Encrypted Automatic Identification System (EAIS)
Interface Design Description (IDD)
04 June 2014

Submitted by: _____ _____

Digitally signed by PARSONS.MICHAEL.W.1089605918
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USCG, cn=PARSONS.MICHAEL.W.1089605918
Reason: I have reviewed this document
Date: 2014.06.04 09:03:13 -04'00'

M. W. Parsons
System Engineer (CT-N1)

Date

Approved by: RECKLEY.ADAM.R.1274982159 _____ _____

Digitally signed by RECKLEY.ADAM.R.1274982159
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USCG, cn=RECKLEY.ADAM.R.1274982159
Date: 2014.06.05 10:26:18 -04'00'

A. R. Reckley, LT
Core Technologies Navigation Branch (CT-N1)
Branch Chief

Date

Approved by: CASTRO.HECTOR.A.1182442344 _____ _____

Digitally signed by CASTRO.HECTOR.A.1182442344
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USCG, cn=CASTRO.HECTOR.A.1182442344
Date: 2014.06.04 16:47:27 -04'00'

H. A. Castro, LCDR
Core Technologies Navigation (CT-N)
Section Chief

Date

Record of Changes

Change#	Date	Title or Brief Description	Entered By
Original	04 Jun 14	C3CEN EAIS IDD v1.0	LT A.R. Reckley

Table of Contents

1. Scope

1.1. Identification

This Interface Design Description (IDD) specifies the interfaces technical characteristics of an Encrypted Automatic Identification System (EAIS) which meets Coast Guard requirements for Sensitive But Unclassified (SBU) Tactical Information Exchange and Display System (STEDS) and Blue Force Tracking (BFT) .

1.2. Policy

This IDD constitutes the U. S. Coast Guard standard for the exchange of SBU Tactical Information using AIS operating frequencies and message protocol. This IDD was developed under the authority of the U. S. Coast Guard Assistant Commandant for C4&IT in order to standardize SBU tactical information exchanges using AIS to meet COMDT (CG-761) operational requirements for STEDS and BFT.

1.3. System Overview

Coast Guard EAIS consists of an EAIS Transponder and an EAIS Presentation Interface (PI). The EAIS Presentation Interface is typically an Electronic Chart System (ECS) or Electronic Chart Display Information System (ECDIS) which integrates EAIS data, navigational sensors, surface-search radar, and cutter electronic charts into one display providing a robust situational awareness tool.

1.4. Interface Overview

The EAIS provides AIS, both positional and static data, Sensitive but Unclassified Tactical Information Exchange and Display System (STEDS), which includes text message communication, Target of Interest (TOI) promulgation and search pattern/overlay exchange and Blue Force Track (BFT) information data that is exclusively between U.S. Coast Guard specific units, to operators.

2. References

Name/Number	Version Date	Title
eNav Requirements	14 Mar 2012	eNav Coast Guard Requirements v1.2
COMD (G-OCC-1) LTR 2000	19 Jul 2005	Operational Requirements for SBU Tactical Information Exchange and Display System (STEDS)
IEC 61174	Mar 2010	Specifications for Chart Content and Display Aspects of ECDIS, Edition 6.0,
NMEA 0183	Jun 2012	Standard for Interfacing Marine Electronic Devices (Ver.4.10)
NMEA 2000	January 2013	Edition 3.00 Includes the following documents: Main Document Version 1.210 Appendix A Version 1.200 (Application Layer - included in Appendix B) Appendix B Version 2.000 (Database of Messages) Appendix C Version 1.200 (Certification Criteria and Test Methods) Appendix D Version 1.210 (Application Notes) Appendix E ISO 11783-3 Data Link Layer Appendix F ISO 11783-5 Network Management Appendix G ISO 11898 Controller Area Network Appendix H (3rd Party Applications w/ NMEA 2000 Certified 3rd Party Gateway)
ITU-R M. 1371-5	Feb 2014	"Technical Characteristics for a Universal Shipborne Automatic Identification System Using Time Division Multiple Access"
ITU-R M.1084	March 2012	Interim solutions for improved efficiency in the use of the band 156-174 MHz by stations in the maritime mobile service

3. Interface Description

Annex 1 contains a technical description of VDL AIS Blue Force Tracking (BFT), which employs standard VDL AIS messages 6 and 8 to transport encrypted data. Annex 1 is based on International Telecommunication Union (ITU) standard ITU-R M.1371-5. Annex 1 addresses only sections and subsections that deviate from the referenced ITU standard, hence the seemingly disjointed numbering. Sections and subsections that appear to be omitted from Annex 1, are identical to corresponding sections and subsections of the ITU standard. The Annex 1 implementation will be phased out completely once operational commands transition to Annex 2.

Annex 2 contains a technical description of VDL Sensitive But Unclassified (SBU) Tactical Information Exchange and Display System (STEDS), which employs standard VDL AIS message 25 and 26 to transport encrypted data. Annex 2 is based on International Telecommunication Union (ITU) standard ITU-R M.1371-5. Annex 2 addresses only sections and subsections that deviate from the referenced ITU standard, hence the seemingly disjointed numbering. Sections and subsections that appear to be omitted from Annex 2 are identical to corresponding sections and subsections of the ITU standard.

Annex 3 contains a technical description of NMEA-0183 messages required to integrate an EAIS capable AIS Transponder with an EAIS capable Presentation Interface (PI) and vice versa. Proprietary NMEA-0183 messages are required for complete integration. Please see the NMEA-0183 standard for NMEA-0183 messages.

Annex 4 contains a technical description of proprietary NMEA-2000/NMEA OneNet PGN messages required to integrate an EAIS capable AIS transponder with an EAIS capable Presentation Interface (PI) and vice versa. Standard NMEA-2000/NMEA OneNet PGN messages are used in the integration, but are not defined by this document. Please see the NMEA-2000/NMEA OneNet PGN standard for NMEA-2000/NMEA OneNet PGN messages.

Annex 5 is an Asset Type List for EAIS

ANNEX 1

Technical characteristics of CG methodology for transmitting Encrypted-AIS (EAIS) Blue Force Tracking (BFT) data payloads using standard AIS messages 6 and 8 on the AIS VHF Data Link (VDL)

ANNEX 1 of ITU-R M.1371-5

1. GENERAL

Coast Guard EAIS operates in accordance with ITU-R M.1371-5, “Technical Characteristics for a Universal Shipborne Automatic Identification System (AIS) Using Time Division Multiple Access (TDMA) in the VHF Maritime Mobile Band”.

Specific deviations and amplifying details required to implement EAIS are contained in this document.

ANNEX 2 of ITU-R M.1371-5

2. PHYSICAL LAYER

This section adheres to Part 2 of Annex 2 to ITU-R M.1371-5.

3. LINK LAYER

This section adheres to Part 3 of Annex 2 to ITU-R M.1371-5, with the following exceptions:

3.1.6.1 Modify Definition of a Free Slot for EAIS “Polite” Operation

The definition of a free slot, as presented in ITU-R M.1371-5, Annex 2, Paragraph 3.1.6, is further refined such that an unreserved slot must also have a received signal strength level, based on the previous frame received signal strength level, that is less than the current CS Detection Threshold, as described in ITU-R M.1371-5, Annex 7, Paragraph 4.3.1.3. This eliminates the possibility of incorrectly identifying a “blurred” slot (two vessels transmitting during the same time slot and received by own-ship with less than 10 dB received signal strength level difference) as a free slot.

3.3.2. Modes of Operation

Add the following explanation to transponder modes of operation:

3.3.2.4. Normal

When in this mode of operation the AIS transponder defaults to operate in Autonomous & Continuous mode, unless switched to Assigned or Polled mode. The transponder sends and receives AIS messages and EAIS messages.

3.3.2.5. Receive-Only

When in this mode of operation the AIS transponder does not transmit any AIS messages, regardless of any commands received from base stations or interrogations from other vessels. The transponder receives AIS messages and EAIS messages, but transmits nothing (maintaining radio silence).

3.3.2.6. Restricted

When in this mode of operation the AIS transponder only transmits EAIS messages, while no non-EAIS messages are sent. The transponder continues to receive AIS messages and EAIS messages.

3.3.8. EAIS Slot Usage

Total number of bits in assembled EAIS message determines # of slots:

0-128	→	1 slot
129-384	→	2 slots
385-640	→	3 slots
641-896	→	4 slots
897-1152	→	5 slots

4. NETWORK LAYER

This section adheres to Part 4 of Annex 2 to ITU-R M.1371-5, with the following exceptions:

4.1.10. Operating Frequency Channels

When operating in Receive-Only or Restricted mode, as defined in Section 3.3.2. of this Annex, the AIS transceiver shall operate exclusively on the normal AIS frequencies and shall not respond to base station or digital selective calling commands to change frequencies.

4.3.3. Restricted Mode Report Rates (Rr)

4.3.3.1. Dynamic Position Report

4.3.3.1.1. <3 knots: When operating in the Restricted Mode (as defined in Section 3.3.2. of this Annex), Report Rate for BFT Dynamic Position Reports (Message 8, FID 56) shall be 30 seconds when Speed Over Ground (SOG) is less than 3 knots for more than 3 minutes.

4.3.3.1.2. >3 knots: When operating in the Restricted Mode (as defined in Section 3.3.2. of this Annex), Report Rate for BFT Dynamic Position Reports (Message 8, FID 56) shall be 15 seconds when Speed Over Ground (SOG) is greater than 3 knots.

4.3.3.2. Static Data Report

When operating in the Restricted Mode (as defined in Section 3.3.2. of this Annex), Report Rate for BFT Static Data Report (Message 8, FID 57) shall be 6 minutes and upon change.

4.3.3.3 Target of Interest (TOI) Message

When operating in the Restricted Mode (as defined in Section 3.3.2 of this Annex). Report Rate for the PI generated Target of Interest (TOI) message shall be every 15 seconds until canceled.

5. Transport Layer

This section adheres to Part 5 of Annex 2 to ITU-R M.1371-5, with the following exceptions:

5.4.1. EAIS Presentation Interface (PI) Protocol

Coast Guard EAIS Transponder and Presentation Interface functional roles are as follows:

Transmit		
Functional Role	Transponder	Presentation Interface
Generate, format (bit stuff & generate check sum), & encrypt EAIS data payloads	Message 6: None Message 8: FID 56 & 57 Messages 6 & 8: Encrypted data payloads received from the PI in ABM (addressed) & BBM (broadcast) messages are inserted into Messages 6 & 8 for data link transmission.	Message 6: FID 55 & 58 Message 8: 55 & 58 Messages 6 & 8: Encrypted data payloads are generated in the PI and sent to the transponder using ABM (addressed) & BBM (broadcast).
Transmit on the VDL	All	None

Receive		
	Transponder	Presentation Interface
Receive over the VDL	Message 6 & 8	None
Decrypt & Parse	Message 6 & 8: All messages are sent to the PI in their encrypted state using VDM message. [Exception: "ALLOW COTS" see 5.4.3.2.] Special Note: Message 8, FID 56 & 57 are decrypted in the transponder so "communications state" data can be used to build the Frame Map.	Message 6 & 8: All messages are decrypted, parsed, and displayed by the PI.

5.4.2. EAIS Overhead Data

5.4.2.1. VDM

VDM messages sent from the Transponder to the PI include 40 bits (broadcast) unencrypted overhead data or 72 bits (addressed) unencrypted overhead data situated ahead of the payload.

5.4.2.2. ABM & BBM

ABM & BBM messages sent from the PI to the Transponder do not include unencrypted overhead data. Only the payload portion is sent.

5.4.3. EAIS Position Report and Static Data Report Decryption

The EAIS Transponder shall have two modes of Position Report Decryption:

5.4.3.1. “Standard”

When “Standard” is selected, EAIS Position Report and Static Data Report data remain encrypted as it is sent to the PI. This mode is for use with an EAIS capable PI only. If this mode is used with a non-EAIS capable PI (COTS), encrypted targets will not be displayed.

5.4.3.2. “Allow COTS”

When “Allow COTS” is selected, EAIS Position Report data and Static Data Report data shall be decrypted by the Transponder and converted to standard VDM messages before it is sent to the PI interface. This allows the non-EAIS capable PI to display blue force tracks as normal AIS targets.

5.4.4. XOR Checksum Computation

When computing the 8-bit XOR checksum used in message 6 & 8 Annex 1 payloads, all the bits before the checksum are used, including the DAC and Function ID. If there are remainder bits just before the checksum, then the bits must be right shifted before the data byte is XOR'ed into the checksum. For example, in the TOI payload there are 141 bits before the checksum. This composes 17 bytes and 5 remainder bits. The 5 bits must be right shifted so that they occupy the lowest 5 bits in the byte, with the highest 3 bits being zero. This byte can then be XOR'ed with the other 17 bytes.

ANNEX 8 of ITU-R M.1371-5

3. Message Descriptions

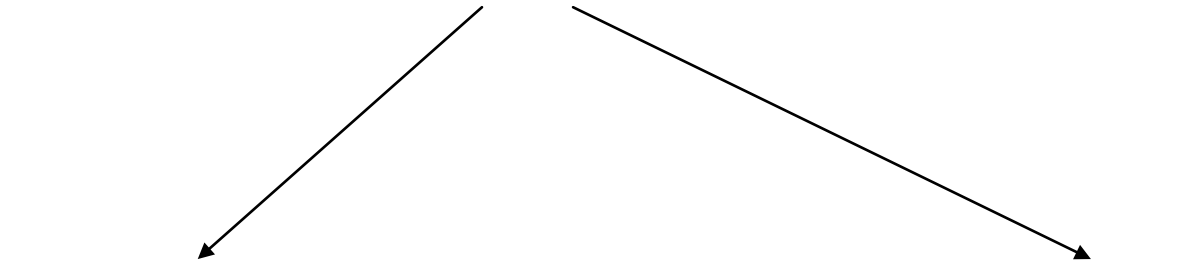
CG EAIS adheres to Part 3 of Annex 8 to ITU-R M.1371-5.

EAIS data is encrypted in Addressed (Message 6) and Broadcast (Message 8) Binary Messages.

The specific content of each message type is described in this section.

3.4. Message 6: Addressed Binary Message

# of bits	72	144 272 400 528 656 784 912
Field Name	Message 6 Overhead	Binary Data (includes bit stuffing)



# of bits	6	2	30	2	30	1	1
Field Name	Msg ID	Rpt. Ind.	Source ID (MMSI)	Seq. #	Destination ID (MMSI)	Retransmit Flag	Spare (set to zero)

3.4.1. "Binary Data" is only encrypted field. General format for Message 6 is:

Parameter	Number of bits (Addressed)	Description	Encryption Status
Message ID	6	Identifier for Message 6; always 6	Unencrypted
Repeat indicator	2	Used by the repeater to indicate how many times a message has been repeated. 0-3; 0 = default; 3 = do not repeat any more	Unencrypted
Source ID (MMSI)	30	MMSI number of source station of message	Unencrypted
Seq #	2	0-3	Unencrypted
Destination ID (MMSI)	30	MMSI of addressed station	Unencrypted
Retransmit Flag	1	0 = no 1 = retransmitted	Unencrypted
Spare bits	1	Set to Zero	Unencrypted
DAC	10	Identifier for this message: 366	Unencrypted
Function ID	6	Function Identifier	Unencrypted
Binary Data STEDS FID 58 & 55 defined message Multiples of 128 bits	128 256 384 512 640 768 896	The length of Binary Data is fundamentally a function of the length of the FID 55 & 58 message to be encapsulated plus the checksum, with bit stuffing to arrive at the next 128 bit increment (128 bit increments are necessitated by AES encapsulation). 8 bits of XOR checksum data is inserted after FID message 55 & 58 data and before the Stuffed bits. Stuffed bits are inserted following the checksum. The number of stuffed bits is equal to the number of bits required to arrive at the next 128 increment for AES encryption. NOTE: In messages 6 & 8, the first two fields of the payload - DAC & Function ID (16 bits) are unencrypted	AES encrypted
TOTAL	216 344 472 600 728 856 984	88 unencrypted bits plus 128, 256, 384, 512, 640, 768 or 896 encrypted bits	

3.4.2. Addressed Message Payload Definitions

This section defines payload content for addressed EAIS messages.

3.4.2.1. Target Of Interest (TOI) PAYLOAD (2 slots total transmission length)

The TOI payload, prior to encryption, is 165 bits in length. Conforming to the AES Encryption scheme with a 128-bit cipher key, the encrypted part of the payload then effectively becomes 256 bits in length to create blocks of 128 bits.

Parameter	Number of bits	Description	Encryption Status
DAC	10	Identifier for this message: 366	Unencrypted
Function ID	6	Function Identifier: 58	Unencrypted
Source ID (MMSI)	30	Source MMSI number	AES encrypted
Target Type	4	1 = AIS, 2 = ARPA, 3 = Dead Reckoned	AES encrypted
Target ID	30	MMSI if type is 1, Sender generated ID otherwise	AES encrypted
SOG	10	Speed over ground in 1/10 knot steps (0-102.2 knots) 1023 = not available, 1022 = 102.2 knots or higher.	AES encrypted
Longitude	28	Longitude in 1/10 000 min (±180 degrees, East = positive, West = negative. 181 degrees (6791AC0 hex) = not available = default)	AES encrypted
Latitude	27	Latitude in 1/10 000 min (±90 degrees, North = positive, South = negative, 91 degrees (3412140 hex) = not available = default)	AES encrypted
COG	12	Course over ground in 1/10 (0-3599). 3600 (E10 hex) = not available = default; 3 601 – 4 095 should not be used.	AES encrypted
Checksum	8	Exclusive OR (XOR) 8-bit	AES encrypted
Stuffed bits	107	Stuffed bits are inserted so that the number of bits in the encrypted field is a multiple of 128 bits; set to zero.	AES encrypted
TOTAL	**272**	16 unencrypted bits plus 256 encrypted bits	

3.4.2.2 Text Message Payload (variable [2-5 slots] total transmission length)

The text message payload, prior to encryption, varies from 74 to 896 bits in length. Conforming to the AES Encryption scheme with a 128-bit cipher key, the encrypted part of the payload then effectively becomes 128, 256, 384, 512, 640, 768 or 896 bits in length to create blocks of 128 bits.

Parameter	Number of bits	Description	Encryption Status
DAC	10	Identifier for this message: 366	Unencrypted
Function ID	6	Function Identifier: 55	Unencrypted
Source ID (MMSI)	30	Source MMSI number.	AES encrypted
Acknowledgement Flag	1	Reserved for future use.	AES encrypted
Segment Number	11	Reserved for future use.	AES encrypted
Text length	8	Length of Text Message	AES encrypted
Text Message	0-822 Variable	User Text Message (6 bits times 0-137 characters)	AES encrypted
Checksum	8	Exclusive OR (XOR) 8-bit	AES encrypted
Stuffed bits	Variable	Variable; stuffed bits are inserted so that the number of bits in the encrypted field is a multiple of 128 bits; set to zero.	AES encrypted
TOTAL	**144 272 400 528 656 784 912**	16 unencrypted bits plus 128, 256, 384, 512, 640, 768 or 896 encrypted bits	

Considering the constraints imposed by the AES encryption algorithm and recommended bit-stuffing guidelines contained in Section 3.2.2.1 of Annex 2 to ITU-R M.1371-5, this results in the following slot usage as a function of number of 6-bit ASCII characters:

Number of Slots	Number of 6-bit ASCII characters
1	not possible to have a 1-slot message
2	0 – 30
3	31 – 73
4	74 – 94
5	95 – 137

3.6. Message 8: Binary broadcast message

# of bits	40	144 272 400 528 656 784 912
Field Name	Message 8 Overhead	Binary Data (includes bit stuffing)

# of bits	6	2	30	2
Field Name	Message ID	Repeat Indicator	Source ID (MMSI of Sender)	Spare (set to zero)

3.6.1. "Binary Data" is only encrypted field. General format for Message 8 is:

Parameter	Number of bits (Addressed)	Description	Encryption Status
Message ID	6	Identifier for Message 8; always 8	Unencrypted
Repeat indicator	2	Used by the repeater to indicate how many times a message has been repeated. 0-3; 0 = default; 3 = do not repeat any more	Unencrypted
Source ID (MMSI)	30	MMSI number of source station of message	Unencrypted
Spare bits	2	Set to Zero	Unencrypted
DAC	10	Identifier for this message: 366	Unencrypted
FID	6	Function identifier	Unencrypted
Binary Data STEDS FID 55 - 58 defined message Multiples of 128 bits	128 256 384 512 640 768 896	The length of Binary Data is fundamentally a function of the length of the FID 55 & 58 message to be encapsulated plus the checksum, with bit stuffing to arrive at the next 128 bit increment (128 bit increments are necessitated by AES encapsulation). 8 bits of XOR checksum data is inserted after FID message 55 - 58 data and before the Stuffed bits. Stuffed bits are inserted following the checksum. The number of stuffed bits is equal to the number of bits required to arrive at the next 128 increment for AES encryption. NOTE: In messages 6 & 8, the first two fields of the payload - DAC & Function ID (16 bits) are unencrypted	AES encrypted
TOTAL	184 312 440 568 696 824 952	56 unencrypted bits plus 128, 256, 384, 512, 640, 768 or 896 encrypted bits	

3.6.2. Broadcast Message Payload Definitions

This section defines the payload content for broadcast message types used by the current AIS BFT asset tracking and data exchange system.

3.6.2.1. Static Data Payload (3 slots total transmission length)

The Static Data Payload format is intended to mirror Message 5 Ship Static and Voyage Related Data format contained in ITU-R M.1371-5. *The table contained here is informational.* Implementers should refer back to ITU-R M.1371-[current revision] for most up to date bit usage and descriptions. The Static Data Payload prior to encryption without bit stuffing is 440 bits in length. Conforming to the AES Encryption scheme with a 128-bit cipher key, the encrypted part of the payload then effectively becomes 512 bits in length to create blocks of 128 bits. The FID 57 static data report shall be transmitted once every 6 minutes.

NOTE: The Message 5 two (2) bit REPEAT INDICATOR field, normally located between FUNCTION ID and USER ID, is omitted in the EAIS Static Data Payload (See below).

Parameter	Number of bits	Description	Encryption Status
DAC	10	Identifier for this message: 366	Unencrypted
Function ID	6	Function Identifier: 57	Unencrypted
Repeat Indicator	0	Not present in EAIS Static Data Payload	no bits
User ID	30	MMSI number.	AES encrypted
AIS Version Indicator	2	0 = station compliant with Recommendation ITU-R M.1371-1 1 = station compliant with Recommendation ITU-R M.1371-3 (or later) 2 = station compliant with Recommendation ITU-R M.1371-5 (or later) 3 = station compliant with future editions	AES encrypted
IMO number	30	0 = not available = default – Not applicable to SAR aircraft 0000000001-0000999999 not used 0001000000-0009999999 = valid IMO number 0010000000-1073741823 = official flag state number	AES encrypted
Call sign	42	7 x 6 bit ASCII characters "@@@@@@@" = not available = default Craft associated with a parent vessel, should use “A” followed by the last 6 digits of the MMSI of the parent vessel. Examples of these craft include towed vessels, rescue boats, tenders, lifeboats and life rafts.	AES encrypted
Name	120	Maximum 20 characters 6 bit ASCII, "@@@@@@@@@@@@@@@@@@@@" = not available = default. The Name should be as shown on the station radio license.	AES encrypted
Type of ship and cargo type	8	0 = not available or no ship = default; 1 - 99 = as defined in 1371-5 100 - 199 = preserved, for regional use; 200 - 255 = preserved, for future use. Not applicable to SAR aircraft	AES encrypted
Dimension/Reference for Position	30	Reference point for reported position; Also indicates the dimension of ship in meters	AES encrypted

Parameter	Number of bits	Description	Encryption Status
Type of Electronic Position Fixing Device	4	0 = Undefined (default) 1 = GPS 2 = GLONASS 3 = Combined GPS/GLONASS 4 = Loran-C 5 = Chayka 6 = Integrated Navigation System 7 = surveyed 8 = Galileo 9 - 14 = not used 15 = internal GNSS	AES encrypted
ETA	20	Estimated Time of Arrival; MMDDHHMM UTC Bits 19 - 16: month; 1 - 12; 0 = not available = default; Bits 15 - 11: day; 1 - 31; 0 = not available = default; Bits 10 - 6: hour; 0 - 23; 24 = not available = default; Bits 5 - 0: minute; 0 - 59; 60 = not available = default	AES encrypted
Maximum Present Static Draught	8	in 1/10 m, 255 = draught *25.5 m* or greater, 0 = not available = default; in accordance with IMO Resolution A.851	AES encrypted
Destination	120	Maximum 20 characters using 6-bit ASCII; "@@@@@@@@@@@@@@@@@@@@" = not available	AES encrypted
DTE	1	Data terminal ready (0 = available, 1 = not available = default)	AES encrypted
Spare	1	Spare. Not used. Should be set to zero.	AES encrypted
Checksum	8	Exclusive OR (XOR) 8-bit	AES encrypted
Stuffed bits	88	Stuffed bits are inserted so that the number of bits in the encrypted field is a multiple of 128 bits (512 for this message); set to zero.	AES encrypted
TOTAL	**528**	16 unencrypted bits plus 512 encrypted bits	

3.6.2.2. Position Report Payload (2 slots total transmission length)

The EAIS Position Report Payload format is intended to mirror ITU-R M.1371-5 Message 1 Position Reports format. *The table contained here is informational.* Implementers should refer back to ITU-R M.1371-[current revision] for most up to date bit usage and descriptions. The EAIS Position Report Payload prior to encryption without bit stuffing is 184 bits in length. Conforming to the AES Encryption scheme with a 128-bit cipher key, the encrypted part of the payload then effectively becomes 256 bits in length to create blocks of 128 bits. The FID 56 position report shall be transmitted once every 30 seconds when the unit has registered a speed over ground (SOG) of less than 3 knots for more than 3 minutes and once every 15 seconds when SOG is 3 knots or greater.

NOTE: The Message 1 two (2) bit REPEAT INDICATOR field, normally located between FUNCTION ID and USER ID, is omitted in the EAIS Position Report Payload (See below).

Parameter	Number of bits	Description	Encryption Status
DAC	10	Identifier for this message: 366	Unencrypted
Function ID	6	Function Identifier: 56	Unencrypted
Repeat Indicator	0	Not present in EAIS Position Report Payload	no bits
User ID	30	MMSI number.	AES encrypted
Navigational Status	4	0 = under way using engine 1 = at anchor 2 = not under command 3 = restricted maneuverability 4 = constrained by her draught 5 = moored 6 = aground 7 = engaged in fishing 8 = under way sailing 9 = reserved for future amendment of navigational status for ships carrying DG, HS, or MP, or IMO hazard or pollutant category C, high speed craft (HSC), 10 = reserved for future amendment of navigational status for ships carrying dangerous goods (DG), harmful substances (HS) or marine pollutants (MP), or IMO hazard or pollutant category A, wing in ground (WIG); 11 = power driven vessel towing astern (regional use), 12 = power-driven vessel pushing ahead or towing alongside (regional use); 13 = reserved for future use, 14 = AIS-SART (active), MOB-AIS, EPIRB-AIS 15 = undefined = default (also used by AIS-SART, MOB-AIS and EPIRBAIS under test)	AES encrypted

Parameter	Number of bits	Description	Encryption Status
Rate of turn ROTAIS	8	0 to +126 = turning right at up to 708° per min or higher 0 to –126 = turning left at up to 708° per min or higher Values between 0 and 708° per min coded by ROTAIS = 4.733 SQRT(ROTsensor) degrees per min where ROTsensor is the Rate of Turn as input by an external Rate of Turn Indicator (TI). ROTAIS is rounded to the nearest integer value. +127 = turning right at more than 5° per 30 s (No TI available) –127 = turning left at more than 5° per 30 s (No TI available) –128 (80 hex) indicates no turn information available (default). ROT data should not be derived from COG information.	AES encrypted
SOG	10	Speed over ground in 1/10 knot steps (0-102.2 knots) 1023 = not available, 1022 = 102.2 knots or higher.	AES encrypted
Position Accuracy	1	The position accuracy (PA) flag 1 = high (≤ 10 m) 0 = low (>10 m) 0 = default	AES encrypted
Longitude	28	Longitude in 1/10 000 min (±180 degrees, East = positive, West = negative. 181 degrees (6791AC0 hex) = not available = default)	AES encrypted
Latitude	27	Latitude in 1/10 000 min (±90 degrees, North = positive, South = negative, 91 degrees (3412140 hex) = not available = default)	AES encrypted
COG	12	Course over ground in 1/10° (0-3599). 3600 (E10 hex) = not available = default; 3 601 – 4 095 should not be used.	AES encrypted
True Heading	9	Degrees (0-359) (511 indicates not available = default).	AES encrypted
Time Stamp	6	UTC second when the report was generated by the electronic position system (EPFS) (0-59, or 60 if time stamp is not available, which should also be the default value, or 61 if positioning system is in manual input mode, or 62 if electronic position fixing system operates in estimated (dead reckoning) mode, or 63 if the positioning system is inoperative)	AES encrypted

Parameter	Number of bits	Description	Encryption Status
Special maneuver indicator	2	0 = not available = default 1 = not engaged in special maneuver 2 = engaged in special maneuver (i.e. regional passing arrangement on Inland Waterway)	AES encrypted
Spare	3	Not used. Should be set to zero.	AES encrypted
RAIM-Flag	1	RAIM (Receiver Autonomous Integrity Monitoring) flag of Electronic Position Fixing Device; 0 = RAIM not in use = default; 1 = RAIM in use)	AES encrypted
Communication State	19	MSG ID 1 & 2 = SOTDMA communication state as described in 1371-5, Annex 2 MSG ID 3 ITDMA communication state as described in 1371-5, Annex 2	AES encrypted
Checksum	8	Exclusive OR (XOR) 8-bit	AES encrypted
Stuffed bits	88	Stuffed bits are inserted so that the number of bits in the encrypted field is a multiple of 128 bits (256 for this message); set to zero.	AES encrypted
TOTAL	**272**	16 unencrypted bits plus 256 encrypted bits	

3.6.2.3. Target Of Interest (TOI) PAYLOAD (2 slots total transmission length)

The TOI payload, prior to encryption, is 165 bits in length. Conforming to the AES Encryption scheme with a 128-bit cipher key, the encrypted part of the payload then effectively becomes 256 bits in length to create blocks of 128 bits. This results in a 2 slot broadcast binary message.

NOTE: TOI messages are repeated every 15 seconds, until cancelled locally. Cancelling a TOI locally stops transmission of TOI message repetitions. Remote units receiving a TOI will apply Lost Target/Auto Drop processing rules to remove the TOI designation from a target.

Parameter	Number of bits	Description	Encryption Status
DAC	10	Identifier for this message: 366	Unencrypted
Function ID	6	Function Identifier: 58	Unencrypted
Source ID (MMSI)	30	Source MMSI number.	AES encrypted
Target Type	4	1 = AIS, 2 = ARPA, 3 = Dead Reckoned	AES encrypted
Target ID	30	MMSI if type is 1, Sender generated ID otherwise	AES encrypted
SOG	10	Speed over ground in 1/10 knot steps (0-102.2 knots) 1023 = not available, 1022 = 102.2 knots or higher.	AES encrypted
Longitude	28	Longitude in 1/10 000 min (±180 degrees, East = positive, West = negative. 181 degrees (6791AC0 hex) = not available = default)	AES encrypted
Latitude	27	Latitude in 1/10 000 min (±90 degrees, North = positive, South = negative, 91 degrees (3412140 hex) = not available = default)	AES encrypted
COG	12	Course over ground in 1/10 (0-3599). 3600 (E10 hex) = not available = default; 3 601 – 4 095 should not be used.	AES encrypted
Checksum	8	Exclusive OR (XOR) 8-bit	AES encrypted
Stuffed bits	107	Stuffed bits are inserted so that the number of bits in the encrypted field is a multiple of 128 bits (256 for this message); set to zero.	AES encrypted
TOTAL	**272**	16 unencrypted bits plus 256 encrypted bits	

3.6.2.4. Text Message Payload (variable [2-5 slots] total transmission length)

The Text Message Payload, prior to encryption, varies from 74 to 896 bits in length. Conforming to the AES Encryption scheme with a 128-bit cipher key, the encrypted part of the payload then effectively becomes 128, 256, 384, 512, 640, 768 or 896 bits in length to create blocks of 128 bits.

Parameter	Number of bits	Description	Encryption Status
DAC	10	Identifier for this message: 366	Unencrypted
Function ID	6	Function Identifier: 55	Unencrypted
Source ID (MMSI)	30	Source MMSI number.	AES encrypted
Acknowledgement Flag	1	Reserved for future use.	AES encrypted
Segment Number	11	Reserved for future use.	AES encrypted
Text length	8	Length of Text Message	AES encrypted
Text Message	0-822 Variable	User Text Message (6 bits times 0-137 characters)	AES encrypted
Checksum	8	Exclusive OR (XOR) 8-bit	AES encrypted
Stuffed bits	Variable	Variable; stuffed bits are inserted so that the number of bits in the encrypted field is a multiple of 128 bits; set to zero.	AES encrypted
TOTAL	**144 272 400 528 656 784 912**	16 unencrypted bits plus 128, 256, 384, 512, 640, 768 or 896 encrypted bits	

Considering the constraints imposed by the AES encryption algorithm and recommended bit-stuffing guidelines contained in Section 3.2.2.1 of Annex 2 to ITU-R M.1371-5, this results in the following slot usage as a function of number of 6-bit ASCII characters:

Number of Slots	Number of 6-bit ASCII characters
1	not possible to have a 1-slot message
2	0 - 30
3	31 - 73
4	74 - 115
5	116 - 137

ANNEX 2

Technical Characteristics for an Encrypted Automatic Identification System (EAIS) to meet Sensitive But Unclassified (SBU) Tactical Information Exchange and Display System (STEDS) Requirements

(Version 5.0)

ANNEX 1 of ITU-R M.1371-5

1 GENERAL

Coast Guard EAIS operates in accordance with ITU-R M.1371-5, “Technical Characteristics for a Universal Shipborne Automatic Identification System (AIS) Using Time Division Multiple Access (TDMA) in the VHF Maritime Mobile Band”. Specific deviations and amplifying details required to implement EAIS are contained in this document.

ANNEX 2 of ITU-R M.1371-5

2 PHYSICAL LAYER

This section adheres to Part 2 of Annex 2 to ITU-R M.1371-5.

3 LINK LAYER

This section adheres to Part 3 of Annex 2 to ITU-R M.1371-5, with the following exceptions:

3.1.6 Slot State

The definition of “externally allocated” shall be expanded to include slots identified in the “communications state” field of received EAIS Message 25 (FID 0 - position report). Slots allocated in this way shall be identified as “externally allocated” in the transponder’s frame map.

3.1.6.1 Modify Definition of a Free Slot for EAIS “Polite” Operation

The definition of a free slot, as presented in ITU-R M.1371-5, Annex 2, Paragraph 3.1.6, is further refined such that an unreserved slot must also have a received signal strength level, based on the previous frame received signal strength level, that is less than the current CS Detection Threshold, as described in ITU-R M.1371-5, Annex 7, Paragraph 4.3.1.3. This eliminates the possibility of incorrectly identifying a “blurred” slot (two vessels transmitting during the same time slot and received by own-ship with less than 10 dB received signal strength level difference) as a free slot.

3.3.2. Modes of Operation

Add the following explanation to transponder modes of operation:

3.3.2.4. Normal

When in this mode of operation the AIS transponder defaults to operate in Autonomous & Continuous mode, unless switched to Assigned or Polled mode. The transponder sends and receives AIS messages and EAIS messages.

3.3.2.5. Receive-Only

When in this mode of operation the AIS transponder does not transmit any AIS messages, regardless of any commands received from base stations or interrogations from other vessels. The transponder receives AIS messages and EAIS messages, but transmits nothing (maintaining radio silence).

3.3.2.6. Restricted

When in this mode of operation the AIS transponder only transmits EAIS messages, while no non-EAIS messages are sent. The transponder continues to receive AIS messages and EAIS messages.

3.3.8. EAIS Slot Usage

Total number of bits in assembled EAIS message determines # of slots:

0-128	→	1 slot
129-384	→	2 slots
385-640	→	3 slots
641-896	→	4 slots
897-1152	→	5 slots

4. NETWORK LAYER

This section adheres to Part 4 of Annex 2 to ITU-R M.1371-5, with the following exceptions:

4.1.10. Operating Frequency Channels

When operating in Receive-Only or Restricted mode, as defined in Section 3.3.2. of this Annex, the AIS transponder shall operate exclusively on the normal AIS frequencies and shall not respond to base station or digital selective calling commands to change frequencies.

4.3.3. Restricted Mode Report Rates (Rr)

4.3.3.1. Dynamic Position Report

4.3.3.1.1. < 3 knots: When operating in the Restricted Mode (as defined in Section 3.3.2. of this Annex), Report Rate for BFT Dynamic Position Reports (Message 25, FIDs 0 & 3) shall be 30 seconds when Speed Over Ground (SOG) is less than 3 knots for more than 3 minutes.

4.3.3.1.2. > 3 knots: When operating in the Restricted Mode (as defined in Section 3.3.2. of this Annex), Report Rate for BFT Dynamic Position Reports (Message 25, FIDs 0 & 3) shall be 15 seconds when Speed Over Ground (SOG) is greater than 3 knots.

4.3.3.2. Static Data Report

When operating in the Restricted Mode (as defined in Section 3.3.2. of this Annex), Report Rate for BFT Static Data Report (Message 25, FID 1) shall be 6 minutes and upon change.

4.3.3.3 Target of Interest (TOI) Message

When operating in the Restricted Mode (as defined in Section 3.3.2 of this Annex). Report Rate for the PI generated Target of Interest (TOI) message shall be every 15 seconds until canceled.

5. TRANSPORT LAYER

This section adheres to Part 5 of Annex 2 to ITU-R M.1371-5, with the following exceptions:

5.4.1 Presentation Interface (PI) Protocol

Coast Guard EAIS Transponder and Presentation Interface functional roles are as follows:

Transmit		
Functional Role	Transponder	Presentation Interface
Generate, format (bit stuff & generate check sum), & encrypt EAIS data payloads	Message 25: FID 0, 1, & 3 Message 26: None Messages 25 (FID2) & 26: Encrypted data payloads received from the PI in ABM (addressed) & BBM (Broadcast) messages are inserted into Messages 25 (FID2) & 26 for transmission.	Message 25: FID 2 Message 26: All Messages 25 (FID2) & 26: Encrypted data payload is generated in the PI and sent to the transponder using ABM (addressed) & BBM (Broadcast).
Transmit on the VDL	All	None

Receive		
	Transponder	Presentation Interface
Receive over the VDL	All	None
Decrypt & Parse	Message 25: FID 0 & 3 (in order to produce and maintain the Frame Map using EAIS payload “communications state” fields) Message 26: None Messages 25 & 26: All messages are “passed-through” to the PI in encrypted format using VDM message. [Exception: “ALLOW COTS” see 5.4.3.2.]	Message 25: All Message 26: All Message 25 & 26: All messages are decrypted, parsed, and displayed by the PI.

5.4.2. EAIS Overhead Data

5.4.2.1. VDM

VDM messages sent from the Transponder to the PI include the 40 bits (Message 25), 64 bits (Message 26 Broadcast), or the 96 bits (Message 26 Addressed) unencrypted overhead data situated ahead of the encrypted payload.

5.4.2.2. ABM & BBM

ABM & BBM messages sent from the PI to the Transponder do not include unencrypted overhead data. Only the encrypted data portion is sent.

5.4.3. EAIS Position Report and Static Data Report Decryption

The EAIS Transponder shall have two modes of Position Report Decryption: “Standard” and “Allow COTS”.

5.4.3.1. Standard

When “Standard” is selected, EAIS position report data remains encrypted as it is sent to the PI. This mode is for use with an EAIS capable PI only. If this mode is used with a non-EAIS capable PI (COTS), encrypted targets will not be displayed.

5.4.3.2. Allow COTS

When “Allow COTS” is selected, EAIS Position Report data and Static Data Report data shall be decrypted by the Transponder and converted to standard VDM messages before it is sent to the PI interface. This allows the non-EAIS capable PI to display blue force tracks as normal AIS targets.

5.4.4. CRC Checksum Computation

When computing the 16-bit CRC checksum, the CRC-CCITT method is used, with a polynomial of 0x1021. All the bits before the checksum are used, starting with the Function ID. The number of bits will always be a multiple of 16.

ANNEX 8 of ITU-R M.1371-5

2. Message Summary

2.1 STEDS Message Summary

Msg ID	Name	Description	Category	Priority	Op mode	Access scheme	Comm state	M/B
25	Single-Slot Binary Message	One-slot binary messages	F	4	AU	ITDMA SOTDMA	N/A	M/B
26	Multi-Slot Binary Message with Comms State	Multi-slot multi-purpose messages with Communications State	F	4	AU	ITDMA SOTDMA	ITDMA	M/B

3. Message Descriptions

3.23. Message 25: Single-Slot Binary

This message is used to exchange operational information, including but not limited to position reports (own-vessel/aircraft position, course & speed), static data (own-vessel/aircraft name & type), and acknowledgement of addressed messages. The message is designed to allow transmission of data in 128-bit Advanced Encryption Standard (AES) encrypted blocks, one block per single-slot transmission. This minimizes STEDS' footprint on the AIS VDL while maximizing the chance of successful message transmission.

# of bits	40	128
Field Name	Message 25 Overhead	Binary Data

# of bits	6	2	30	1	1
Field Name	Msg ID	Rpt. Ind.	MMSI	Destination indicator	Binary data flag

Parameter	Number of bits	Description	Encryption Status
Message ID	6	Identifier for Message 25; always 25	Unencrypted
Repeat indicator	2	Used by the repeater to indicate how many times a message has been repeated. 0-3; 0 = default; 3 = do not repeat any more	Unencrypted
MMSI	30	MMSI number of source station of message	Unencrypted
Destination indicator	1	0=Broadcast (Destination indicator of 1 is not used in STEDS message 25.)	Unencrypted
Binary data flag	1	0 = unstructured binary data (Always zero for all STEDS messages).	Unencrypted
Binary Data	128	Payload Note: Any unused bits set to zero.	AES encrypted Binary Data
TOTAL	**168**	40 unencrypted bits plus 128 encrypted bits	

3.23.1 Payload Format

The following sections detail the currently defined (FIDs 0-3) Message 25 payload content options which have been designed specifically to meet USCG STEDS Operational Requirements. There exist an additional 28 unassigned Function ID (FID) numbers available for definition of additional payloads, as may be required in the future. The payloads will be AES-encrypted to protect Sensitive but Unclassified (SBU) information.

3.23.1.1 Position Report for Vessels (FID 0)

Position Report for Vessels (FID 0) and Position Report for Aircraft (FID 3) are the only Message 25 payloads that include a 20-bit encrypted ITDMA Communications State. This allows STEDS units to maintain awareness of the planned activity of other STEDS users, thereby avoiding multiple STEDS transmissions during any one slot. Despite this self-organization among STEDS users, they will continue to yield to non-STEDS Class A traffic, who will "see" STEDS transmissions as strictly well-behaved transmissions on the VDL. The FID 0 and FID 3 position reports shall be transmitted once every 30 seconds when the unit has registered a speed over ground (SOG) of less than 3 knots for more than 3 minutes and once every 15 seconds when SOG is 3 knots or greater.

Parameter	Number of bits	Description	Encryption Status
Function ID	5	0 = Position report	AES encrypted
Operating Mode	1	0 = Autonomous 1 = Fixed	AES encrypted
Navigational Status	4	0 = under way using engine 1 = at anchor 2 = not under command 3 = restricted maneuverability 4 = constrained by her draught 5 = moored 6 = aground 7 = engaged in fishing 8 = under way sailing 9 = reserved for future amendment of navigational status for ships carrying DG, HS, or MP, or IMO hazard or pollutant category C, high speed craft (HSC), 10 = reserved for future amendment of navigational status for ships carrying dangerous goods (DG), harmful substances (HS) or marine pollutants (MP), or IMO hazard or pollutant category A, wing in ground (WIG); 11 = power driven vessel towing astern (regional use), 12 = power-driven vessel pushing ahead or towing alongside (regional use); 13 = reserved for future use, 14 = AIS-SART (active), MOB-AIS, EPIRB-AIS 15 = undefined = default (also used by AIS-SART, MOB-AIS and EPIRBAIS under test)	AES encrypted

Parameter	Number of bits	Description	Encryption Status
Hour of position	5	0-23	AES encrypted
Minute of position	6	0-59	AES encrypted
Second of position	6	0-59	AES encrypted
Longitude	25	Longitude in 1/1000 min (±180 degrees, East = pos; West = neg 181 degrees = not available = default)	AES encrypted
Latitude	24	Latitude in 1/1000 min (±90 degrees, North = pos; South = neg, 91 degrees = not available = default)	AES encrypted
COG	9	Course over ground (0-359°). (511 indicates not available = default).	AES encrypted
SOG	7	Speed over ground in knots (0-126 knots) with 127 = not available (default) and 126 = 126 knots or higher.	AES encrypted
Communication state selector flag	1	0 = SOTDMA communications state 1 = ITDMA communications state	AES encrypted
Communications State	19	Per Annex 2 to ITU-R M.1371-5 para 3.3.7.2.2 (SOTDMA) and 3.3.7.3.2 (ITDMA).	AES encrypted
Encryption checksum	16	Cyclic Redundancy Check (CRC) 16-bit polynomial	AES encrypted
TOTAL	**128**	128 encrypted bits	

3.23.1.2 Static Data Report for Vessels and Aircraft (FID 1)

Static Data Reports for Vessels and Aircraft (FID 1) are transmitted once every 6 minutes and matched with FID 0 or FID 3 messages using the sender MMSI number to provide additional information about a STEDS Vessel or Aircraft unit.

Parameter	Number of bits	Description	Encryption Status
Function ID	5	1 = Static data report	AES encrypted
Asset Name	96	Maximum 16 characters 6 bit ASCII, "@@@@@@@@@@@@@@@@ " = not available = default. All unused bits set to zero	AES encrypted
Asset Type	10	0-1023 Numeric asset type from table in Annex 5	AES encrypted
DTE	1	Data terminal ready 0 = available, 1 = not available = default	AES encrypted
Checksum	16	Cyclic Redundancy Check (CRC) 16-bit polynomial.	AES encrypted
TOTAL	**128**	128 encrypted bits	

3.23.1.3 Addressed Message Acknowledgement (FID 2)

This Message 25 payload is used to acknowledge reception of the Addressed Text Message, Addressed TOI or Addressed Overlay (Message 26, FIDs 0-3). FID 2 shall always be transmitted after receipt of the complete Addressed Message.

Parameter	Number of bits	Description	Encryption Status
Function ID	5	2 = Text message acknowledgement	AES encrypted
MMSI	30	MMSI number of addressed message originator	AES encrypted
Type of Acknowledgement	2	0 = Text Message 1 = TOI Message 2 = Overlay Message 3 = undefined	AES encrypted
Hour	5	0-23 Hour of acknowledged message	AES encrypted
Minute	6	0-59 Minute of acknowledged message	AES encrypted
Second	6	0-59 Second of acknowledged message	AES encrypted
Hour	5	0-23 Hour of this acknowledgement	AES encrypted
Minute	6	0-59 Minute of this acknowledgement	AES encrypted
Second	6	0-59 Second of this acknowledgement	AES encrypted
TOI Number	20	TOI ID number assigned by designating unit; used for TOI acknowledgements only	AES encrypted
Overlay Number	5	Overlay ID number assigned by originating unit; used for Overlay acknowledgements only	AES encrypted
Unused bits set to zero	16	Unused bits set to zero.	AES encrypted
Checksum	16	Cyclic Redundancy Check (CRC) 16-bit polynomial.	AES encrypted
TOTAL	**128**	128 encrypted bits	

3.23.1.4 Position Report for Aircraft (FID 3)

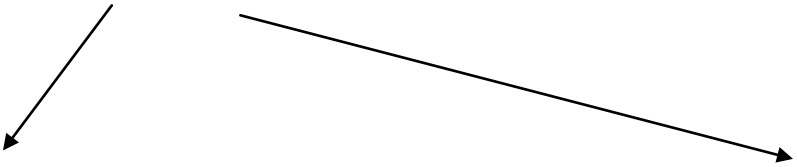
Position Report for Vessels (FID 0) and Position Report for Aircraft (FID 3) are the only Message 25 payloads that include a 20-bit encrypted ITDMA Communications State. This allows STEDS units to maintain awareness of the planned activity of other STEDS users, thereby avoiding multiple STEDS transmissions during any one slot. Despite this self-organization among STEDS users, they will continue to yield to non-STEDS Class A traffic, who will "see" STEDS transmissions as strictly well-behaved transmissions on the VDL. The FID 0 and FID 3 position reports will be transmitted once every 30 seconds when the unit has registered a speed over ground (SOG) of less than 3 knots for over 3 minutes and once every 15 seconds when SOG is 3 knots or greater.

Parameter	Number of bits	Description	Encryption Status
Function ID	5	3 = Aircraft position report	AES encrypted
Operating Mode	1	0 = Autonomous 1 = Fixed	AES encrypted
Altitude	12	Defined in Message 9 of ITU-R M.1371-5	AES encrypted
Time stamp	6	Defined in Message 9 of ITU-R M.1371-5	AES encrypted
Longitude	25	Longitude in 1/1000 min (±180 degrees, East = pos; West = neg 181 degrees = not available = default)	AES encrypted
Latitude	24	Latitude in 1/1000 min (±90, degrees, North = pos; South = neg 91 degrees = not available = default)	AES encrypted
COG	9	Course over ground (0-359°). (511 indicates not available = default).	AES encrypted
SOG	10	Defined in Message 9 of ITU-R M.1371-5	AES encrypted
Communication state selector flag	1	0 = SOTDMA communications state 1 = ITDMA communications state	AES encrypted
Communications State	19	Per Annex 2 to ITU-R M.1371-5 para 3.3.7.2.2 (SOTDMA) and 3.3.7.3.2 (ITDMA).	AES encrypted
Encryption checksum	16	Cyclic Redundancy Check (CRC) 16-bit polynomial	AES encrypted
TOTAL	**128**	128 encrypted bits	

3.24 Message 26: Multi-Slot Multi-Purpose Binary with Communications State

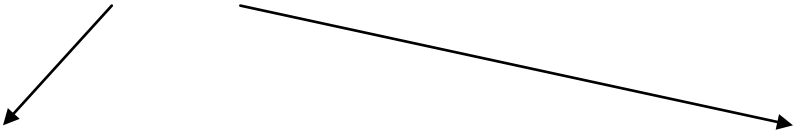
This message is used to exchange operational information, including Text Message, Addressed or Broadcast (FID 0); Target of Interest (TOI), Addressed or Broadcast (FID 1); Expanding Square, Sector, Parallel Line & Creeping Line Search & Rescue (SAR) Pattern or Circle, Overlay Option 1 (FID 2); and Track Line Search Pattern, Route or Polygon, Overlay Option 2 (FID 3). Transmission of multi-slot messages via Message 26 reduces the total slot usage by about half as compared to breaking the message up into multiple occurrences of Message 25, due to a significant reduction in the number of required overhead bits. The Message 26 structure allows for either broadcast or addressed message variants, as well as a communications state transmitted in the clear. NOTE: When an addressed format is used, repeat send until message 25 FID 2 received or up to 4 times, whichever occurs first.

Broadcast Message 26 **# of bits**	44	128 256 384 512 640 768 896	20
Field Name	Message 26 Overhead	Binary Data (includes bit stuffing)	Comms State



# of bits	6	2	30	1	1	0	4
Field Name	Msg ID	Repeat Indicator	MMSI	Destination indicator	Binary Data Flag	Destination ID	Spare Bits

Addressed Message 26 **# of bits**	76	128 256 384 512 640 768 896	20
Field Name	Message 26 Overhead	Binary Data (includes bit stuffing)	Comms State



# of bits	6	2	30	1	1	30	6
Field Name	Msg ID	Repeat Indicator	MMSI	Destination indicator	Binary Data Flag	Destination ID	Spare Bits

3.24.1 "Message Content" is only encrypted field. General format for Message 26 is:

Parameter	Number of bits (Broadcast)	Number of bits (Addressed)	Description
Message ID (unencrypted)	6	6	Identifier for Message 26; always 26
Repeat indicator (unencrypted)	2	2	Used by the repeater to indicate how many times a message has been repeated. 0-3; 0 = default; 3 = do not repeat any more
MMSI (unencrypted)	30	30	MMSI number of source station of message
Destination indicator (unencrypted)	1	1	0=Broadcast (no Destination ID field used) 1=Addressed (Destination ID uses 30 data bits for MMSI)
Binary data flag (unencrypted)	1	1	0 = unstructured binary data (Always zero for all STEDS messages).
Destination ID (unencrypted)	0	30	MMSI of addressed station
Spare bits (unencrypted)	4	6	Set to Zero
Message Content (Encrypted) STEDS FID 0-3 defined message Multiples of 128 bits	128 256 384 512 640 768 896	128 256 384 512 640 768 896	The length of Message Content is fundamentally a function of the length of the FID 0-3 message to be encapsulated plus the checksum, with bit stuffing to arrive at the next 128 bit increment (128 bit increments are necessitated by AES encapsulation). Unused bits set to zero are inserted after FID message 0-3 data and before the checksum. The number of unused bits set to zero is equal to the number of bits required to arrive at the next 128 increment. CRC checksum data always occupies the final 16 bits of Message Content.
Communication state selector flag (unencrypted)	1	1	0 = SOTDMA communications state 1 = ITDMA communications state
Communications State (unencrypted)	19	19	Per Annex 2 to ITU-R M.1371-5 para 3.3.7.2.2 (SOTDMA) and 3.3.7.3.2 (ITDMA).
TOTAL	**192** **320** **448** **576** **704** **832** **960**	**224** **352** **480** **608** **736** **864** **992**	Broadcast : 44 unencrypted bits plus 128, 256, 384, 512, 640, 768 or 896 encrypted bits plus 20 bits unencrypted Comm State. Addressed: 76 unencrypted bits; plus 128, 256, 384, 512, 640, 768 or 896 encrypted bits; plus 20 bits unencrypted Comm State.

3.24.2 Payload Format (the Message Content (Encrypted))

The following sections detail the currently defined (FIDs 0-3) Message 26 payload content options which have been designed specifically to meet USCG STEDS Operational Requirements. There exist 28 additional unassigned Function ID (FID) numbers available for definition of additional payloads, as may be required in the future. The payloads will be AES-encrypted to protect SBU information.

3.24.2.1 Text Message, Addressed or Broadcast (FID 0)

The STEDS Message 26 Text Message format provides for both a broadcast and addressed text message. The text may be up to 141 6-bit ASCII characters (up to 846 bits). Message addressing, when required, shall be performed using the Destination Indicator and Destination ID fields inherent to the Message 26 structure.

Parameter	Number of bits	Description	Encryption Status
Function ID	5	0 = Text Message	AES encrypted
Hour	5	0-23	AES encrypted
Minute	6	0-59	AES encrypted
Second	6	0-59	AES encrypted
Text Length	8	Length of the text message, expressed as the number of 6-bit ASCII characters	AES encrypted
Text	0-846 bits Variable	Maximum number of 6-bit ASCII characters is 141 for both message types.	AES encrypted
Unused bits set to zero	Variable	Unused bits set to zero are inserted so that the number of bits in the encrypted field is a multiple of 128 bits.	AES encrypted
Checksum	16	Cyclic Redundancy Check (CRC) 16-bit polynomial	AES encrypted
TOTAL	**128 256 384 512 640 768 896**	128, 256, 384, 512, 640, 768 or 896 encrypted bits	AES encrypted

3.24.2.2 Target of Interest (TOI), Addressed or Broadcast (FID 1)

The STEDS Message 26 TOI Message format provides for both a broadcast and addressed TOI message variation. The text may be up to 121 6-bit ASCII characters (up to 726 bits). Addressing, when required, shall be performed using the Destination Indicator and Destination ID fields inherent to the Message 26 structure.

NOTE: TOI messages repeat every 15 seconds, until cancelled locally or a cancellation message is received. Cancelling a TOI locally stops transmission of TOI message repetitions and transmits a cancellation message. In the absence of a cancelation message, remote units receiving a TOI will apply Lost Target/Auto Drop processing rules the TOI designation from a target. Cancellation messages repeat four (4) times, 15 seconds apart.

Parameter	Number of bits	Description	Encryption Status
Function ID	5	1 = TOI Report	AES encrypted
Target Type	4	1 = AIS, 2 = Radar, 3 = Manual/Other, 4-15 = undefined	AES encrypted
Target ID	20	Sender generated ID.	AES encrypted
MMSI	30	MMSI number of the TOI, if contact type is “AIS”; otherwise all zeros	AES encrypted
TOI Status Designator	1	0 = cancel; 1 = active	AES encrypted
Hour	5	0-23	AES encrypted
Minute	6	0-59	AES encrypted
Second	6	0-59	AES encrypted
Longitude	25	Longitude in 1/1000 min (±180 degrees, East = positive, West = negative. 181 degrees = not available = default)	AES encrypted
Latitude	24	Latitude in 1/1000 min (±90 degrees, North = positive, South = negative, 91 degrees = not available = default)	AES encrypted
COG	9	Course over ground (0-359°). (511 indicates not available = default).	AES encrypted
SOG	7	Speed over ground in knots (0-126 knots) with 127 = not available (default) and 126 = 126 kts or higher.	AES encrypted
Length of Text	8	Length of the text message, expressed as the number of 6-bit ASCII characters	AES encrypted
Text	0-726 bits Variable	Maximum number of 6-bit ASCII characters is 121.	AES encrypted
Unused bits set to zero	Variable	Unused bits set to zero are inserted so that the number of bits in the encrypted field is a multiple of 128 bits.	AES encrypted
Checksum	16	Cyclic Redundancy Check (CRC) 16-bit polynomial	AES encrypted
TOTAL	**128 256 384 512 640 768 896**	128, 256, 384, 512, 640, 768 or 896 encrypted bits	AES encrypted

3.24.2.3 Expanding Square, Sector, Parallel Line & Creeping Line Search & Rescue (SAR) Pattern or Circle, Overlay Option 1 (FID 2)

The STEDS Message 26 Overlay Option 1 Message format provides for both a broadcast and addressed Expanding Square, Sector, Parallel Line, Creeping Line or Circle overlay message variation. Addressing, when required, shall be performed using the Destination Indicator and Destination ID fields inherent to the Message 26 structure.

Parameter	Number of bits	Description	Encryption Status
Function ID	5	2 = Overlay, Option 1	AES encrypted
Overlay Type	4	0 = Expanding Square 1 = Sector 2 = Parallel Line 3 = Creeping Line 4-5 = not allowed [for use with FID 3] 6 = Circle 7-15 = undefined	AES encrypted
Overlay Number	5	Sender generated (0-31)	AES encrypted
Center/Origin Longitude	25	Longitude to nearest 1/1000 min (±180 degrees; East = positive; West = negative; 181 degrees = not available = default) [± 1.8 meter accuracy]	AES encrypted
Center/Origin Latitude	24	Latitude to nearest 1/1000 min (±90 degrees; North = positive; South = negative; 91 degrees = not available = default) [± 1.8 meter accuracy]	AES encrypted
Radius/Length	17	0000.01-1310.72 nautical miles; Radius dimension for Expanding Square, Sector & Circle Overlays, Length dimension for Parallel & Creeping Line Overlays	AES encrypted
Width	17	Width 0000.01-1310.72 nautical miles; 0000.00 = not Parallel Line or Creeping Line Pattern	AES encrypted
Orientation	9	Major axis direction in degrees (0-359);	AES encrypted
Number of sectors	7	Number of sectors, up to 128; 0 = not a Sector Pattern	AES encrypted
Track Spacing	14	Track Spacing 000.01-163.84; 000.00 = Sector Pattern, Polygon or single trackline	AES encrypted
First turn	1	0 = left; 1 = right	AES encrypted
Search Speed	10	Specified search speed in knots; 0 = default = not applicable/specified.	AES encrypted
Search Altitude	12	Specified search altitude in feet; 0 = default = not applicable/specified.	AES encrypted
Unused bits set to zero	90	Unused bits set to zero are inserted so that the number of bits in the encrypted field is a multiple of 128 bits.	AES encrypted
Checksum	16	Cyclic Redundancy Check (CRC) 16-bit polynomial	AES encrypted
TOTAL	**256**	256 encrypted bits	AES encrypted

3.24.2.4 Track Line Search Pattern, Route or Polygon, Overlay Option 2 (FID 3)

The STEDS Message 26 Overlay Option 2 Message format provides for both a broadcast and addressed Track Line or Polygon overlay message variation. Addressing, when required, shall be performed using the Destination Indicator and Destination ID fields inherent to the Message 26 structure.

Parameter	Number of bits	Description	Encryption Status
Function ID	5	3 = Overlay, Option 2	AES encrypted
Overlay Type	4	0-3 = not allowed [for use with FID 2] 4 = Track Line Search Pattern or Route; 5 = Polygon 6 = not allowed [for use with FID 2]; 7-15 = undefined	AES encrypted
Overlay Number	5	Sender generated (0-31)	AES encrypted
Origin Longitude	25	Longitude to nearest 1/1000 min (±180 degrees; East = positive; West = negative; 181 degrees = not available = default) [± 1.8 meter accuracy]	AES encrypted
Origin Latitude	24	Latitude to nearest 1/1000 min (±90 degrees; North = positive; South = negative; 91 degrees = not available = default) [± 1.8 meter accuracy]	AES encrypted
Number of Additional Waypoints	4	Number of additional waypoints for a Track Line or polygon overlay (maximum = 15);	AES encrypted
Additional Waypoints – Maximum of 15	Each: Lon = 25 Lat = 24 Up to 735 bits	Longitude to nearest 1/1000 min (±180 degrees; East = positive; West = negative; 181 degrees = not available = default) [±1.8 m accuracy Latitude to nearest 1/1000 min (±90 degrees; North = positive; South = negative; 91 degrees = not available = default) [±1.8 m accuracy]	AES encrypted
Search Speed	10	Specified search speed in knots; 0 = default = not applicable/specified.	AES encrypted
Search Altitude	12	Specified search altitude in feet; 0 = default = not applicable/specified.	AES encrypted
Unused bits set to zero	Variable	Unused bits set to zero are inserted so that the number of bits in the encrypted field is a multiple of 128 bits.	AES encrypted
Checksum	16	Cyclic Redundancy Check (CRC) 16-bit polynomial	AES encrypted
TOTAL	**128** **256** **384** **512** **640** **768** **896**	128, 256, 384, 512, 640, 768 or 896 encrypted bits	AES encrypted

ANNEX 3

NMEA-0183

1. Data Description

1.1. The EAIS Transponder may provide EAIS data to the Presentation Interface using NMEA-0183 version 4.10.

1.2. NMEA has granted the United States Coast Guard the following NMEA-0183 OEM Registration Code: UCG

1.3. The EAIS Transponder can operate in as normal Class-A transponder or in an Encrypted AIS (EAIS) mode.

1.4. Outputs from the EAIS Transponder are identified by the “AI” talker identifier in the NMEA 0183 address field.

1.5. In EAIS mode, the Transponder must be configured to use either Annex 1 (messages 6 and 8) or Annex 2 (Messages 25 & 26) on the VHF Data Link.

1.6. The EAIS Transponder and PI shall support the following NMEA-0183 Standard messages:

1.6.1. AIS Specific Messages:

ABK	AIS addressed and binary broadcast acknowledgement
ABM	AIS addressed binary and safety related (send only)
ACA	Channel assignment
ACK	Acknowledge Alarm
ACS	UAIS Channel Management information source
ALR	Alarm status
BBM	AIS broadcast binary message (send only)
SSD	Station static data
TXT	Text transmission
VDM	AIS VHF data-link message
VDO	AIS VHF data-link own-vessel report
VSD	Voyage static data

1.6.2. Sensor Integration Messages (Position; Speed; Heading; ROT):

DTM	Datum Reference
GBS	GNSS Satellite Fault Detection
GGA	Global Positioning System Fix Data
GLL	Geographic Position -- Latitude / Longitude
GNS	GNSS Fix Data
GRS	GNSS Range Residuals
GSA	GNSS DOP and Active Satellites
GST	GNSS Pseudorange Error Statistics
GSV	GNSS Satellites in View
HDT	Heading True
RMC	Recommended Minimum Specific GNSS Data
ROT	Rate of Turn
VBW	Dual Ground / Water Speed
VTG	Course Over Ground and Ground Speed
ZDA	Time and Date

1.7. The EAIS Transponder shall support the following NMEA-0183 proprietary messages:

PUCG,STEDS	STEDS configuration message
PUCG,KEY	Passphrase configuration message

Data Sentence	Sentence Description
PUCG STEDS	$PUCG,STEDS,c,x,x,x,x,x*hh Where: c = Query/Set/Reply status 1 x = Transmit Mode 2 x = Message Selection 3 x = NV Persist 4 x = Unit Type 5 x = Asset Type 6 Notes: 1) This field is used to indicate if this is a command sent to the AIS, if this is a query sent to the AIS or if this is a query reply from the AIS: 'S' – Command sent to the AIS to set the data in the AIS. 'Q' – Query sent to the AIS. 'R' – Query reply from the AIS. 2) Transmit Mode: '0' – Normal: When in this mode of operation the AIS transponder defaults to operate in Autonomous & Continuous mode, unless switched to Assigned or Polled mode. The transponder sends and receives AIS messages and EAIS messages.. '1' – Receive-Only: When in this mode of operation the AIS transponder does not transmit any AIS messages, regardless of any commands received from base stations or interrogations from other vessels. The transponder receives AIS messages and EAIS messages, but transmits nothing (maintaining radio silence). '2' – Restricted: When in this mode of operation the AIS transponder only transmits EAIS messages, while no non-EAIS messages are sent. The transponder continues to receive AIS messages and EAIS messages. 3) STEDS encrypted message selection. '0' – use VDL messages 25/26 for encrypted transmission. '1' – use VDL messaged 6/8 for encrypted transmissions. 4) Default Transmit Mode of Operation.. '0' – Transponder will default to last known Mode of Operation when power is cycled. '1' – Transponder will default to Restricted Mode of Operation when power is cycled. 5) Type of AIS Transponder. '0' – Vessel. '1' – Aircraft. 6) Asset Type. This field has a valid range of 0-1023 equating to asset types found in Annex 5.

Data Sentence	Sentence Description
PUCG KEY	$PUCG,KEY,x,x…x*hh Where: x = Key bits 1 x…x = AES key, Hex format 2 Note: 1) Key bit size. Valid sizes: '0' - 128, '1' – 192 '2' - 256 2) The AES Key. The AES Key is entered as an ASCII string, which represents the HEX value of the Key. The string length should be limited by the key size with the maximum string length being 64. Example: "4142435A" translates into a key value of 0x4142435A 3) This message is sent by transponder when key is entered or changed

ANNEX 4

NMEA-2000

1. Data Description

1.1. The EAIS Transponder may provide EAIS data to the Presentation Interface using NMEA-2000 or NMEA OneNet.

1.2. NMEA has granted the United States Coast Guard the following NMEA-2000 Registration Code: 591 (decimal)

1.3. The EAIS Transponder can operate in a normal Class-A mode or in an Encrypted AIS (EAIS) mode.

1.4. In EAIS mode, the Transponder must be configured to use either Annex 1 (messages 6 and 8) or Annex 2 (Messages 25 & 26) on the VHF Data Link.

1.5. The EAIS Transponder and PI shall support the following NMEA-2000 PGN messages contained in NMEA 2000 v1.201 Appendix B.1 – Parameter Groups Report:

1.5.1. AIS Specific Messages:

129038	AIS Class A position report
129039	AIS Class B position report
129040	AIS Class B extended position report
129041	AIS AtoN
129792	AIS DGNSS Broadcast Binary Message
129793	AIS UTC and Date Report
129794	AIS Class A static and voyage related data
129795	AIS addressed binary message
129796	AIS acknowledge
129797	AIS binary broadcast message
129798	AIS SAR aircraft position report
129800	AIS UTC/Date Inquiry
129801	AIS addressed safety related message
129802	AIS safety related broadcast message
129803	AIS Interrogation
129804	AIS Assignment Mode Command
129805	AIS Data Link Management Message
129806	AIS Channel Management
129807	AIS Group Assignment
129809	AIS Class B “CS” static data report, part A
129810	AIS Class B “CS” static data report, part B
129041	AIS AtoN

1.5.2. Sensor Integration Messages (Position; Speed; Heading; ROT):

128259	Speed, water referenced
129025	Position, rapid update
129029	GNSS position data
129044	Datum
129033	Time & date
129026	COG & SOG, rapid update
130577	Direction data
127250	Vessel heading
127251	Rate of Turn
130578	Vessel Speed Component for Speed

1.6. The EAIS Transponder shall support the following NMEA-2000 proprietary PGN message:

USCG STEDS Configuration Command/Report — PGN: 126720 hex: 1EF00

Fields 1 – 3 of this PGN defines this as an USCG Proprietary PGN.
Field 4 of this PGN defines the specific purpose and structure of this USCG Proprietary PGN.

The value of "0" in field 4 defines the as an USCG STEDS Configuration Command/Report.

This PGN supports encrypted AIS. The PGN is a USCG proprietary addressed PGN.

When sent as a command, the Command/Report field must be set to "0" meaning this is a configuration command to a device.

When sent as a report, the Command/Report field must be set to "1" meaning this is a configuration report from a device.

Required Behavior:
When sent as an addressed command to a device, the receiving device shall respond with this PGN as an addressed report, containing all configuration information (updated or not) as a consequence of receiving this PGN, or with an addressed Acknowledgement Group Function (PGN 126208) identifying the reason for the NAK. This enables the device sending this PGN as a command to determine success or failure of the intended configuration.

This PGN shall be sent as an addressed report in response to either an ISO Request PGN 059904 or Request Group Function PGN 126208.

When this PGN exceeds 223 data bytes (when the AES Encryption Key is greater then 512 bits long), the PGN is transmitted on NMEA 2000 using ISO Mullti-Packet TP.CM Protocol.

Single Frame:	N	Priority Default:	6	Default Update Rate:	milliseconds	Frequency:	NA cycles per second
Destination:	Address	Query Support:	Required	Command Support:	Prohibited	ACK Rqmnts:	Yes

Original Reference ID # 230

Field #	Field Name						
1	**Manufacturer Code**	Byte Field Size:				Request Parameter	Required
		Bit Field Size:	11			Command Parameter:	Prohibited
	DD154 Manufacturer's Code			Company identifier as specified by NMEA			
	DF52 Bit field	**bit(n)**	Range:	Variable	Resolution: 1		Used to construct bit fields
	This is always set to "591" and identifies the USCG as the owner of this PGN specification.						
2	**NMEA Reserved**	Byte Field Size:				Request Parameter	
		Bit Field Size:	resv 2			Command Parameter:	
	DD001 Reserved field			Variable number of reserved bits, all set to logic "1"			
	DF52 Bit field	**bit(n)**	Range:	Variable	Resolution: 1		Used to construct bit fields
	Used to align subsequent data on a byte boundary.						
3	**Industry Group**	Byte Field Size:				Request Parameter	Optional
		Bit Field Size:	3			Command Parameter:	Prohibited
	DD168 Industry Group			0 = Global; 1 = On-Highway; 2 = Agricultural and Forestry; 3 = Construction; 4 = Marine; 5 = Industrial - Process Control - Stationary (Gen-Sets) 6 = Reserved for SAE 7 = Reserved for SAE			
	DF52 Bit field	**bit(n)**	Range:	Variable	Resolution: 1		Used to construct bit fields
	Always set to "4" for Marine						

Version 2.001A — **USCG STEDS Configuration Command/Report**
Printed: 18-Apr-14 10:52 — **PGN: 126720**

USCG STEDS Configuration Command/Report — PGN: 126720 hex: 1EF00

4	**USCG PGN ID**		Byte Field Size:		Request Parameter	Required
			Bit Field Size:	8	Command Parameter:	Prohibited
	DD377 USCG PGN ID		0 = STEDS 1 – 253 = Reserved for future assignments 254 = Error 255 = Data not available			
	DF52 Bit field	**bit(n)**	Range:	Variable	Resolution: 1	Used to construct bit fields
5	**NMEA Reserved**		Byte Field Size:		Request Parameter	
			Bit Field Size:	resv 1	Command Parameter:	
	DD001 Reserved field		Variable number of reserved bits, all set to logic "1"			
	DF52 Bit field	**bit(n)**	Range:	Variable	Resolution: 1	Used to construct bit fields
	Used to align subsequent data on a byte boundary.					
6	**Command/Report Indicator**		Byte Field Size:		Request Parameter	Prohibited
			Bit Field Size:	3	Command Parameter:	Prohibited
	DD376 Command / Report		0 = Command 1 = Report 3 – 5 = Reserved 6 = Error 7 = Data not available			
	DF52 Bit field	**bit(n)**	Range:	Variable	Resolution: 1	Used to construct bit fields
7	**Transmit Mode of Operation**		Byte Field Size:		Request Parameter	Prohibited
			Bit Field Size:	3	Command Parameter:	Prohibited
	DD378 Transmit Mode of Operation		0 = Normal: When in this mode of operation the AIS transponder defaults to operate in Autonomous & Continuous mode, unless switched to Assigned or Polled mode. The transponder sends and receives AIS messages and eAIS messages. 1 = Receive-Only: When in this mode of operation the AIS transponder does not transmit any AIS messages, regardless of any commands received from base stations or interrogations from other vessels. The transponder receives AIS messages and eAIS messages, but transmits nothing (maintaining radio silence). 2 = Restricted: When in this mode of operation the AIS transponder only transmits eAIS messages, while no non-eAIS messages are sent. The transponder continues to receive AIS messages and eAIS messages. 3 – 5 = Reserved for future assignments 6 = Error 7 = Data not available			
	DF52 Bit field	**bit(n)**	Range:	Variable	Resolution: 1	Used to construct bit fields
8	**NMEA Reserved**		Byte Field Size:		Request Parameter	
			Bit Field Size:	resv 1	Command Parameter:	
	DD001 Reserved field		Variable number of reserved bits, all set to logic "1"			
	DF52 Bit field	**bit(n)**	Range:	Variable	Resolution: 1	Used to construct bit fields
	Used to align subsequent data on a byte boundary.					

9	**Encrypted Message Selection**		*Byte Field Size:*		*Request Parameter*	Prohibited
			Bit Field Size:	3	*Command Parameter:*	Prohibited
	DD379 Encrypted Message Selection		0 = ITU-R M.1371 Messages 25 and 26 1 = ITU-R M.1371 Messages 6 and 8 2 – 5 = Reserved for future assignments 6 = Error 7 = Data not available			
	DF52 Bit field	**bit(n)**	*Range:*	Variable	*Resolution:* 1	Used to construct bit fields
10	**Non Volatile Persistence**		*Byte Field Size:*		*Request Parameter*	Prohibited
			Bit Field Size:	3	*Command Parameter:*	Prohibited
	DD380 Non Volatile Persistence		0 = Transponder will default to last known Mode of Operation when power is cycled. 1 - Transponder will default to Restricted Mode of Operation when power is cycled. 2 -5 = Reserved for future assignments 6 = Error 7 = Data Not available			
	DF52 Bit field	**bit(n)**	*Range:*	Variable	*Resolution:* 1	Used to construct bit fields
11	**NMEA Reserved**		*Byte Field Size:*		*Request Parameter*	
			Bit Field Size:	resv 2	*Command Parameter:*	
	DD001 Reserved field		Variable number of reserved bits, all set to logic "1"			
	DF52 Bit field	**bit(n)**	*Range:*	Variable	*Resolution:* 1	Used to construct bit fields
	Used to align subsequent data on a byte boundary.					
12	**Type of AIS Asset**		*Byte Field Size:*		*Request Parameter*	Prohibited
			Bit Field Size:	3	*Command Parameter:*	Prohibited
	DD381 Type of AIS Asset		0 = Vessel 1 = Aircraft 2 -5 = Reserved for future assignment 6 = Error 7 = Data not available			
	DF52 Bit field	**bit(n)**	*Range:*	Variable	*Resolution:* 1	Used to construct bit fields
13	**AES Encryption Key Size**		*Byte Field Size:*		*Request Parameter*	Prohibited
			Bit Field Size:	3	*Command Parameter:*	Prohibited
	DD382 AES Encryption Key Size		0 = 128 bits 1 = 192 bits 2 = 256 bits 3 – 5 = Reserved for future assignment 6 = Error 7 = Data not available			
	DF52 Bit field	**bit(n)**	*Range:*	Variable	*Resolution:* 1	Used to construct bit fields

14	**NMEA Reserved**		*Byte Field Size:*			*Request Parameter*	
			Bit Field Size:	resv 2		*Command Parameter:*	
	DD001 Reserved field		Variable number of reserved bits, all set to logic "1"				
	DF52 Bit field	**bit(n)**	*Range:*	Variable	*Resolution:* 1	Used to construct bit fields	
	Used to align subsequent data on a byte boundary.						
15	**USCG Reserved**		*Byte Field Size:*			*Request Parameter*	
			Bit Field Size:	resv 16		*Command Parameter:*	
	DD001 Reserved field		Variable number of reserved bits, all set to logic "1"				
	DF52 Bit field	**bit(n)**	*Range:*	Variable	*Resolution:* 1	Used to construct bit fields	
	Purpose is to provide spare bits for future assignment.						
16	**AES Key**		*Byte Field Size:*	8 or 16		*Request Parameter*	Prohibited
			Bit Field Size:			*Command Parameter:*	Prohibited
	DD375 AES Encryption Key		This is an ASCII string containing Hex characters. A 128-bit Key would require 32 ASCII Hex characters for a total string size of 35 characters including the two count bytes and control byte. A 192-bit key would require 48 ASCII Hex characters for a total string size of 51 characters. A 256-bit key would require 64 ASCII Hex characters for a total string size of 67 characters. A 512-bit key would require 128 ASCII Hex characters for a total string size of 131 characters. A 1024-bit key would require 256 ASCII Hex characters for a total string size of 259 characters.				
	DF51 String, variable, medium	**ch8or16(n)**	*Range:*	0 to 1,782 ASCII or 0 to 891 Unicode Characters	*Resolution:* 1 ASCII or 1 Unicode Character	3 to 1,785 bytes. First and Second bytes in string (unit16) is the Count byte indicating the number of bytes in the string, including the Count and Control bytes. Third byte in string is the Control byte. The Control byte indicates if the string consists of ASCII characters (Char8) or Unicode characters (Char16). Control byte = 0 => Unicode characters Control byte = 1 => ASCII characters A string with no characters (total length of 3 bytes, i.e. Count = 3) is a null string.	
	This is an ASCII string containing Hex characters						

ANNEX 5

Asset Type List for Encrypted AIS

#	Type	STEDS ABBREVIATION
	USCG - CUTTERS	**(max. 5 characters)**
1	Maritime Security Cutter Large	WMSL
2	Maritime Security Cutter Medium	WMSM
3	Patrol Craft	WPC
4	USCG 420' WAGB	WAGB
5	USCG 399' WAGB	WAGB
6	USCG 378' WHEC	WHEC
7	USCG 240' WLBB	WLBB
8	USCG 295' WIX	WIX
9	USCG 282' WMEC	WMEC
10	USCG 270' WMEC	WMEC
11	USCG 225' WLB	WLB
12	USCG 213' WMEC	WMEC
13	USCG 210' WMEC	WMEC
14	USCG 175' WLM	WLM
15	USCG 179' WPC	WPC
16	USCG 160 WLIC	WLIC
17	USCG 100' WLIC	WLIC
18	USCG 75' WLIC	WLIC
19	USCG 140' WTGB	WTGB
20	USCG 110' WPB	WPB
21	USCG 100' WLI	WLI
22	USCG 65' WLI	WLI
23	USCG 75' WLR	WLR
24	USCG 65' WLR	WLR
25	USCG 65' WYTL	WYTL
26	USCG 87' WPB	WPB
27-49	Reserved for future CG cutter types	
	USCG - BOATS	
50	Short Range Prosecutor	SRP
51	Long Range Interceptor	LRI
52	USCG ANB	ANB
53	USCG ATB	ATB
54	USCG ASB	ASB
55	USCG BU	BU
56	USCG BUSL	BUSL
57	USCG CB-L	CB-L
58	USCG CB-M	CB-M
59	USCG CB-S	CB-S
60	USCG MLB	MLB
61	USCG MSB	MSB
62	USCG RB-HS	RB-HS
63	USCG RB-S	RB-S
64	USCG TANB	TANB
65	USCG UTB	UTB
66	USCG UTL	UTL
67	USCG UTM	UTM
68	USCG CB-OTH	CBOTH

69	USCG TPSB	TPSB
70	Special Purpose Craft – Law Enforcement	SPC-LE
71	Special Purpose Craft – Heavy Weather	SPC-HWX
72	Special Purpose Craft – Shallow Water	SPC-SW
73	Special Purpose Craft – Nearshore Lifeboat	SPC-NLB
74-99	Reserved for future CG boat types	
	USCG - AIRCRAFT	
100	Vertical takeoff Unmanned Arial Vehicle	VUAV
101	High Altitude Endurance Unmanned Arial Vehicle	HAE-UAV
102	USCG HC-130H	HC130H
103	USCG HC-130J	HC130J
104	USCG HU-25A	HU25A
105	USCG HU-25B	HU25B
106	USCG HU-25C	HU25C
107	USCG HC-144A	HC144A
108	USCG HH-60	HH60
109	USCG MH-60	MH60
110	USCG HH-65C	HH65C
111	USCG MH-65C	MH65C
112	USCG MH-68A	MH68A
113-129	Reserved for future CG aircraft types	
	USCG - OTHER	
130	Boarding Team	CGBT
131	Patrol from shore	CGSP
132	Mobile Team	CGMT
133-199	Reserved for future CG asset types	
	OTHER GOVERNMENT AGENCIES	
200	Navy: Ship	
201	Navy: Boat	
202	Navy: Submarine	
203	Navy: Helicopter	
204	Navy: Fixed-Wing	
205	Navy: UAV	
206	Military Sealift Command (MSC): Ship	
207	Military Sealift Command (MSC): Boat	
208	DOD – Other: UAV	
209	DOD – Other: Fixed-Wing	
210	DOD – Other: Helicopter	
211	DOD – Other: Boat	
212	Customs & Border Protection (CBP): Boat	
213	Customs & Border Protection (CBP): Helicopter	
214	Customs & Border Protection (CBP): Fixed-Wing	
215	Federal Law Enforcement: Boat	
216	Federal Law Enforcement: Helicopter	
217	Federal Law Enforcement: Fixed-Wing	
218	Federal Agency – Other: Ship	
219	Federal Agency – Other: Boat	
220	Federal Agency – Other: Helicopter	
221	Federal Agency – Other: Fixed Wing	
222	Coast Guard Auxiliary Boat	
223	Coast Guard Auxiliary Fixed-Wing	

224	Air Force Auxiliary Fixed-Wing	
225	State Police: Boat	
226	State Police: Helicopter	
227	State Agency – Other: Boat	
228	State Agency – Other: Helicopter	
229	Local Police: Boat	
230	Local Police: Helicopter	
231	Local Fire/Rescue: Boat	
232	Local Agency – Other: Boat	
233	Local Agency – Other: Helicopter	
234-299	Reserved for future OGA asset types	
300-1023	Reserved for future use	