.5	Header Format Notations	5.5.6.3	M M	Yes ___ ___ No ___ ___	
1.1.6	Application Header Formatting Rules and Construction Procedures	5.7	M M	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.1	VERSION	5.6.1 5.7.4.2	M M	Yes ___ ___ No ___ ___	
2.1.a	MIL-STD-2045-47001	5.6.1	2.1:O.<4>	Yes ___ ___ No ___ ___	
2.1.b	MIL-STD-2045-47001B	5.6.1	2.1:O.<4>	Yes ___ ___ No ___ ___	
2.1.c	MIL-STD-2045-47001C	5.6.1	2.1:O.<4>	Yes ___ ___ No ___ ___	
2.1.d	VERSION SENT NOT IMPLEMENTED	5.6.1 5.7.4.2	2.1:O.<4>	Yes ___ ___ No ___ ___	
2.2	FPI	5.5.1 5.7.2.1.2 5.7.2.1.5 5.7.4.2 5.7.4.10	M M	Yes ___ ___ No ___ ___	
2.2.a	NOT PRESENT	5.5.1	2.2:M.<2>	Yes ___ ___ No ___ ___	
2.2.b	PRESENT	5.5.1	2.2:M.<2>	Yes ___ ___ No ___ ___	
2.2.1	DATA COMPRESSION TYPE	5.6.2	O M	Yes ___ ___ No ___ ___	
2.2.1.a	LZW	5.5.6.2	2.2.1:O	Yes ___ ___ No ___ ___	
2.2.1.b	LZ-77	5.6.2	2.2.1:M	Yes ___ ___ No ___ ___	
2.3	GPI FOR G1 (ORIGINATOR ADDRESS GROUP)	5.5.3 5.6.3 5.7.2.1.2 5.7.2.2.1 5.7.4.2 5.7.4.6	M M	Yes ___ ___ No ___ ___	
2.3.a	NOT PRESENT	5.5.3	2.3:M.<2>	Yes ___ ___ No ___ ___	
2.3.b	PRESENT	5.5.3	2.3:M.<2>	Yes ___ ___ No ___ ___	
2.3.1	FPI	5.5.1 5.7.2.2.2 5.7.2.2.5	2.3:M	Yes ___ ___ No ___ ___	
2.3.1.a	NOT PRESENT	5.5.1	2.3.1:M.<2>	Yes ___ ___ No ___ ___	
2.3.1.b	PRESENT	5.5.1	2.3.1:M.<2>	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.3.1.1	URN	5.6.3.1	2.3.1.b:M 2.3.2.b:E	Yes ___ ___ No ___ ___	
2.3.2	FPI	5.5.1 5.7.2.2.3 5.7.2.2.4	2.3:M	Yes ___ ___ No ___ ___	
2.3.2.a	NOT PRESENT	5.5.1	2.3.2:M.<2>	Yes ___ ___ No ___ ___	
2.3.2.b	PRESENT	5.5.1	2.3.2:M.<2>	Yes ___ ___ No ___ ___	
2.3.2.1	UNIT NAME	5.6.3.2	2.3.2.b:M 2.3.1.b:E	Yes ___ ___ No ___ ___	
2.4	GPI FOR G2 (RECIPIENT ADDRESS GROUP)	5.5.3 5.6.3 5.7.2.1.2 5.7.4.2 5.7.4.3 5.7.4.6	M M	Yes ___ ___ No ___ ___	
2.4.a	NOT PRESENT	5.5.3	2.4:M.<2>	Yes ___ ___ No ___ ___	
2.4.b	PRESENT	5.5.3	2.4:M.<2>	Yes ___ ___ No ___ ___	
2.4.1.1	GRI FOR R1 (0<N<=16)	5.5.4 5.7.2.1.2	2.4.b:M	Yes ___ ___ No ___ ___	
2.4.1.1.a	NOT REPEATED	5.5.4	2.4.1.1:M.<2>	Yes ___ ___ No ___ ___	
2.4.1.1.b	REPEATED	5.5.4	2.4.1.1:M.<2>	Yes ___ ___ No ___ ___	
2.4.1.1.1	The recipient and information addressee fields shall be extendible to a combined total of 16 addressees.	5.6.3.a.	2.4.1.1:M	Yes ___ ___ No ___ ___	
2.4.1.2	FPI	5.5.1 5.7.2.2.2 5.7.2.2.5	O M	Yes ___ ___ No ___ ___	
2.4.1.2.a	NOT PRESENT	5.5.1	2.4.1.2:M.<2>	Yes ___ ___ No ___ ___	
2.4.1.2.b	PRESENT	5.5.1	2.4.1.2:M.<2>	Yes ___ ___ No ___ ___	
2.4.1.2.1	URN	5.6.3.1	2.4.1.2.b:M 2.4.1.3.1:E	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.4.1.3	FPI	5.5.1 5.7.2.2.3 5.7.2.2.4	O M	Yes ___ ___ No ___ ___	
2.4.1.3.a	NOT PRESENT	5.5.1	2.4.1.3:M.<2>	Yes ___ ___ No ___ ___	
2.4.1.3.b	PRESENT	5.5.1	2.4.1.3:M.<2>	Yes ___ ___ No ___ ___	
2.4.1.3.1	UNIT NAME	5.6.3.2	2.4.1.3.b:M 2.4.1.2.1:E	Yes ___ ___ No ___ ___	
2.5	GPI FOR G3 (INFORMATION ADDRESS GROUP)	5.5.3 5.6.3 5.7.2.1.2 5.7.4.3 5.7.4.6	M M	Yes ___ ___ No ___ ___	
2.5.a	NOT PRESENT	5.5.3	2.5:M.<2>	Yes ___ ___ No ___ ___	
2.5.b	PRESENT	5.5.3	2.5:M.<2>	Yes ___ ___ No ___ ___	
2.5.1.1	GRI FOR R2 (16 – N)	5.5.4	2.5.b:M	Yes ___ ___ No ___ ___	
2.5.1.1.a	NOT REPEATED	5.5.4	2.5.1.1:M.<2>	Yes ___ ___ No ___ ___	
2.5.1.1.b	REPEATED	5.5.4	2.5.1.1:M.<2>	Yes ___ ___ No ___ ___	
2.5.1.1.1	The recipient and information addressee fields shall be extendible to a combined total of 16 addressees.	5.6.3a.	2.5.1.1:M	Yes ___ ___ No ___ ___	
2.5.1.2	FPI	5.5.1 5.7.2.2.2 5.7.2.2.5	O M	Yes ___ ___ No ___ ___	
2.5.1.2.a	NOT PRESENT	5.5.1	2.5.1.2:M.<2>	Yes ___ ___ No ___ ___	
2.5.1.2.b	PRESENT	5.5.1	2.5.1.2:M.<2>	Yes ___ ___ No ___ ___	
2.5.1.2.1	URN	5.6.3.1	2.5.1.2.b:M 2.5.1.3.1:E	Yes ___ ___ No ___ ___	
2.5.1.3	FPI	5.5.1 5.7.2.2.3 5.7.2.2.4	O M	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.5.1.3.a	NOT PRESENT	5.5.1	2.5.1.3:M.<2>	Yes ___ ___ No ___ ___	
2.5.1.3.b	PRESENT	5.5.1	2.5.1.3:M.<2>	Yes ___ ___ No ___ ___	
2.5.1.3.1	UNIT NAME	5.6.3.2	2.5.1.3.b:M 2.5.1.2.1:E	Yes ___ ___ No ___ ___	
2.6	FPI	5.5.1	M M	Yes ___ ___ No ___ ___	
2.6.a	NOT PRESENT	5.5.1	2.6:M.<2>	Yes ___ ___ No ___ ___	
2.6.b	PRESENT	5.5.1	2.6:M.<2>	Yes ___ ___ No ___ ___	
2.6.1	HEADER SIZE	5.6.27 5.7.2.2.7 5.7.4.5 5.7.4.6	2.6.b:M 6.5:M 6.6:M 6.12:M	Yes ___ ___ No ___ ___	
2.7.1	GRI FOR R3 (MESSAGE HANDLING GROUP) (16)	5.5.4 5.6.9 5.7.2.1.2 5.7.2.2.7 5.7.4.5 5.7.4.6	M M	Yes ___ ___ No ___ ___	
2.7.1.a	NOT REPEATED	5.5.4	2.7.1:M.<2>	Yes ___ ___ No ___ ___	
2.7.1.b	REPEATED	5.5.4	2.7.1:M.<2>	Yes ___ ___ No ___ ___	
2.7.2	UMF	5.6.4	M M	Yes ___ ___ No ___ ___	
2.7.2.a	LINK 16 (J-SERIES)	5.6.4	2.7.2:O.<9>	Yes ___ ___ No ___ ___	
2.7.2.b	BINARY FILE	5.6.4.1 5.7.2.1.3	2.7.2:O.<9>	Yes ___ ___ No ___ ___	
2.7.2.c	VARIABLE MESSAGE FORMAT (VMF) (K-SERIES)	5.6.4	2.7.2:O.<9>	Yes ___ ___ No ___ ___	
2.7.2.d	NATIONAL IMAGERY TRANSMISSION FORMAT SYSTEM (NITFS)	5.6.4	2.7.2:O.<9>	Yes ___ ___ No ___ ___	
2.7.2.e	FORWARDED MESSAGE	5.6.4.2 5.7.2.1.4	2.7.2:O.<9>	Yes ___ ___ No ___ ___	
2.7.2.f	UNITED STATES MESSAGE TEXT FORMAT (USMTF)	5.6.4.3	2.7.2:O.<9>	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.2.g	DOI-103	5.6.4.4	2.7.2:O.<7>	Yes ___ ___ No ___ ___	
2.7.2.h	XML-MTF	5.6.4.5	2.7.2:O.<9>	Yes ___ ___ No ___ ___	
2.7.2.i	XML-VMF	5.6.4.6	2.7.2:O.<9>	Yes ___ ___ No ___ ___	
2.7.3	FPI	5.5.1	M M	Yes ___ ___ No ___ ___	
2.7.3.a	NOT PRESENT	5.5.1	2.7.3:M.<2>	Yes ___ ___ No ___ ___	
2.7.3.b	PRESENT	5.5.1	2.7.3:M.<2>	Yes ___ ___ No ___ ___	
2.7.3.1	MESSAGE STANDARD VERSION	5.6.4.5	2.7.3.b:M	Yes ___ ___ No ___ ___	
2.7.4	GPI FOR G4 (MESSAGE IDENTIFICATION GROUP)	5.5.3 5.7.2.1.2 5.7.2.1.3	2.7.2.c:M	Yes ___ ___ No ___ ___	
2.7.4.a	NOT PRESENT	5.5.3	2.7.4:M.<2>	Yes ___ ___ No ___ ___	
2.7.4.b	PRESENT	5.5.3	2.7.4:M.<2>	Yes ___ ___ No ___ ___	
2.7.4.1	FAD	5.6.5 A.3.2	2.7.2.c:M 2.7.4.b:M	Yes ___ ___ No ___ ___	
2.7.4.2	MESSAGE NUMBER	5.6.6	2.7.2.c:M 2.7.4.b:M	Yes ___ ___ No ___ ___	
2.7.4.3	FPI	5.5.1 5.7.4.7	2.7.2.c:M 2.7.4.1:M 2.7.4.2:M	Yes ___ ___ No ___ ___	
2.7.4.3.a	NOT PRESENT	5.5.1	2.7.4.3:M.<2>	Yes ___ ___ No ___ ___	
2.7.4.3.b	PRESENT	5.5.1	2.7.4.3:M.<2> 2.7.2.c:O 2.7.4.1:O 2.7.4.2:O 6.7:M	Yes ___ ___ No ___ ___	
2.7.4.3.1	MESSAGE SUBTYPE	5.6.7 A.3.4	2.7.4.3.b:M	Yes ___ ___ No ___ ___	
2.7.5	FPI	5.5.1 5.7.2.1.2	M M	Yes ___ ___ No ___ ___	
2.7.5.a	NOT PRESENT	5.5.1	2.7.5:M.<2>	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.5.b	PRESENT	5.5.1	2.7.5:M.<2> 2.7.2.b:O	Yes ___ ___ No ___ ___	
2.7.5.1	FILE NAME	5.6.8	2.7.5.b:M 2.7.2.b:M	Yes ___ ___ No ___ ___	
2.7.6	FPI	5.5.1 5.7.2.1.2 5.7.2.2.7 5.7.4.5 5.7.4.6	2.2:M 2.7.1:M	Yes ___ ___ No ___ ___	
2.7.6.a	NOT PRESENT	5.5.1	2.7.6:M.<2>	Yes ___ ___ No ___ ___	
2.7.6.b	PRESENT	5.5.1	2.7.6:M.<2>	Yes ___ ___ No ___ ___	
2.7.6.1	MESSAGE SIZE	5.6.9 5.7.2.2.7 5.7.4.5 5.7.4.6	2.7.6.b:M 6.5:M 6.6:M 6.12:M	Yes ___ ___ No ___ ___	
2.7.7	OPERATION INDICATOR	5.6.10	M M	Yes ___ ___ No ___ ___	
2.7.8	RETRANSMIT INDICATOR	5.6.11	M M	Yes ___ ___ No ___ ___	
2.7.9	MESSAGE PRECEDENCE CODE	5.6.12	M M	Yes ___ ___ No ___ ___	
2.7.10	SECURITY CLASSIFICATION	5.6.13	M M	Yes ___ ___ No ___ ___	
2.7.11	FPI	5.5.1 5.7.2.1.2	M M	Yes ___ ___ No ___ ___	
2.7.11.a	NOT PRESENT	5.5.1	2.7.11:M.<2>	Yes ___ ___ No ___ ___	
2.7.11.b	PRESENT	5.5.1	2.7.11:M.<2>	Yes ___ ___ No ___ ___	
2.7.11.1	CONTROL/RELEASE MARKING	5.6.14	2.7.11.b:M	Yes ___ ___ No ___ ___	
2.7.12	GPI FOR G5 (ORIGINATOR DTG)	5.5.3 5.6.15 5.7.2.1.2 5.7.2.2.11	M M 2.7.14.1:M 2.7.14.2:M	Yes ___ ___ No ___ ___	
2.7.12.a	NOT PRESENT	5.5.3	2.7.12:M.<2>	Yes ___ ___ No ___ ___	
2.7.12.b	PRESENT	5.5.3	2.7.12:M.<2>	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.12.1	YEAR	5.6.15	2.7.12.b:M	Yes ___ ___ No ___ ___	
2.7.12.2	MONTH	5.6.15	2.7.12.b:M	Yes ___ ___ No ___ ___	
2.7.12.3	DAY	5.6.15	2.7.12.b:M	Yes ___ ___ No ___ ___	
2.7.12.4	HOUR	5.6.15	2.7.12.b:M	Yes ___ ___ No ___ ___	
2.7.12.5	MINUTE	5.6.15	2.7.12.b:M	Yes ___ ___ No ___ ___	
2.7.12.6	SECOND	5.6.15	2.7.12.b:M	Yes ___ ___ No ___ ___	
2.7.12.7	FPI	5.5.1 5.7.4.4	2.7.12.b:M	Yes ___ ___ No ___ ___	
2.7.12.7.a	NOT PRESENT	5.5.1	2.7.12.7:M.<2>	Yes ___ ___ No ___ ___	
2.7.12.7.b	PRESENT	5.5.1	2.7.12.7:M.<2>	Yes ___ ___ No ___ ___	
2.7.12.7.1	DTG EXTENSION	5.6.16	2.7.12.7.b:M	Yes ___ ___ No ___ ___	
2.7.13	GPI FOR G6 (PERISHABILITY DTG)	5.5.3 5.6.17 5.7.2.1.2 5.7.4.1	O M	Yes ___ ___ No ___ ___	
2.7.13.a	NOT PRESENT	5.5.3	2.7.13:M.<2>	Yes ___ ___ No ___ ___	
2.7.13.b	PRESENT	5.5.3	2.7.13:M.<2>	Yes ___ ___ No ___ ___	
2.7.13.1	YEAR	5.6.15	2.7.13.b:M	Yes ___ ___ No ___ ___	
2.7.13.2	MONTH	5.6.15	2.7.13.b:M	Yes ___ ___ No ___ ___	
2.7.13.3	DAY	5.6.15	2.7.13.b:M	Yes ___ ___ No ___ ___	
2.7.13.4	HOUR	5.6.15	2.7.13.b:M	Yes ___ ___ No ___ ___	
2.7.13.5	MINUTE	5.6.15	2.7.13.b:M	Yes ___ ___ No ___ ___	
2.7.13.6	SECOND	5.6.15	2.7.13.b:M	Yes ___ ___ No ___ ___	
2.7.14	GPI FOR G7 (ACKNOWLEDG-MENT REQUEST GROUP)	5.5.3 5.7.2.1.2 5.7.2.2.1	M M	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
		5.7.2.2.14 5.7.2.2.15 5.7.4.8			
2.7.14.a	NOT PRESENT	5.5.3	2.7.14:M.<2>	Yes ___ ___ No ___ ___	
2.7.14.b	PRESENT	5.5.3	2.7.14:M.<2>	Yes ___ ___ No ___ ___	
2.7.14.1	MACHINE ACKNOWLEDGE REQUEST INDICATOR	5.6.18 5.7.2.2.11 5.7.2.2.15 5.7.3.1 5.7.4.1	2.7.14.b:M	Yes ___ ___ No ___ ___	
2.7.14.2	OPERATOR ACKNOWLEDGE REQUEST INDICATOR	5.6.19 5.7.2.2.11 5.7.2.2.15 5.7.3.2	2.7.14.b:M	Yes ___ ___ No ___ ___	
2.7.14.3	OPERATOR REPLY REQUEST INDICATOR	5.6.20 5.7.2.2.11 5.7.3.3	2.7.14.b:M	Yes ___ ___ No ___ ___	
2.7.15	GPI FOR G8 (RESPONSE DATA GROUP)	5.5.3 5.6.21 5.7.2.1.1 5.7.2.1.2 5.7.2.1.5 5.7.4.9	4.1.2:M	Yes ___ ___ No ___ ___	
2.7.15.a	NOT PRESENT	5.5.3	2.7.15:M.<2>	Yes ___ ___ No ___ ___	
2.7.15.b	PRESENT	5.5.3	2.7.15:M.<2>	Yes ___ ___ No ___ ___	
2.7.15.1	YEAR (DTG OF MESSAGE BEING ACKNOWLEDGED)	5.6.15	2.7.15.b:M	Yes ___ ___ No ___ ___	
2.7.15.2	MONTH	5.6.15	2.7.15.b:M	Yes ___ ___ No ___ ___	
2.7.15.3	DAY	5.6.15	2.7.15.b:M	Yes ___ ___ No ___ ___	
2.7.15.4	HOUR	5.6.15	2.7.15.b:M	Yes ___ ___ No ___ ___	
2.7.15.5	MINUTE	5.6.15	2.7.15.b:M	Yes ___ ___ No ___ ___	
2.7.15.6	SECOND	5.6.15	2.7.15.b:M	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.15.7	FPI	5.5.1 5.7.4.9	2.7.15.b:M	Yes ___ ___ No ___ ___	
2.7.15.7.a	NOT PRESENT	5.5.1	2.7.15.7:M.<2>	Yes ___ ___ No ___ ___	
2.7.15.7.b	PRESENT	5.5.1	2.7.15.7:M.<2>	Yes ___ ___ No ___ ___	
2.7.15.7.1	DTG EXTENSION	5.6.16	2.7.15.7.b:M 4.1.2:M 6.8:M	Yes ___ ___ No ___ ___	
2.7.15.8	R/C	5.6.22 5.7.3.1	4.1.2:M	Yes ___ ___ No ___ ___	
2.7.15.8.a	MACHINE RECEIPT [MR]	5.6.22 5.7.2.2.8 5.7.2.2.9	2.7.15.8:M.<6>	Yes ___ ___ No ___ ___	
2.7.15.8.b	CANNOT PROCESS [CANTPRO]	5.6.22 5.7.2.2.8 5.7.3.1 5.7.3.2 5.7.3.3 5.7.3.4 5.7.4.1	2.7.15.8:M.<6>	Yes ___ ___ No ___ ___	
2.7.15.8.c	OPERATOR ACKNOWLEDGE [OPRACK]	5.6.22 5.7.2.2.8 5.7.2.2.9 5.7.3.2	2.7.15.8:M.<6>	Yes ___ ___ No ___ ___	
2.7.15.8.d	WILL COMPLY [WILCO]	5.6.22 5.7.2.2.8 5.7.2.2.9 5.7.3.3	2.7.15.8:M.<6>	Yes ___ ___ No ___ ___	
2.7.15.8.e	HAVE COMPLIED [HAVCO]	5.6.22 5.7.2.2.8 5.7.2.2.9 5.7.3.3	2.7.15.8:M.<6>	Yes ___ ___ No ___ ___	
2.7.15.8.f	CANNOT COMPLY [CANTCO]	5.6.22 5.7.2.2.9 5.7.3.3	2.7.15.8:M.<6>	Yes ___ ___ No ___ ___	
2.7.15.9	FPI	5.5.1	M M	Yes ___ ___ No ___ ___	
2.7.15.9.a	NOT PRESENT	5.5.1	2.7.15.9:M.<2> 4.2.8:M	Yes ___ ___ No ___ ___	
2.7.15.9.b	PRESENT	5.5.1	2.7.15.9:M.<2> 2.7.15.8.f:O	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.15.9.1	CANTCO REASON CODE	5.6.23 5.7.2.2.8 A.3.5	2.7.15.9.b:M	Yes ___ ___ No ___ ___	
2.7.15.9.1.a	COMMUNICATIONS PROBLEM	A.3.5	2.7.15.9.1:O.<8>	Yes ___ ___ No ___ ___	
2.7.15.9.1.b	AMMUNITION PROBLEM	A.3.5	2.7.15.9.1:O.<8>	Yes ___ ___ No ___ ___	
2.7.15.9.1.c	PERSONNEL PROBLEM	A.3.5	2.7.15.9.1:O.<8>	Yes ___ ___ No ___ ___	
2.7.15.9.1.d	FUEL PROBLEM	A.3.5	2.7.15.9.1:O.<8>	Yes ___ ___ No ___ ___	
2.7.15.9.1.e	TERRAIN/ENVIRONMENT PROBLEM	A.3.5	2.7.15.9.1:O.<8>	Yes ___ ___ No ___ ___	
2.7.15.9.1.f	EQUIPMENT PROBLEM	A.3.5	2.7.15.9.1:O.<8>	Yes ___ ___ No ___ ___	
2.7.15.9.1.g	TACTICAL SITUATION PROBLEM	A.3.5	2.7.15.9.1:O.<8>	Yes ___ ___ No ___ ___	
2.7.15.9.1.h	OTHER	A.3.5	2.7.15.9.1:O.<8>	Yes ___ ___ No ___ ___	
2.7.15.10	FPI	5.5.1 5.7.2.2.9	M M	Yes ___ ___ No ___ ___	
2.7.15.10.a	NOT PRESENT	5.5.1	2.7.15.10:M.<2> 4.2.9:M	Yes ___ ___ No ___ ___	
2.7.15.10.b	PRESENT	5.5.1	2.7.15.10:M.<2> 2.7.15.8.b:O	Yes ___ ___ No ___ ___	
2.7.15.10.1	CANTPRO REASON CODE	5.6.24 A.3.6	2.7.15.10.b:M	Yes ___ ___ No ___ ___	
2.7.15.10.1.a	FIELD CONTENT INVALID	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.b	MESSAGE INCORRECTLY ROUTED	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.c	ADDRESS INACTIVE	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.d	REFERENCE POINT UNKNOWN TO RECEIVING AGENCY	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.e	FIRE UNITS SHALL BE CONTROLLED BY RECEIVING AGENCY	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.f	MISSION SHALL BE CONTROLLED BY RECEIVING AGENCY	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.15.10.1.g	MISSION NUMBER UNKNOWN BY RECEIVING AGENCY	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.h	TARGET NUMBER UNKNOWN BY RECEIVING AGENCY	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.i	SCHEDULE NUMBER UNKNOWN BY RECEIVING AGENCY	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.j	INCORRECT CONTROLLING ADDRESS FOR A GIVEN TRACK NUMBER	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.k	TRACK NUMBER NOT IN OWN TRACK FILE	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.l	INVALID ACCORDING TO GIVEN FIELD	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.m	MESSAGE CANNOT BE CONVERTED	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.n	AGENCY FILE FULL	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.o	AGENCY DOES NOT RECOGNIZE THIS MESSAGE NUMBER	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.p	AGENCY CANNOT CORRELATE MESSAGE TO CURRENT FILE CONTENT	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.q	AGENCY LIMIT EXCEEDED ON REPEATED FIELDS OR GROUPS	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.r	AGENCY COMPUTER SYSTEM INACTIVE	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.s	ADDRESSEE UNKNOWN	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.t	CAN'T FORWARD (AGENCY FAILURE)	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.u	CAN'T FORWARD (LINK FAILURE)	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.15.10.1.v	ILLOGICAL JUXTAPOSITION OF HEADER FIELDS	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.w	CANNOT UNCOMPRESS UNIX (LZW) COMPRESSED DATA	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.x	CANNOT UNCOMPRESS LZ-77 COMPRESSED DATA	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.y	MESSAGE TO OLD, BASED ON PERISHABILITY	5.7.4.1 A.3.6	2.7.15.10.1:O.<32> 6.1:M	Yes ___ ___ No ___ ___	
2.7.15.10.1.z	SECURITY LEVEL RESTRICTION	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.aa	AUTHENTICATION FAILURE	5.7.3.4 A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.bb	CERTIFICATE NOT FOUND	5.7.3.4 A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.cc	CERTIFICATE INVALID	5.7.3.4 A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.dd	DO NOT SUPPORT THIS SPI VALUE	5.7.3.4 A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.ee	CAN NOT GENERATE A SIGNED ACKNOWLEDGMENT	5.7.3.4 A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.10.1.ff	RESPONSE NOT AVAILABLE FOR RETRANSMISSION	A.3.6	2.7.15.10.1:O.<32>	Yes ___ ___ No ___ ___	
2.7.15.11	FPI	5.5.1	M M	Yes ___ ___ No ___ ___	
2.7.15.11.a	NOT PRESENT	5.5.1	2.7.15.11:M.<2>	Yes ___ ___ No ___ ___	
2.7.15.11.b	PRESENT	5.5.1	2.7.15.11:M.<2>	Yes ___ ___ No ___ ___	
2.7.15.11.1	REPLY AMPLIFICATION	5.6.25	2.7.15.11.b:M	Yes ___ ___ No ___ ___	
2.7.16	GPI FOR G9 (REFERENCE MESSAGE DATA GROUP)	5.5.3 5.6.26 5.7.2.1.2	M M	Yes ___ ___ No ___ ___	
2.7.16.a	NOT PRESENT	5.5.3	2.7.16:M.<2>	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.16.b	PRESENT	5.5.3	2.7.16:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.1	GRI FOR R4 (4)	5.5.4 5.6.26	2.7.16.b:M	Yes ___ ___ No ___ ___	
2.7.16.1.1.a	NOT REPEATED	5.5.4	2.7.16.1.1:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.1.b	REPEATED	5.5.4	2.7.16.1.1:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.2	FPI	5.5.1 5.7.2.2.2 5.7.2.2.5 5.7.4.11 5.7.4.12	2.7.16.b:M	Yes ___ ___ No ___ ___	
2.7.16.1.2.a	NOT PRESENT	5.5.1	2.7.16.1.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.2.b	PRESENT	5.5.1	2.7.16.1.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.2.1	URN	5.6.3.1	2.7.16.1.2.b:M 2.7.16.1.3.1:E	Yes ___ ___ No ___ ___	
2.7.16.1.3	FPI	5.5.1 5.7.2.2.3 5.7.2.2.4 5.7.4.11 5.7.4.12	2.7.16:M	Yes ___ ___ No ___ ___	
2.7.16.1.3.a	NOT PRESENT	5.5.1	2.7.16.1.3:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.3.b	PRESENT	5.5.1	2.7.16.1.3:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.3.1	UNIT NAME	5.6.3.2	2.7.16.1.3.b:M 2.7.16.1.2.1:E	Yes ___ ___ No ___ ___	
2.7.16.1.4	YEAR	5.6.15	2.7.16.b:M	Yes ___ ___ No ___ ___	
2.7.16.1.5	MONTH	5.6.15	2.7.16.b:M	Yes ___ ___ No ___ ___	
2.7.16.1.6	DAY	5.6.15	2.7.16.b:M	Yes ___ ___ No ___ ___	
2.7.16.1.7	HOUR	5.6.15	2.7.16.b:M	Yes ___ ___ No ___ ___	
2.7.16.1.8	MINUTE	5.6.15	2.7.16.b:M	Yes ___ ___ No ___ ___	
2.7.16.1.9	SECOND	5.6.15	2.7.16.b:M	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.16.1.10	FPI	5.5.1	2.7.16.b:M	Yes ___ ___ No ___ ___	
2.7.16.1.10.a	NOT PRESENT	5.5.1	2.7.16.1.10:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.10.b	PRESENT	5.5.1	2.7.16.1.10:M.<2>	Yes ___ ___ No ___ ___	
2.7.16.1.10.1	DTG EXTENSION	5.6.16	2.7.16.1.10.b:M	Yes ___ ___ No ___ ___	
2.7.17	GPI FOR G10 (MESSAGE SECURITY GROUP)	5.5.3 5.7.2.1.2 5.7.2.1.6 APPEN D	M M	Yes ___ ___ No ___ ___	
2.7.17.a	NOT PRESENT	5.5.3	2.7.17:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.b	PRESENT	5.5.3	2.7.17:M.<2> 4.1.6:M	Yes ___ ___ No ___ ___	
2.7.17.1	SECURITY PARAMETERS INFORMATION	5.6.28 5.7.2.2.13 D.4.1	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.1.a	AUTHENTICATION (USING SHA-1 AND DSA) / NO ENCRYPTION	5.6.28 D.4.1.1.1	2.7.17.1:M	Yes ___ ___ No ___ ___	
2.7.17.2	GPI FOR G11 (KEYING MATERIAL GROUP)	5.5.3 5.7.2.2.13	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.2.a	NOT PRESENT	5.5.3	2.7.17.2:M.<2> 2.7.17.1.a:M	Yes ___ ___ No ___ ___	
2.7.17.2.b	PRESENT	5.5.3	2.7.17.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.2.1	KEYING MATERIAL ID LENGTH	5.6.29 D.4.1.1.2	2.7.17.2.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.2.2	KEYING MATERIAL ID	5.6.30	2.7.17.2.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.3	GPI FOR G12 (CRYPTOGRAPHIC INITIALIZATION GROUP)	5.5.3 5.7.2.2.13	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.3.a	NOT PRESENT	5.5.3	2.7.17.3:M.<2> 2.7.17.1.a:M	Yes ___ ___ No ___ ___	
2.7.17.3.b	PRESENT	5.5.3	2.7.17.3:M.<2>	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.17.3.1	CRYPTOGRAPHIC INITIALIZATION LENGTH	5.6.31 D.4.1.1.3	2.7.17.3.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.3.2	CRYPTOGRAPHIC INITIALIZATION	5.6.32	2.7.17.3.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.4	GPI FOR G13 (KEY TOKEN GROUP)	5.5.3 5.7.2.2.13	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.4.a	NOT PRESENT	5.5.3	2.7.17.4:M.<2> 2.7.17.1.a:M	Yes ___ ___ No ___ ___	
2.7.17.4.b	PRESENT	5.5.3	2.7.17.4:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.4.1	KEY TOKEN LENGTH	5.6.33 D.4.1.1.4	2.7.17.4.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.4.2	FRI (17)	5.5.2	2.3, 2.4, 2.5, 2.7.17.4:C	Yes ___ ___ No ___ ___	
2.7.17.4.2.a	NOT REPEATED	5.5.2	2.7.17.4.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.4.2.b	REPEATED	5.5.2	2.7.17.4.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.4.3	KEY TOKEN	5.6.34	2.7.17.4.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.5	GPI FOR G14 (AUTHENTICATION GROUP (A))	5.5.3 5.7.2.2.13 D.4.1.1.5	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.5.a	NOT PRESENT	5.5.3	2.7.17.5:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.5.b	PRESENT	5.5.3	2.7.17.5:M.<2> 2.7.17.1.a:M	Yes ___ ___ No ___ ___	
2.7.17.5.1	AUTHENTICATION DATA (A) LENGTH	5.6.35	2.7.17.5.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.5.2	AUTHENTICATION DATA (A)	5.6.36	2.7.17.5.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.6	GPI FOR G15 (AUTHENTICATION GROUP (B))	5.5.3 5.7.3.4 D.4.1.1.6	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.6.a	NOT PRESENT	5.5.3	2.7.17.6:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.6.b	PRESENT	5.5.3	2.7.17.6:M.<2> 2.7.17.7:C 2.7.14.b:C	Yes ___ ___ No ___ ___	
2.7.17.6.1	AUTHENTICATION DATA (B) LENGTH	5.6.37	2.7.17.6.b:M	Yes ___ ___ No ___ ___	

TABLE XXII. MIL-STD-2045-47001C application header (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
2.7.17.6.2	AUTHENTICATION DATA (B)	5.6.38	2.7.17.6.b:M	Yes ___ ___ No ___ ___	
2.7.17.7	SIGNED ACKNOWLEDGE REQUEST INDICATOR	5.6.39 0 5.7.2.2.14 5.7.3.4 D.4.1.1.7	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.8	GPI FOR G16 (MESSAGE SECURITY PADDING GROUP)	5.5.3 5.7.2.2.13	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.8.a	NOT PRESENT	5.5.3	2.7.17.8:M.<2> 2.7.17.1.a:M	Yes ___ ___ No ___ ___	
2.7.17.8.b	PRESENT	5.5.3	2.7.17.8:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.8.1	MESSAGE SECURITY PADDING LENGTH	5.6.40	2.7.17.8.b:M	Yes ___ ___ No ___ ___	
2.7.17.8.2	FPI	5.5.1	2.7.17.8.b:M	Yes ___ ___ No ___ ___	
2.7.17.8.2.a	NOT PRESENT	5.5.1	2.7.17.8.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.8.2.b	PRESENT	5.5.1	2.7.17.8.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.8.2.1	MESSAGE SECURITY PADDING	5.6.41 D.4.1.1.8	2.7.17.8.2.b:M	Yes ___ ___ No ___ ___	

TABLE XXIII. Post application header receipt requirements

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
3.1	Upon receipt of an application header, validate the presence of all mandatory groups and fields.	5.7.1.9	M M	Yes ___ ___ No ___ ___	
3.2	Validate that all occurrence category conditions are satisfied, and validate the legality of all field entries to determine the legality for the header.	5.7.1.9	M M	Yes ___ ___ No ___ ___	
3.3	It is the responsibility of the receiving system to apply default values, if specified, in those fields unspecified by the transmitting system.	5.7.1.9	M M	Yes ___ ___ No ___ ___	

TABLE XXIV. Cases

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
4.1.1	**CASE 1:** Message is an original message. **THIS CASE REQUIRES** GPI for G8 [Response Data Group] is specified “0” (NOT PRESENT) **AND** the message body shall be present **END CASE**	5.7.2.1.1	M M	Yes ___ ___ No ___ ___	

TABLE XXIV. Cases (Continued)

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
4.1.2	**CASE 2**: Message is an acknowledgment message. **THIS CASE REQUIRES** GPI for Group 8 [Response Data Group] is specified "1" (PRESENT) **AND** GPI for G6 [Perishability DTG] is specified “0” (NOT PRESENT) **AND** GPI for G7 [Acknowledgment Request Group] is specified “0” (NOT PRESENT) **AND** the User Data shall not be present **END CASE**	5.7.2.1.2 5.7.5.2	M	M	Yes ___ No ___	___ ___	
4.1.3	**CASE 3**: Message is a Computer File/Data Block Transfer. **THIS CASE REQUIRES** UMF is specified “1” (BINARY FILE) **AND** GPI for G4 [Message Identification Group] is specified “0” (NOT PRESENT) **END CASE**	5.7.2.1.3	M	M	Yes ___ No ___	___ ___	
4.1.4	**CASE 4**: Message is a Forwarded Message. **THIS CASE REQUIRES** UMF is specified “4” (FORWARDED MESSAGE) **AND** GPI for G4 [Message Identification Group] is specified “0” (NOT PRESENT) **AND** User Data shall be present **END CASE**	5.7.2.1.4	M	M	Yes ___ No ___	___ ___	
4.1.5	**CASE 5**: Message was compressed. **THIS CASE REQUIRES** FPI for Data Compression is specified “1” (PRESENT) **AND** GPI for G8 [Response Data Group] is specified “0” (NOT PRESENT) **AND** User Data shall be present **END CASE**	5.7.2.1.5	M	M	Yes ___ No ___	___ ___	
4.1.6	**CASE 6:** Message has security services applied. **THIS CASE REQUIRES** GPI for G10 [Message Security Group] is specified “1” (PRESENT) **END CASE**	5.7.2.1.6	O	M	Yes ___ No ___	___ ___	
4.1.7	**CASE 7:** Message is a signed acknowledgment. **THIS CASE REQUIRES** GPI for G8 [Response Data Group] is specified “1” (PRESENT) **AND** GPI for G6 [Perishability DTG Group] is specified “0” (NOT PRESENT)	5.7.2.1.7	O	M	Yes ___ No ___	___ ___	

TABLE XXIV. Cases (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
	AND GPI for G7 [Acknowledgment Request Group] is specified “0” (NOT PRESENT) **AND** GPI for G14 [Authentication Data (A)] is specified “1” (PRESENT) **AND** GPI for G15 [Authentication Data (B)] is specified “1” (PRESENT) **AND** Signed Acknowledge Request Indicator is specified “0” (SIGNED RESPONSE NOT REQUIRED) **AND** User Data shall be present **END CASE**				

TABLE XXV. Conditions

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
4.2.1	**CONDITION 1:** **IF** GPI for G1 [Originator Address Group] is specified “0” (NOT PRESENT) **THEN** GPI for G7 [Acknowledgment Request Group] is specified “0” (NOT PRESENT) **ENDIF**	5.7.2.2.1	M M	Yes ___ ___ No ___ ___	
4.2.2	**CONDITION 2:** **IF** FPI for URN is specified “1” (PRESENT) **THEN** FPI for Unit Name is specified “0” (NOT PRESENT) **ENDIF**	5.7.2.2.2	M M	Yes ___ ___ No ___ ___	
4.2.3	**CONDITION 3:** **IF** FPI for URN is specified “0” (NOT PRESENT) **THEN** FPI for Unit Name is specified “1” (PRESENT) **ENDIF**	5.7.2.2.3	M M	Yes ___ ___ No ___ ___	
4.2.4	**CONDITION 4:** **IF** FPI for Unit Name is specified “1” (PRESENT) **THEN** FPI for URN is specified “0” (NOT PRESENT) **ENDIF**	5.7.2.2.4	M M	Yes ___ ___ No ___ ___	
4.2.5	**CONDITION 5:** **IF** FPI for Unit Name is specified “0” (NOT PRESENT) **THEN** FPI for URN is specified “1” (PRESENT) **ENDIF**	5.7.2.2.5	M M	Yes ___ ___ No ___ ___	
4.2.6	**CONDITION 6**: This paragraph is left blank to maintain paragraph conformity.	5.7.2.2.6	NA		
4.2.7	**CONDITION 7:** **IF** GRI for R3 is specified “1” (REPEATED)	5.7.2.2.7	M M	Yes ___ ___ No ___ ___	

TABLE XXV. Conditions (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
	THEN FPI for Message Size is specified “1” (PRESENT) **AND** FPI for Header Size is specified "1" (PRESENT) **ENDIF**				
4.2.8	**CONDITION 8:** **IF** R/C is NOT specified “6” (CANTCO) **THEN** FPI for CANTCO Reason Code is specified “0” (NOT PRESENT) **ENDIF**	5.7.2.2.8	M M	Yes ___ ___ No ___ ___	
4.2.9	**CONDITION 9:** **IF** R/C is NOT specified “2” (CANTPRO) **THEN** FPI for CANTPRO Reason Code is specified “0” (NOT PRESENT) **ENDIF**	5.7.2.2.9	M M	Yes ___ ___ No ___ ___	
4.2.10	**CONDITION 10:** This paragraph is left blank to maintain paragraph conformity.	5.7.2.2.10	NA		
4.2.11	**CONDITION 11:** **IF** Machine Acknowledge Request Indicator is specified “1” (MACHINE ACKNOWLEDGMENT REQUIRED) **OR** Operator Acknowledge Request Indicator is specified “1” (OPERATOR ACKNOWLEDGMENT REQUIRED) **OR** Operator Reply Request Indicator is specified “1” (OPERATOR REPLY REQUIRED) **THEN** GPI for G5 [Originator DTG] is specified “1” (PRESENT) **ENDIF**	5.7.2.2.11	M M	Yes ___ ___ No ___ ___	
4.2.12	**CONDITION 12:** This paragraph is left blank to maintain paragraph conformity.	5.7.2.2.12	NA		
4.2.13	**CONDITION 13:** **IF** Security Parameters Information is specified “0” (AUTHENTICATION (USING SHA-1 AND DSA)/ NO ENCRYPTION)) **THEN** GPI for G11 [Keying Material Group] is specified “0” (NOT PRESENT) **AND** GPI for G12 [Cryptographic Initialization Group] is specified “0” (NOT PRESENT) **AND** GPI for G13 [Keying Token Group] is specified “0” (NOT PRESENT) **AND** GPI for G14 [Authentication (A) Group] is specified “1” (PRESENT) **AND** GPI for G16 [Message Security Padding Group] is specified “0” (NOT PRESENT) **ENDIF**	5.7.2.2.13	O M	Yes ___ ___ No ___ ___	

TABLE XXV. Conditions (Continued)

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
4.2.14	**CONDITION 14:** **IF** GPI for G7 [Acknowledgment Request Group] is specified “0” (NOT PRESENT) **THEN** Signed Acknowledge Request Indicator is specified “0” (SIGNED ACKNOWLEDGMENT NOT REQUIRED) **ENDIF**	5.7.2.2.14	O	M	Yes ___ No ___	___ ___	
4.2.15	**CONDITION 15:** **IF** Signed Acknowledge Request Indicator is specified “1” (SIGNED ACKNOWLEDGMENT REQUIRED) **THEN** GPI for G7 [Acknowledgment Request Group] is specified “1” (PRESENT) **ENDIF**	5.7.2.2.15	O	M	Yes ___ No ___	___ ___	

TABLE XXVI. Expected response requirement

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
5.1	Machine Acknowledge Requested: **IF** Machine Acknowledge Request Indicator is specified “1” (MACHINE ACKNOWLEDGMENT REQUIRED) **THEN** Response Message R/C is specified “1” (MACHINE RECEIPT) **OR** Response Message R/C is specified “2” (CANTPRO) **ENDIF**	5.7.3.1	M	M	Yes ___ No ___	___ ___	
5.2	Operator Acknowledge Requested: **IF** Operator Acknowledge Request Indicator is specified “1” (OPERATOR ACKNOWLEDGMENT REQUIRED) **THEN** Response Message R/C is specified “3” (OPERATOR ACKNOWLEDGE) **OR** Response Message R/C is specified “2” (CANTPRO) **ENDIF**	5.7.3.2	M	M	Yes ___ No ___	___ ___	
5.3	Operator Reply Requested: **IF** Operator Reply Request Indicator is specified “1” (OPERATOR REPLY REQUIRED) **THEN** Response Message R/C is specified “4” (WILCO) **OR** Response Message R/C is specified “5” (HAVCO)	5.7.3.3	M	M	Yes ___ No ___	___ ___	

TABLE XXVI. Expected response requirement (Continued)

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
	OR Response Message R/C is specified "6" (CANTCO) **OR** Response Message R/C is specified "2" (CANTPRO) **ENDIF**						
5.4	Signed Acknowledge Requested: **IF** Signed Acknowledge Request Indicator is specified "1" (SIGNED ACKNOWLEDGMENT REQUIRED) **THEN** Response shall have GPI for G15 [Authentication (B) Group] is specified "1" (PRESENT) **OR** {Response shall have R/C is specified "2" (CANTPRO) **AND** [CANTPRO Reason Code is specified "27" (AUTHENTICATION FAILURE) **OR** CANTPRO Reason Code is specified "28" (CERTIFICATE NOT FOUND) **OR** CANTPRO Reason Code is specified "29" (CERTIFICATE INVALID) **OR** CANTPRO Reason Code is specified "30" (DO NOT SUPPORT THIS SPI VALUE) **OR** CANTPRO Reason Code is specified "31" (CAN NOT GENERATE A SIGNED ACKNOWLEDGMENT)} **ENDIF**	5.7.3.4	O	M	Yes ___ ___ No ___ ___	

TABLE XXVII. Special considerations

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
6.1	Perishable Data Check: **IF** GPI for G6 [Perishable Data DTG] is specified "1" (PRESENT) **AND** G6 [Perishable Data DTG] is earlier than current DTG **THEN** Message Data shall be ignored **AND** **IF** Machine Acknowledge Request Indicator is specified "1" (MACHINE ACKNOWLEDGMENT REQUIRED) **THEN** Response Message R/C is specified "2" (CANTPRO) **AND** CANTPRO Reason Code is	5.7.4.1	M	M	Yes ___ ___ No ___ ___		

.

TABLE XXVII. Special considerations (Continued)

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
	specified “25” (MESSAGE TOO OLD, BASED ON PERISHABILITY) **ENDIF** **ENDIF**						
6.2	Response to version non-interoperability. **IF** Recipient does not implement Version sent **THEN** Version is specified "15" (VERSION SENT NOT IMPLEMENTED) **AND** FPI for Data Compression Type is specified "0" (NOT PRESENT) **AND** GPI for Group 1 [Originator Address Group] is specified "1" (PRESENT) **AND** Originator specified is the Original Recipient **AND** GPI for Group 2 [Recipient Address Group] is specified "1" (PRESENT) **AND** Recipient specified is the Originator of the original message **ENDIF**	5.7.4.2	M	M	Yes ___ ___ No ___ ___	
6.3	Broadcast Transmission Check. **IF** GPI for G2 [Recipient Address Group] is specified “0” (NOT PRESENT) **AND** GPI for G3 [Information Address Group] is specified “0” (NOT PRESENT) **THEN** message shall be broadcast in accordance with lower layer broadcast protocols **ENDIF**	5.6.3.b. 5.7.4.3	M	M	Yes ___ ___ No ___ ___	
6.4	Add DTG Extensions when Originator DTGs are the same: **IF** Originator DTG is equal to the Originator DTG of a previously sent message **THEN** FPI for DTG Extension is specified “1” (PRESENT) **AND** DTG Extension shall be unique **ENDIF**	5.7.4.4	M	M	Yes ___ ___ No ___ ___	
6.5	Message sent via a streaming/undelimited transport protocol: **IF** GRI for R3 is specified “0” (NOT REPEATED) **AND** the message is being set via a streaming/undelimited transport **THEN** FPI for Message Size is specified “1” (PRESENT) **AND** FPI for Header Size is specified "1" (PRESENT) **ENDIF**	5.7.4.5	M	M	Yes ___ ___ No ___ ___	

.

TABLE XXVII. Special considerations (Continued)

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
6.6	Message concatenation: GPI for G1 [Originator Address Group] is specified "1" (PRESENT) (**OR** GPI for G2 [Recipient Address Group] is specified "1" (PRESENT) **OR** GPI for G3 [Information Address Group] is specified "1" (PRESENT)) **THEN** Groups G1 [Originator Address Group], G2 [Recipient Address Group] and G3 [Information Address Group] addresses are common to all concatenated messages **AND** GRI for R3 [Message Handling Group] is specified "1" (REPEATED) (**AND** Each iteration shall match in sequence specifying information about its respective concatenated message) **AND** FPI for Message Size is specified "1" (PRESENT) **AND** FPI for Header Size is specified "1" (PRESENT) **AND** Message Size, including application header, shall not exceed 1,048,575 bytes **XOR** N-layer pass through is being invoked **AND** S/R not used **THEN** Total size of a concatenated message block shall not exceed 3283 octets **ENDIF**	5.7.4.6 5.7.5.5	M	M	Yes ___ ___ No ___ ___	
6.7	Message Case and Message Subtype Relationship: **IF** Cases exist for transmitted VMF message **THEN** FPI for Message Subtype is specified "1" (PRESENT) **ENDIF**	5.7.4.7	M	M	Yes ___ ___ No ___ ___	
6.8	Sending Response to a large message: **IF** The received Message Size is greater than Maximum Segment Size **AND** The received message GPI for G7 [Acknowledgment Request Group] is specified "1" (PRESENT) **AND** The message was received via a reliable transport mechanism **THEN** Response(s), to the received message shall be sent via a reliable transport mechanism **ENDIF**	5.7.4.8	M	M	Yes ___ ___ No ___ ___	

.

TABLE XXVII. Special considerations (Continued)

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes

6.9	DTG Extension to DTG of Message Being Acknowledged.
	IF GPI for G8 [Response Data Group] is specified “1” (PRESENT)
	THEN
	IF FPI for DTG Extension discriminating the Originator DTG is specified “1” (PRESENT)
	THEN Response message shall have GPI for G8 [Response Data Group] identifying the DTG of Message Being Acknowledged is specified “1” (PRESENT)
	AND FPI for DTG Extension discriminating the DTG of Message Being Acknowledged is specified “1” (PRESENT)
	ELSE
	Response message shall have GPI for G8 [Response Data Group] identifying the DTG of Message Being Acknowledged is specified “1” (PRESENT)
	AND FPI for DTG Extension discriminating the DTG of Message Being Acknowledged is specified “0” (NOT PRESENT)
	ENDIF
	ENDIF
		5.7.4.9	M	M	Yes ___ ___
					No ___ ___	

6.10	Decompression of messages prior to parsing. **IF** FPI for Data Compression Type field is specified “1” (PRESENT) **THEN** Receiving system shall decompress the user data prior to parsing **ENDIF**	5.7.4.10	M	M	Yes ___ ___ No ___ ___	
6.11	Unit Name usage in a response message. **IF** FPI for Unit Name identifying the originator is specified “1” (PRESENT) **THEN** Response message shall have the FPI for Unit Name identifying the recipient is specified “1” (PRESENT) **AND** FPI for URN is specified “0” (NOT PRESENT) **ENDIF**	5.7.4.11	M	M	Yes ___ ___ No ___ ___	

.

TABLE XXVII. Special considerations (Continued)

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
6.12	URN usage in a response message. **IF** FPI for URN identifying the originator is specified "1" (PRESENT) **THEN** Response message shall have the FPI for URN identifying the recipient specified "1" (PRESENT) **AND** FPI for Unit Name is specified "0" (NOT PRESENT) **ENDIF**	5.7.4.12	M	M	Yes ___ No ___	___ ___	
6.13	Addressee URN uniqueness. A specified URN shall occur at most once as an addressee of a message either as a recipient destination or as an information destination. A duplicate destination URN in the recipient address group and the information address group of a message is not permitted.	5.7.4.13	O	M	Yes ___ No ___	___ ___	
6.14	Message uses Segmentation/Reassembly protocol: **IF** Data transfer is greater than the maximum segment size (MSS) permitted **THEN** Message Segmentation/Reassembly protocol shall be used **ENDIF**	5.7.4.14 C.1.1	O	M	Yes ___ No ___	___ ___	

TABLE XXVIII. Segmentation/reassembly protocol

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
7.1	Data transfers greater than maximum segment size (MSS) permitted shall be segmented and reassembled in accordance with the Appendix C.	C.1.1 5.7.4.14	M M	Yes ___ ___ No ___ ___	
7.1.1	Segmentation and reassembly protocol shall be supported within end systems.	C.1.2	7.1:M	Yes ___ ___ No ___ ___	
7.2	Data transfers, which are larger than the designated MSS, shall be segmented by the source device prior to transmission, and reassembled at the destination device prior to delivery to the application.	C.3	7.1:M	Yes ___ ___ No ___ ___	
7.2.1	An end-to-end acknowledgment shall be employed to ensure reliable delivery of all segments.	C.3	O M	Yes ___ ___ No ___ ___	
7.2.2	MSS shall be calculated as follows: MMTU: Maximum Message Transfer Unit size SH: S/R header size UDP: UDP header size IP: IP header size IL: Intranet layer header size MSS = MMTU – (SH + UDP + IP) for IP datagrams; and MSS = MMTU – (SH + IL) for n-layer pass through	C.3.1	O M	Yes ___ ___ No ___ ___	
7.2.2.1	For n-layer pass through exchanges: If the application isn't using S/R with n-layer pass through, message size shall not exceed 3283 octets otherwise it has to segment the message into 3283 octets.	C.3.1.2	O M	Yes ___ ___ No ___ ___	
7.2.3	A partial acknowledgment scheme shall be employed in which correctly received segments are acknowledged, even if all segments comprising a data transfer have not been received.	C.3.2	7.2.1:M	Yes ___ ___ No ___ ___	
7.2.3.1	Every data segment shall contain a last segment number from which the destination device may estimate the time required to receive all segments of a given data transfer.	C.3.2	O M	Yes ___ ___ No ___ ___	
7.2.3.2	A receive timer is set during which the receiving unit is waiting for the expected segments of a data transfer to be arrived correctly. When this timer expires, all segments correctly received shall be acknowledged through a bit map in the SH.	C.3.2	O M	Yes ___ ___ No ___ ___	
7.2.3.3	Upon successful receipt of all segments, the data transfer shall be reassembled and transferred to the application layer.	C.3.2	O M	Yes ___ ___ No ___ ___	
7.2.3.4	The source device shall only retransmit those segments that the receiver indicates are missing (via Partial Acknowledgment).	C.3.2	O M	Yes ___ ___ No ___ ___	
7.2.4	Two of the interface parameters that the S/R service interface has in common with UDP are the source and destination ports. Source and destination port parameters provided in the S/R service interface shall be placed in	C.3.3	O M	Yes ___ ___ No ___ ___	

TABLE XXVIII. Segmentation/reassembly protocol (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
	corresponding Source Port and Destination Port fields of the S/R header. The port named “udp-sr-port” has been registered with the Internet Assigned Number Authority and assigned port number 1624 (decimal) to indicate S/R protocol as defined by this standard.				
7.2.4.1	Port 1581 as defined in paragraph 5.8.3.7 of this standard shall be used to indicate MIL-STD-2045-47001 as an ALP when S/R is used with n-layer pass through. If N-layer pass through with S/R is used with an ALP other than MIL-STD-2045-47001, use the respective port nubmer for the ALP.	C.3.3.2	O M	Yes ___ ___ No ___ ___	
7.2.5	All data transfers received from the application which exceed the MSS shall be segmented.	C.3.4	O M	Yes ___ ___ No ___ ___	
7.2.5.1	The data transfer is segmented and a SH is appended to each segment. A serial number shall be assigned and copied into the header of each segment of that data transfer. Each information segment is then sequentially sent starting with segment number equal to 1.	C.3.4	O M	Yes ___ ___ No ___ ___	
7.2.5.2	The originator shall indicate in the segmentation header whether the data transfer requires an end-to-end acknowledgment (Type field = 0) or does not require an end-to-end acknowledgment (Type field = 2).	C.3.4	O M	Yes ___ ___ No ___ ___	
7.2.5.3	A retransmission timer shall be used for segment retransmission when end-to-end acknowledgment is invoked.	C.3.4	O M	Yes ___ ___ No ___ ___	
7.2.5.4	If the retransmission timer expires without the receipt of at least a partial acknowledgment, an Acknowledgment Request shall be issued to the recipient requesting for segments acknowledgment status.	C.3.4	O M	Yes ___ ___ No ___ ___	
7.2.5.5	If no response to the Acknowledgment Request, the source device shall resend the Acknowledgment Request.	C.3.4	O M	Yes ___ ___ No ___ ___	
7.2.5.6	If no response to the Acknowledgment Request after N number of tries, the data transfer shall be aborted and an error indication shall be returned to the upper layer process or application.	C.3.4	O M	Yes ___ ___ No ___ ___	
7.2.5.7	If no end-to-end-acknowledgment is needed the originator shall assume the transmission completed successfully when the retransmission timer expires.	C.3.4	O M	Yes ___ ___ No ___ ___	
7.2.6	Upon receipt of a segment of a new data transfer, the recipient shall set an accumulation timer during which it expects to receive coming segments from the sender.	C.3.5	O M	Yes ___ ___ No ___ ___	

TABLE XXVIII. Segmentation/reassembly protocol (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
7.2.6.1	If the accumulation timer expires before receiving all expected segments, a partial Acknowledgment (100) shall be sent to the sender indicating in the segment Acknowledgment bit map which segments of the data transfer have been received correctly. Otherwise, the timer shall be stopped.	C.3.5	O M	Yes ___ ___ No ___ ___	
7.2.6.2	For a data transfer which requires an end-to-end acknowledgment, a Partial Acknowledgment or a Complete Acknowledgment shall be sent to the sender when all expected segments of the data transfer have been received correctly.	C.3.5	O M	Yes ___ ___ No ___ ___	
7.2.6.3	The recipient shall accumulate segments of a data transfer with the same serial number from the same source IP address and reassemble that data transfer when all segments have been successfully received, using segment numbers to indicate segment position relative to the whole data transfer.	C.3.5	O M	Yes ___ ___ No ___ ___	
7.2.6.4	SHs shall be removed. The whole data transfer is then passed to the upper layer process indicated by the port number.	C.3.5	O M	Yes ___ ___ No ___ ___	
7.3	S/R PDU Format.	C.4	O M	Yes ___ ___ No ___ ___	
7.3.1	Source Port	C.4.1.1	O M	Yes ___ ___ No ___ ___	
7.3.2	Destination Port	C.4.1.2	O M	Yes ___ ___ No ___ ___	
7.3.3	Type	C.4.1.3	O M	Yes ___ ___ No ___ ___	
7.3.3.a	End-to-End Acknowledgment Required	C.4.1.3	7.3.3: O.<7>	Yes ___ ___ No ___ ___	
7.3.3.b	Abort Request	C.4.1.3	7.3.3: O.<7>	Yes ___ ___ No ___ ___	
7.3.3.c	End-to-End Acknowledgment not Required	C.4.1.3	7.3.3: O.<7>	Yes ___ ___ No ___ ___	
7.3.3.d	Acknowledgment Request	C.4.1.3	7.3.3: O.<7>	Yes ___ ___ No ___ ___	
7.3.3.e	Partial Acknowledgment	C.4.1.3	7.3.3: O.<7>	Yes ___ ___ No ___ ___	
7.3.3.f	Abort Confirm	C.4.1.3	7.3.3: O.<7>	Yes ___ ___ No ___ ___	
7.3.3.g	Complete Acknowledgment	C.4.1.3	7.3.3: O.<7>	Yes ___ ___ No ___ ___	
7.3.4	Header Length (HLEN)	C.4.1.4	O M	Yes ___ ___ No ___ ___	

TABLE XXVIII. Segmentation/reassembly protocol (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
7.3.5	Poll/Final (P/F)	C.4.1.5	O M	Yes ___ ___ No ___ ___	
7.3.5.1	Data Segment with Poll/Final (P/F) field specifying an immediate response. **IF** a Data Segment is received **AND** P/F specifies “1” (IMMEDIATE RESPONSE) **THEN** (receiving unit shall immediately) Respond specifying Type field “4” (PARTIAL ACKNOWLEDGMENT) **OR** specifying Type field “6” (COMPLETE ACKNOWLEDGMENT) **AND** P/F field specified “1” (IMMEDIATE RESPONSE) **ENDIF**	C.4.1.5.a.	O M	Yes ___ ___ No ___ ___	
7.3.5.2	Abort Request Segment with Poll/Final (P/F) field specifying an immediate response. **IF** an Abort Request Segment is received **AND** P/F specifies “1” (IMMEDIATE RESPONSE) **THEN** (receiving unit shall immediately) Respond specifying Type field “5” (ABORT CONFIRM) **AND** P/F field specified “1” (IMMEDIATE RESPONSE) **ENDIF**	C.4.1.5.b.	O M	Yes ___ ___ No ___ ___	
7.3.6	Serial Number	C.4.1.6	O M	Yes ___ ___ No ___ ___	
7.4	Data Segment	C.4.2	O M	Yes ___ ___ No ___ ___	
7.4.1	The length of the data portion shall be the same for all segments of a data transfer except for the last segment, which may be shorter.	C.4.2	O M	Yes ___ ___ No ___ ___	
7.4.1.a	Data Segment sent with Type field specifying “0” (END-TO-END ACKNOWLEDGMENT REQUIRED)	C.4.2	7.4.1: O.<2>	Yes ___ ___ No ___ ___	
7.4.1.b	Data Segment sent with Type field specifying “2” (END-TO-END ACKNOWLEDGMENT NOT REQUIRED)	C.4.2	7.4.1: O.<2>	Yes ___ ___ No ___ ___	
7.4.2	**IF** Type field specifies ”0” (END-TO-END ACKNOWLEDGMENT REQUIRED) **THEN** (receiving unit shall immediately) Respond specifying Type field “6” (COMPLETE ACKNOWLEDGMENT) **ENDIF**	C.4.2	7.4.1.a :M	Yes ___ ___ No ___ ___	
7.4.3	Segment Number	C.4.2.1	O M	Yes ___ ___ No ___ ___	

TABLE XXVIII. Segmentation/reassembly protocol (Continued)

Item Number	Field Name	Reference	Status Tx Rx	Support Tx Rx	Notes
7.4.4	Last Segment Number	C.4.2.2	O M	Yes ___ ___ No ___ ___	
7.5	Partial Acknowledgment	C.4.3	O M	Yes ___ ___ No ___ ___	
7.5.1	S/R PDU fields present **AND** Type field specifying “4” (PARTIAL ACKNOWLEDGMENT) **AND** Starting Segment Number **AND** Bit Map field **AND** Padded field if required.	C.4.3	O M	Yes ___ ___ No ___ ___	
7.5.2	Starting segment number specifies all previous segments successfully received in sequence.	C.4.3.1	O M	Yes ___ ___ No ___ ___	
7.5.3	Acknowledgment Segment Bitmap. The bits in this field are used to indicate which segments of a data transfer have been successfully received at the receiving unit.	C.4.3.2	O M	Yes ___ ___ No ___ ___	
7.5.3.a	A bit set (binary 1) means the segment has been correctly received.	C.4.3.2	7.5.3: O.<2>	Yes ___ ___ No ___ ___	
7.5.3.b	A bit set (binary 0) means the segment was not correctly received.	C.4.3.2	7.5.3: O.<2>	Yes ___ ___ No ___ ___	
7.5.3.1	This field is extensible in 32-bit increments. Unused bits added to pad the field to a 32-bit boundary shall be set to “0”.	C.4.3.2	O M	Yes ___ ___ No ___ ___	
7.6	Complete Acknowledgment Segment.	C.4.4	O M	Yes ___ ___ No ___ ___	
7.6.1	S/R PDU fields present **AND** Type field specifying “6” (COMPLETE ACKNOWLEDGMENT)	C.4.4	O M	Yes ___ ___ No ___ ___	
7.6.1.1	No data field shall be permitted with the complete Acknowledgment.	C.4.4	O M	Yes ___ ___ No ___ ___	
7.7	Abort Request.	C.4.5	O M	Yes ___ ___ No ___ ___	
7.7.1	S/R PDU fields present **AND** Type field specifying “1” (ABORT REQUEST)	C.4.5	O M	Yes ___ ___ No ___ ___	
7.7.2	Either the data transfer originator or its recipient may initiate the abort action.	C.4.5	O M	Yes ___ ___ No ___ ___	
7.7.3	No data field shall be permitted with the Abort Request.	C.4.5	O M	Yes ___ ___ No ___ ___	
7.7.4	All segments associated with the Serial Number shall be discarded.	C.4.5	O M	Yes ___ ___ No ___ ___	
7.8	Abort Confirm.	C.4.6	O M	Yes ___ ___ No ___ ___	
7.8.1	S/R PDU fields present **AND** Type field specifying “5” (ABORT CONFIRM)	C.4.6	O M	Yes ___ ___ No ___ ___	

TABLE XXVIII. Segmentation/reassembly protocol (Continued)

Item Number	Field Name	Reference	Status Tx	Status Rx	Support Tx	Support Rx	Notes
7.8.2	After receiving an Abort Request, the receiving addressee shall confirm its acceptance of the abort by transmitting an Abort confirm.	C.4.6	O	M	Yes ___ No ___	___ ___	
7.8.3	No data field shall be permitted with the Abort confirm.	C.4.6	O	M	Yes ___ No ___	___ ___	
7.8.4	All segments, which have the same Serial Number as identified in the Abort Request, previously received shall be discarded.	C.4.6	O	M	Yes ___ No ___	___ ___	
7.9	Acknowledgment Request.	C.4.7	O	M	Yes ___ No ___	___ ___	
7.9.1	S/R PDU fields present **AND** Type field specifying “3” (ACKNOWLEDGMENT REQUEST) **AND** Last Sent Segment Number **AND** Padded field if required.	C.4.7 C.4.7.1	O	M	Yes ___ No ___	___ ___	
7.9.2	An Acknowledgment Request shall be used by the data transfer originator to request the acknowledgment status of all previous transmitted Data segments.	C.4.7	O	M	Yes ___ No ___	___ ___	
7.9.3	Upon receiving an Acknowledgment Request, the receiver shall return a Partial Acknowledgment to the sender.	C.4.7	O	M	Yes ___ No ___	___ ___	

CONCLUDING MATERIAL

a. Preparing Activity:

US Army Communications Electronics Command (USACECOM): CR1

b. Custodians:

Army:	CR1
Navy:	OM
Air Force:	02
DISA:	DC1
DIA:	DI
NSA:	NS
NORAD & USSPACECOM:	US

c. Review Activities:

OSD:	IR, SE
Army:	AC, CR, IE, PT, TM1, TM3
Navy:	CG, CH, EC, MC, ND, TD
Air Force:	11, 13, 33, 99
DCMA:	CM
NIMA:	MP
DOT:	OST

d. Project number:

DCPS-00580

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.

2. The submitter of this form must complete blocks 4, 5, 6, and 7, and send to preparing activity.

3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	**1. DOCUMENT NUMBER** MIL-STD-2045-47001C	**2. DOCUMENT DATE (YYYYMMDD)** 20020322

3. DOCUMENT CONNECTIONLESS DATA TRANSFER APPLICATION LAYER STANDARD

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME *(Last, First, Middle Initial)*	b. ORGANIZATION	
c. ADDRESS *(Include Zip Code)*	d. TELEPHONE (Include Area Code) (1) Commercial (2) AUTOVON *(if applicable)*	**7.DATE SUBMITTED** (YYYYMMDD)

8. PREPARING ACTIVITY

NAME Mr. Raymond Menell	b. TELEPHONE *Include Area Code)* (1) Commercial (732) 532-0654 (2) AUTOVON DSN 992-0654
c. ADDRESS *(Include Zip Code)* Commander, USACECOM, ATTN: AMSEL-SE-CD Building 1209, Fort Monmouth, NJ 07703	**IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:** Defense Standardization Program Office (DLSC-LM) 8725 John J. Kingman road, Suite 2533, Ft. Belvoir, VA 22060-2533 Telephone (703) 767-6888 AUTOVON 427-6888