Encrypted Automatic Identification System (EAIS)
Interface Design Description (IDD) v 5.4
8 May 2017

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: 2017.05.08 15:04:41 -04'00'

M. W. Parsons, GS-13, USCG — Date
Core Technologies Navigation Branch (CT-N1)
System Engineer

Approved by: _____ KEMPE.MATTHEW.VIG.1248444815
c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USCG, cn=KEMPE.MATTHEW.VIG.1248444815
2017.05.08 15:12:11 -04'00'

M. V. Kempe, LCDR — Date
Core Technologies Navigation (CT-N)
Acting Branch Chief

Record of Changes

Change#	Date	Title or Brief Description	Entered By
Original	04 Jun 14	C3CEN EAIS IDD v1.0	LT A.R. Reckley
v2	27 Oct 14	Added IEC 61993-2 to references; clarified para 3.1.6.1; added para 3.3.1.2; added para 3.3.4.1.1; added para 5.3.1; added SOTDMA to msg 26 Comm State in Annex 2 para 2.1; deleted “Text” from para 3.23.1.3	M. W. Parsons
v3	N/A	Version not released	
v4	N/A	Version not released	
v5	25 Jul 16	Added FIDs 9-37 and complied with revision to USCG EAIS VDL Standard.	LCDR M. Kempe
V5.1	7 Mar 17	Removed FID 10, fixed numerous errata with bit widths. Restored ITU1371 conformance for OTAR messages.	LCDR M. Kempe
V5.2	28 Mar 17	Fixed errata for MMSI use on FID 17 & 18. Added message ack/retry rules.	LCDR M. Kempe
V 5.3	20 Apr 17	Added details regarding AES methods. Increased OTAR ASM’s to AIS slot limits. Added KMM preamble, made all multi-slot messages structured. Included revised NMEA 2000 PGN.	LCDR M. Kempe
V 5.4	2 May 17	Added Message 26 variants of SITREP and Static Data ASM, removed Message 25 variants.	LCDR M. Kempe
V 5.4	8 May 17	Corrected table of contents.	LCDR M. Kempe

Table of Contents

1. Scope 1

2. References 2

3. Interface Description 3

Annex 1 – Technical VDL Information 4

Annex 2 – Application Specific Messages 7

Annex 3 – NMEA-0183 Support 97

Annex 4 – NMEA 2000 Support 99

Annex 5 – OTAR Requirements 105

Appendix 1 – Asset Type List 106

Appendix 2 – Search Definitions 109

Appendix 3 – Vessel Target Descriptions 115

Appendix 4 – OTAR Primitive Field Descriptions 117

Appendix 5 – Key Name Codes 118

1. Scope

1.1. Identification

This Interface Design Description (IDD) specifies the interface 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 meets 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). In order to comply with the provisions of recommendation 1371-5 from the International Telecommunications Union, the sending PI generates Application Specific Messages (ASMs), which are passed directly without modification to the receiving PI for decryption and interpretation.

2. References

Name/Number	Version Date	Title
Nav Requirements	Mar 2012	eNav Coast Guard Requirements v1.2
COMD (G-OCC-1) LTR 2000	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,
IEC 61993-2 Ed.2	Oct 2012	Class A shipborne equipment of the AIS - Operational and performance requirements
NMEA 0183	Jun 2012	Standard for Interfacing Marine Electronic Devices (Ver.4.10)
NMEA 2000	Jan 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	Mar 2012	Interim solutions for improved efficiency in the use of the band 156-174 MHz by stations in the maritime mobile service
TIA-102.AACA-A	Sep 2014	Project25 Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures
FIPS 140-2	May 2001	Security Requirements For Cryptographic Modules

3. Interface Description

Annex 1 contains a technical description of the eAIS VDL when the AIS messages 25 & 26 are used to transport the Sensitive But Unclassified (SBU) Tactical Information Exchange and Display System (STEDS) Application Specific Messages (ASM). Annex 1 is based on International Telecommunication Union (ITU) standard ITU-R M.1371-5.

Annex 2 contains the listing of the ASMs used with this IDD.

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 contains OTAR requirements for the PI.

Appendix 1 contains a listing of the asset types used with this IDD.
Appendix 2 contains an explanation of Search Pattern Definitions, along with nomenclature and designations.
Appendix 3 contains a listing of vessel, aircraft and submarine Target Descriptions for use with Target of Interest ASMs.
Appendix 4 contains an explanation of the OTAR Primitive Field Descriptions
Appendix 5 contains a listing of Key Name Codes used with OTAR Key names.

ANNEX 1

EAIS Transponder Modes of Operation

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.

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 operates exclusively on normal AIS frequencies and does not respond to base station or digital selective calling commands to change frequencies. The transponder receives AIS messages and EAIS messages, but transmits nothing (maintaining radio silence).

Restricted

When in this mode of operation the AIS transponder only transmits EAIS messages, while no non-EAIS messages are sent. The transponder shall operate exclusively on normal AIS frequencies and shall not respond to base station or digital selective calling commands to change frequencies. The transponder continues to receive AIS messages and EAIS messages.

CRC Checksum Computation

When computing the 16-bit CRC checksum for the encrypted ASMs, this VDL utilizes the “reflected table driven” implementation, as described in RFC 1662 (Std 51), found at http://www.armware.dk/RFC/rfc/rfc1662.html. RFC 1662 describes the standards for High-level Data Control Link (HDCL). Appendix C.2 of that document lists the code to implement the “reflected table driven” algorithm.

The RFC 1662 code implements the 16-bit CRC as specified below.

- Width: 16 bits
- Polynomial: 1021
- Initial CRC value (seed): FFFF
- Input bytes (8 bits) are processed with bit 0 being treated as the most significant bit (MOB) and bit 7 being treated as the least significant bit
- Final CRC is XORed with: FFFF
- Output CRC (16 bits) is reflected.
- The lower eight bits of the CRC are swapped with the higher eight bits of the CRC

FID 9: CRC is applied to payload prior to encryption using all bits from the Function Identifier field up to, but not including the CRC field. This will be a multiple of 128-bits minus 16 bits.

FID 13, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38 and 39: CRC is applied using all the bits from the DAC field up to but not including the CRC field after the payload has been encrypted.

AES Encryption

All encryption modules used to encrypt and decrypt STEDS ASM's must be FIPS 140-2 certified.

STEDS Payload FID 9, 11, 12, 13, 15, 17, 18, 36, 37, 38 and 39 are encrypted using the AES Electronic Code Book (ECB) mode with a key length of 128 bits for compactness:

> FID 9: All bits from the [Function Identifier] field through the CRC inclusive are encrypted. This will be multiples of 128-bits.
>
> FID 13, 15, 17, 18, 36, 37, 38, 39: All bits from the [Version] field through the [Encryption Bit Padding] field, inclusive are encrypted; this will be multiples of 128-bits.

OTAR Payload FID 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, and 35 are encrypted using the AES Output Feed Back (OFB) mode with a key length of 128 bits to comply with less compact, but more stringent TIA Project 25 OTAR requirements.

> FID 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, and 35: All bits from the [OTAR Message ID] field through the [Encryption Bit Padding] field inclusive are encrypted. This will be multiples of 128-bits.
> The KMM preamble governs the preparation for the OFB decryption operation.

Per TIA Project 25 OTAR requirements, the key wrap algorithm separately encrypts keys using the AES-ECB mode, prior to encryption for transport.

For clarity – In addition to the above, the AES Cipher Block Chaining (CBC) mode is used to add an additional level of protection against "reflection" attacks by separately encrypting the Message Authentication Code (MAC) data field of OTAR messages FID 19, 20, 21, 22, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, and 35 prior to encryption of the entire payload. This OTAR Message authentication code, is of key length/2, and is calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.

ANNEX 2

Legend:
In the message format tables in this chapter, red shading indicates the encrypted portions of the ASM, olive indicates message data governed by the Project25 OTAR guidance, and lavender shading indicates optional message data for various OTAR fields.

2.1 Message Acknowledgement

DAC**: 366** FI**:** **9** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:
Version 0:
This is an RTCM compliant update of the FID 2 message listed in the Oct 2014 EAIS IDD.

2.1.1 Introduction

This Message 25 payload is used to acknowledge reception of addressed, encrypted STEDS messages.

2.1.2 Usage Notes

- Acknowledgement linkage back to the original message is based upon source MMSI, source FI, and source Message Linkage ID.
- If the received FID 17 (Encrypted Text Message), has its “ACK flag” field set to zero, then this acknowledgement shall not be sent. Otherwise, all encrypted, addressed STEDS messages receive an ACK.
- If the sending PI does not receive an ACK after 4 seconds, the sending PI shall retry transmission. The sending PI shall retry a maximum of three times, waiting 4 seconds each time for an ACK. This indicates a maximum of four transmitted messages: one initial and three retries.

2.1.3 Message 25, FID 9 (Encrypted) Format

Encrypted Message Acknowledgement (Message 25, Broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 25; always 25.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 0 (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to zero (unstructured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.
Binary Application Data (encrypted)	Function Identifier	6	Function identifier. Set to 9.
	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
	Original Message Source	30	MMSI of the source of the message being acknowledged.
	Original Message DAC	10	DAC of the message to be acknowledged. Set to 0 if no DAC (AIS message 25/26 messages).
	Original Message FI	6	Functional Identifier of message being acknowledged. 0 – 63.
	Original Message MLID	10	MLID of the source message to be acknowledged.
	Original Message Checksum	16	16-bit CRC of the source message to be acknowledged.
	UTC Hour	5	UTC Hour of ACK. 0 – 23; 24 = UTC hour not available = default; 25 - 31 = reserved.
	UTC Min	6	UTC Minute of ACK. 0 – 59; 60 = UTC minute not available = default; 61 - 63 (reserved for future use).
	UTC Sec	6	UTC Second of ACK. 0 – 59; 60 = UTC second not available = default; 61-63 (reserved for future use).
	Encryption Bit Padding	14	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (128). Set to 0.
	Checksum	16	16-bit CRC calculated as per EAIS Specification
	Total bits	168	1 Slot Binary Message

2.2 Search Pattern Report

DAC**: 366** FI**:** **13** (Encrypted)
14 (Unencrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant update of the FID 2 message listed in the Oct 2014 EAIS IDD. The FID was changed to avoid confusion with ASMs used by the Saint Lawrence Seaway Corp.

The encrypted Message 8 isn't implemented.

2.2.1 Introduction

The Search Pattern Report (SPR) communicates a search pattern from the SAR Mission Coordinator (SMC) to a Search UNIT (SRU) (either to transmit a pattern for action or to cancel a pattern) or from a SRU to the SMC (reporting acceptance or completion). Search plan nomenclature is included for reference in Appendix 2 of this IDD.

2.2.2 Usage Notes

- The Search execution status is controlled by the Search Pattern Status field. A State Diagram is shown in Figure 1 with the execution flow as follows:
  - The pattern is initially sent from the MC to the action SRU with the Status set as 0 (direction to execute a plan).
  - The SRU should respond with either:
    - Status set as 0 to indicate that the pattern was received and will be started (identical pattern parameters).
      - Status set to 7 to say the pattern cannot be executed.
  - If the SRU sends a status of 7 the MC needs to send a new pattern (followed up with communications between the MC and SRU to discuss WHY the pattern cannot be executed).
  - Once the search plan is started the SRU shall send a message with status 1 with the time and position fields updated to reflect the actual commence search time and position.
  - Once the pattern is complete the SRU should send the Search pattern report with a status of 2 and with the time and position fields updated to reflect time and position of completion.
  - If the SRU needs to abort the plan prior to completion a message with status=3 should be sent with the time and position fields updated to reflect time and position when aborted plan.
  - If the SMC wants to cancel a SAR pattern prior to completion then the message is sent with status = 3.

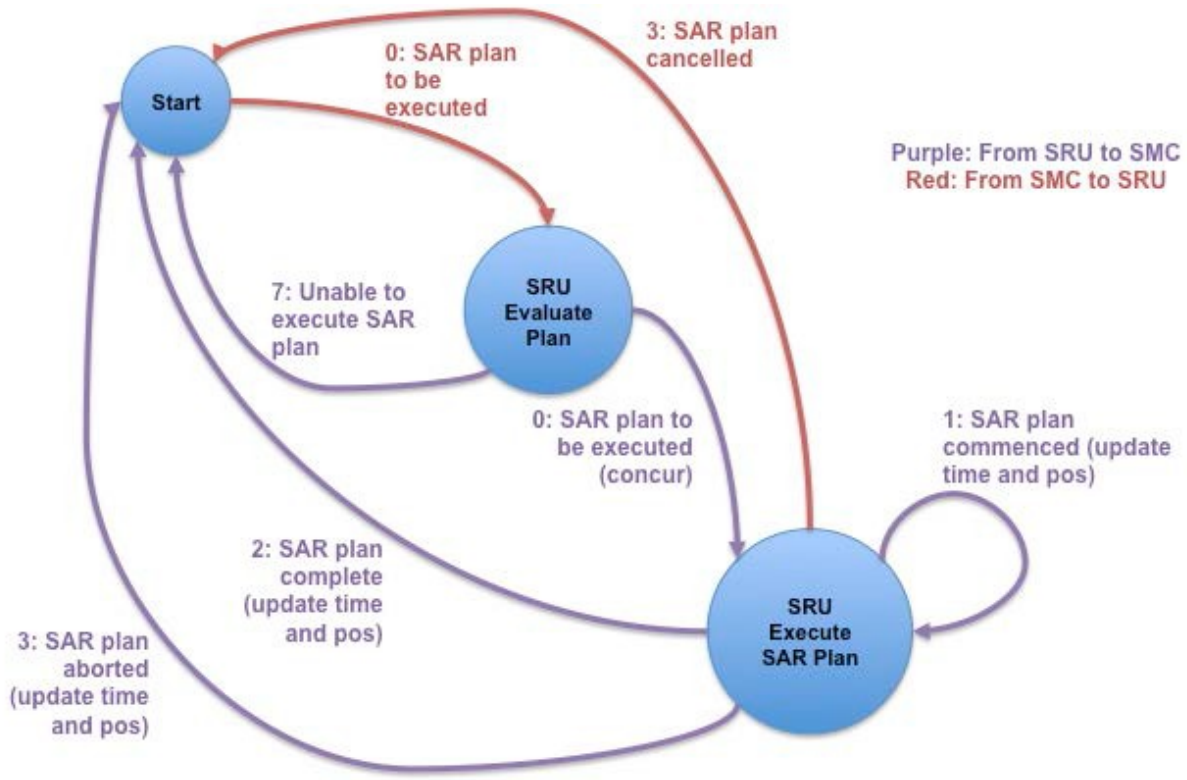

Figure 1: SAR Plan Message State Diagram

- The Message Linkage ID can be used to link additional text (e.g., a separate Linked Text message). However, the same source MMSI needs to be included in both the SPR and the Linked Text Message (LTM). This could be used to communicate a SAR pattern designation or additional notes about the pattern or search object.
- A message version number is encoded as part of the message; if the received version number is different than what the display system has been programmed for, then the charting system should alert the user to the difference.
- All headings are in degrees true.
- All positions are in WGS 84 Datum.
- If less than 5 characters, the remainder of the Case ID parameter should be filled with "@" characters (set bits to 0); but, not shown on the presentation.
- For the expanding square search the track spacing should equal the first leg length; to ensure this is true the value should be specified in the first leg length field and track spacing field set to 0.
- For the Message 26 version, the 20 bits Communications State are added by the transmitter if transmission is initiated by a BBM sentence.

2.2.2.1 Expanding Square Search (SS) Parameters

An expanding square search pattern uses the following parameters:

- CSP
- Initial heading
- Track spacing
- Direction of turns (L/R)

All turns are 90°, typically to starboard. Each even turn, increase the distance of the leg by 1 track space. See Figure 1 within Appendix 2 of this VDL. For this pattern track spacing and initial leg length are the same and both fields should be set to the same value.

2.2.2.2 Sector Search (VS) Parameters

A sector search pattern uses the following parameters:

- CSP
- Initial heading
- Leg length
- Number of legs (defined as the equal-length segments)

All turns are 120° to starboard, and all legs are of equal length. The legs are the equal length segments (from CSP to radius of the circle). It takes 9 equal length legs to complete one VS pattern (less than 9 legs can be specified if the full pattern is not desired). After completing 9 equal length legs (back to the CSP) the pattern can be repeated with a new initial heading 30° to starboard of the initial. So if the number of legs specified is greater than 9, after 9 legs, rotate the pattern 30° to the right and continue. After 18 legs, rotate the pattern another 30° to the right. See Figure 2 within Appendix 2 of this VDL.

2.2.2.3 Parallel Search (PS) Parameters

A parallel search pattern uses the following parameters:

- CSP
- Initial direction
- Leg length
- Track spacing
- First turn (L/R)

All turns are 90° – 2 turns in same direction then switch direction. Cross leg lengths are equal to track spacing. Go leg length, turn go track space, turn same direction go leg length, turn opposite direction go track space, turn same, etc. See Figure 3 within Appendix 2 of this VDL.

2.2.2.4 Creeping Line Search (CS) Parameters

The creeping line search is the same as the parallel search except that the search legs are oriented along the minor axis of the search area vice the major axis.

2.2.3 Message 26, FID 13 (Encrypted) Format

SAR Pattern Report (Message 26, Broadcast, Encrypted)

	Parameter		# of Bits	Description
Standard Message Header	Message ID		6	Identifier for Message 26; always 26.
	Repeat Indicator		2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI		30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator		1	0 = Broadcast (no Destination ID field used) 1 = Addressed (Destination ID uses 30 data bits for MMSI) Set to 0, broadcast.
	Binary Data Flag		1	0 = unstructured binary data (no Application Identifier bits used); 1 = binary data coded as defined by using the16-bit Application identifier. Set to 1, structured.
Binary Data	Designated Area Code		10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
	Function Identifier		6	Function identifier. Set to 13.
	Encrypted Payload	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID	10	Identifier for the SAR Pattern Report. This number uniquely identifies a search pattern sent from a given SMC (MMSI) and is used to connect additional information with the search. Source MMSI and this ID uniquely identify the event. Set to 1 - 1023 by message originator; 0 = not available.
		Pattern Type	3	Type of search pattern: 0 = Expanding Square (SS) = default; 1 = Sector (VS); 2 = Parallel Line (PS); 3 = Creeping Line (CS); 4 – 7 = reserved.
		Search Pattern Status	3	

Code	From MC	From Action SRU
0	Search plan to be executed	Search plan to be executed (concur w/ mission plan, and will take FORAC)
1	Reserved	Search plan started (time and search position updated to actual CST and CSP)
2	Reserved	Search plan completed. (time and point updated to reflect completion time and last position)
3	Search plan cancelled by SMC	Search plan aborted (time and point updated to reflect aborted time and position)
4	Directions to divert from search plan at this position, execute new search plan.	Indicates unit has diverted from search plan at this position
5	Direction to resume search plan at this position	Indicates the unit has resumed search plan at this position
6	Reserved	Reserved for future use
7	Reserved	Unable to execute search plan

Binary Data	Encrypted Payload	Reference Time	UTC Day	5	UTC Day 1 – 31; 0 = UTC day not available = default.
			UTC Hour	5	UTC Hour. 0 – 23; 24 = UTC hour not available = default; 25 - 31 = reserved.
			UTC Min	6	UTC Minute. 0 – 59; 60 = UTC minute not available = default; 61 - 63 (reserved for future use)
		Action SRU MMSI		30	MMSI of the Action SRU. This varies according to the MMSI of the desired unit. 0 = unknown = default;
		Case ID Number		30	Case ID. Maximum 5 characters 6-bit ASCII as defined in ITU 1371-5, Table 47. "@@@@@" = not available = default. If less than 5 characters, the remainder of the parameter should be filled with "@" characters (set bits to 0); but, not shown on the presentation.
		Search Point	Longitude	25	Longitude in 1/1000 minute. (±180°) East = positive (as per 2's complement); West = negative (as per 2's complement); 181° = not available = default.
			Latitude	24	Latitude in 1/1000 minute (±90°) North = positive (as per 2's complement); South = negative (as per 2's complement); 91° = not available = default.
		Initial Heading		9	Direction of the first leg. 0 – 359 degrees; 360 = not specified = default; 361 – 510 = reserved; 511 = not to be used.
		First Leg Length		12	Length of the first leg (lengths of succeeding legs depend upon the type of pattern) in 0.1 NM increments. 0 = not specified = default; 0.1 – 400.0 NM; 4001-4094 = reserved; 4095 = not to be used.
		No. of Legs		10	Total number of legs (search and cross) to execute. 0 = not specified = default; 1 – 1000 legs; 1001-1022 = reserved; 1023 = not to be used.
		Track Spacing		9	Track spacing in 0.1 NM increments. 0 = not specified = default; 0.1 – 50.0 NM; 501 – 510 = reserved; 511 – not to be used.
		First Turn Direction		1	Direction of first turn. 0 = port; 1 = starboard = default.
		Search Altitude		7	Altitude for search pattern in 50 ft increments. 0 = sea level; 50 – 6000 ft; 121 = not specified = default; 122 – 127 = reserved.
		Search Speed		9	Speed to execute the search pattern in 1kt increments. 0 = not specified = default; 1 – 500 kts; 501 – 510 = reserved; 511 – not to be used.
		Search Area Width		11	Total width of search area in tenths of NM 0 = unknown = default; 0.1 – 200.0 NM; 2001-2047 reserved.
		Search Area Length		11	Total length of search area in tenths of NM 0 = unknown = default; 0.1 – 200.0 NM; 2001-2047 reserved.
		Encryption Bit Padding		33	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256). Set to 0.
	Checksum			16	16-bit CRC calculated as per EAIS Specification

Footer	Spare	4	Four extra bits added to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	352	2 Slot Binary Message

2.2.4 Message 8, FID 14 (Unencrypted) Format

Unencrypted SAR Pattern Report (Message 8, Broadcast)

Parameter				# of Bits	Description
Standard Message Header	Message ID			6	Identifier for Message 8; always 8.
	Repeat Indicator			2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI			30	MMSI number of source station. Varies according to the transmitter ID.
	Spare			2	Not used. Set to zero.
Binary Data	Designated Area Code			10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
	Function Identifier			6	Function identifier. Set to 14.
	Application Data (unencrypted)	Version		3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID		10	Identifier for the SAR Pattern Report. This number uniquely identifies a search pattern sent from a given SMC (MMSI) and is used to connect additional information with the search. Source MMSI and this ID uniquely identify the event. Set to 1 - 1023 by message originator; 0 = not available.
		Pattern Type		3	Type of search pattern: 0 = Expanding Square (SS) = default; 1 = Sector (VS); 2 = Parallel Line (PS); 3 = Creeping Line (CS); 4 – 7 = reserved.
		Search Pattern Status		3	See table below
		Reference Time	UTC Day	5	UTC Day 1 – 31; 0 = UTC day not available = default.
			UTC Hour	5	UTC Hour. 0 – 23; 24 = UTC hour not available = default; 25 - 31 = reserved.
			UTC Min	6	UTC Minute. 0 – 59; 60 = UTC minute not available = default; 61 - 63 (reserved for future use).

Code	From MC	From Action SRU
0	Search plan to be executed	Search plan to be executed (concur w/ mission plan, and will take FORAC)
1	Reserved	Search plan started (time and search position updated to actual CST and CSP)
2	Reserved	Search plan completed. (time and point updated to reflect completion time and last position)
3	Search plan cancelled by SMC	Search plan aborted (time and point updated to reflect aborted time and position)
4	Directions to divert from search plan at this position, execute new search plan.	Indicates unit has diverted from search plan at this position
5	Direction to resume search plan at this position	Indicates the unit has resumed search plan at this position
6	Reserved	Reserved for future use
7	Reserved	Unable to execute search plan

	Binary Data	Application Data (unencrypted)	Action SRU MMSI		30	MMSI of the Action SRU. This varies according to the MMSI of the desired unit. 0 = unknown = default;
			Case ID Number		30	Case ID. Maximum 5 characters 6-bit ASCII as defined in ITU 1371-5, Table 47. "@@@@@" = not available = default. If less than 5 characters, the remainder of the parameter should be filled with "@" characters (set bits to 0); but, not shown on the presentation.
			Search Point	Longitude	25	Longitude in 1/1000 minute. (±180°) East = positive (as per 2's complement); West = negative (as per 2's complement); 181° = not available = default.
				Latitude	24	Latitude in 1/1000 minute (±90°) North = positive (as per 2's complement); South = negative (as per 2's complement); 91° = not available = default.
			Initial Heading		9	Direction of the first leg. 0 – 359 degrees; 360 = not specified = default; 361 – 510 = reserved; 511 = not to be used.
			First Leg Length		12	Length of the first leg (lengths of succeeding legs depend upon the type of pattern) in 0.1 NM increments. 0 = not specified = default; 0.1 – 400.0 NM; 4001-4094 = reserved; 4095 = not to be used.
			No. of Legs		10	Total number of legs (search and cross) to execute. 0 = not specified = default; 1 – 1000 legs; 1001-1022 = reserved; 1023 = not to be used.
			Track Spacing		9	Track spacing in 0.1 NM increments. 0 = not specified = default; 0.1 – 50.0 NM; 501 – 510 = reserved; 511 – not to be used.
			First Turn Direction		1	Direction of first turn. 0 = port; 1 = starboard = default.
			Search Altitude		7	Altitude for search pattern in 50 ft increments. 0 = sea level; 50 – 6000 ft; 121 = not specified = default; 122 – 127 = reserved.
			Search Speed		9	Speed to execute the search pattern in 1kt increments. 0 = not specified = default; 1 – 500 kts; 501 – 510 = reserved; 511 – not to be used.
			Search Area Width		11	Total width of search area in tenths of NM 0 = unknown = default; 0.1 – 200.0 NM; 2001-2047 reserved.
			Search Area Length		11	Total length of search area in tenths of NM 0 = unknown = default; 0.1 – 200.0 NM; 2001-2047 reserved.
			Spare		1	Set to zero.
				Total bits	280	2 Slot Binary Message

2.3 Trackline Report

DAC**: 366** FI**:** **15 (**Encrypted)
16 (Unencrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant update of the FID 3 message listed in the Oct 2014 EAIS IDD. The FID was changed to avoid confusion with previously published message definitions.

There are AIS Message 25 and 8 variants of this message, but the encrypted message 8 is not implemented.

2.3.1 Introduction

The Trackline Report (SPR) communicates a search pattern from the mission controller to a SRU (either to transmit a pattern for action or to cancel a pattern) or from a SRU to the MC (reporting acceptance or completion).

2.3.2 Usage Notes

- The SAR execution status is controlled by the SAR Pattern Status field. A State Diagram is shown in Figure 1 with the execution flow as follows:
  - The pattern is initially sent from the SMC to the action SRU with the Status set as 0 (direction to execute a plan).
  - The SRU should respond with either:
    - Status set as 0 to indicate that the pattern was received and will be started (identical pattern parameters).
    - Status set to 7 to say the pattern cannot be executed.
  - If the SRU sends a status of 7 the SMC needs to send a new pattern (followed up with communications between the MC and SRU to discuss WHY the pattern cannot be executed).
  - Once the search plan is started the SRU shall send a message with status 1 with the time and position fields updated to reflect the actual commence search time and position.
  - Once the pattern is complete the SRU should send the SAR pattern report with a status of 2 and with the time and position fields updated to reflect time and position of completion.
  - If the SRU needs to abort the plan prior to completion a message with status=3 should be sent with the time and position fields updated to reflect time and position when aborted plan.
  - If the SMC wants to cancel a SAR pattern prior to completion then the message is sent with status of 3.
- The Message Linkage ID can be used to link additional text (e.g., a separate Linked Text message). However, the same source MMSI needs to be included in both the SPR and the Linked Text Message (LTM). This could be used to communicate a SAR pattern designation or additional notes about the pattern or search object.
- A message version number is encoded as part of the message; if the received version number is different than what the display system has been programmed for, then the charting system should alert the user to the difference.
- Positions are in WGS 84 Datum.

- If less than 10 characters, the remainder of the SRU designation parameter should be filled with "@" characters (set bits to 0); but, not shown on the presentation.
- To allow the SRU to transmit the message it should be kept to a maximum of 3 slots, which equates to a maximum of 7 additional waypoints for unencrypted and 6 for the encrypted version.
- A trackline search pattern is specified by the waypoints (Lat/Long).
- If pattern type is polygon then the track connects back to the CSP.
- The Trackline Report is sent as several short message segments that need to be assembled by the recipient. The segments are identified by segment number and list the total number of segments (1 of 3, 2 of 3 etc.).
- The first Trackline Report segment contains the information about the type of pattern and search parameters. All succeeding segments just contain waypoint information.

2.3.3 Message 26, FID 15 (Encrypted) Format

Encrypted Trackline Report Segment 1 (Message 26, Broadcast)

Parameter			# of Bits	Description
Standard Message Header	Message ID		6	Identifier for Message 26; always 26.
	Repeat Indicator		2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI		30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator		1	0 = Broadcast (no Destination ID field used) 1 = Addressed (Destination ID uses 30 data bits for MMSI) Set to 0, broadcast.
	Binary Data Flag		1	0 = unstructured binary data (no Application Identifier bits used); 1 = binary data coded as defined by using the16-bit Application identifier. Set to 1, structured.
Binary Data	Designated Area Code		10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
	Function Identifier		6	Function identifier. Set to 15.
	Encrypted Payload	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID	10	Identifier for the SAR Pattern Report. This number uniquely identifies a search pattern sent from a given SMC (MMSI) and is used to connect additional information with the search. Source MMSI and this ID uniquely identify the event. Set to 1 - 1023 by message originator; 0 = not available.
		Message Segment	5	Number of this message segment; sequential number. Recipient will need to receive all segments and put in order sequentially. 0 – 31. Set to 0.
		Number of Segments	5	Total number of segments comprising the complete Trackline Report (Total = N+1). N = 0- 31.
		Pattern Type	2	Type of search pattern: 0 = Trackline Search Pattern or route = default; 1 = Polygon; 2-3 = reserved.

<table>
<tr><td rowspan="15"></td><td rowspan="15"></td><td rowspan="15">Encrypted Payload</td><td colspan="2">Search Pattern Status</td><td>3</td><td>
<table>
<tr><th>Code</th><th>From MC</th><th>From Action SRU</th></tr>
<tr><td>0</td><td>Search plan to be executed</td><td>Search plan to be executed (concur w/ mission plan, and will take FORAC)</td></tr>
<tr><td>1</td><td>Reserved</td><td>Search plan started (time and search position updated to actual CST and CSP)</td></tr>
<tr><td>2</td><td>Reserved</td><td>Search plan completed. (time and point updated to reflect completion time and last position)</td></tr>
<tr><td>3</td><td>Search plan cancelled by SMC</td><td>Search plan aborted (time and point updated to reflect aborted time and position)</td></tr>
<tr><td>4</td><td>Directions to divert from search plan at this position, execute new search plan.</td><td>Indicates unit has diverted from search plan at this position</td></tr>
<tr><td>5</td><td>Direction to resume search plan at this position</td><td>Indicates the unit has resumed search plan at this position</td></tr>
<tr><td>6</td><td>Reserved</td><td>Reserved for future use</td></tr>
<tr><td>7</td><td>Reserved</td><td>Unable to execute search plan</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">Reference Time</td><td>UTC Day</td><td>5</td><td>UTC Day
1 – 31; 0 = UTC day not available = default.</td></tr>
<tr><td>UTC Hour</td><td>5</td><td>UTC Hour.
0 – 23; 24 = UTC hour not available = default; 25 - 31 = reserved.</td></tr>
<tr><td>UTC Min</td><td>6</td><td>UTC Minute.
0 – 59; 60 = UTC minute not available = default; 61 - 63 (reserved for future use).</td></tr>
<tr><td colspan="2">Action SRU MMSI</td><td>30</td><td>MMSI of the Action SRU. This varies according to the MMSI of the desired unit. 0 = unknown = default;</td></tr>
<tr><td colspan="2">Case ID Number</td><td>30</td><td>Case ID. Maximum 5 characters 6-bit ASCII as defined in ITU 1371-5, Table 47.
“@@@@@” = not available = default.
If less than 5 characters, the remainder of the parameter should be filled with “@” characters (set bits to 0); but, not shown on the presentation.</td></tr>
<tr><td rowspan="2">Search Point</td><td>Longitude</td><td>28</td><td>Longitude in 1/10,000 minute. (±180°)
East = positive (as per 2’s complement); West = negative (as per 2’s complement); 181° = not available = default.</td></tr>
<tr><td>Latitude</td><td>27</td><td>Latitude in 1/10,000 minute (±90°)
North = positive (as per 2’s complement); South = negative (as per 2’s complement); 91° = not available = default.</td></tr>
<tr><td colspan="2">Search Altitude</td><td>7</td><td>Altitude for search pattern in 50 ft increments.
0 = sea level; 50 – 6000 ft; 121 = not specified = default; 122 – 127 = reserved.</td></tr>
<tr><td colspan="2">Search Speed</td><td>9</td><td>Speed to execute the search pattern in 1kt increments.
0 = not specified = default; 1 – 500 kts;
501 – 510 = reserved; 511 – not to be used.</td></tr>
<tr><td colspan="2">Encryption Bit Padding</td><td>81</td><td>Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256). Set to 0.</td></tr>
<tr><td colspan="3">Checksum</td><td>16</td><td>16-bit CRC calculated as per EAIS Specification</td></tr>
</table>

Footer	Spare	4	Four extra bits added to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows, 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	352	2 Slot Binary Message

Encrypted Trackline Report Segment 2-32 (Message 26, Broadcast)

Parameter			# of Bits	Description
Standard Message Header	Message ID		6	Identifier for Message 26; always 26.
	Repeat Indicator		2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI		30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator		1	0 = Broadcast (no Destination ID field used), 1 = Addressed (Destination ID uses 30 data bits for MMSI) Set to 0, broadcast.
	Binary Data Flag		1	0 = unstructured binary data (no Application Identifier bits used); 1 = binary data coded as defined by using the16-bit Application identifier. Set to 1, structured.
Binary Data	Designated Area Code		10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
	Function Identifier		6	Function identifier. Set to 15.
	Encrypted Payload	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID	10	Identifier for the SAR Pattern Report. This number uniquely identifies a search pattern sent from a given SMC (MMSI) and is used to connect additional information with the search. Source MMSI and this ID uniquely identify the event. Set to 1 - 1023 by message originator; 0 = not available.
		Message Segment	5	Number of this message segment; sequential number. Recipient will need to receive all segments and put in order sequentially. 1 – 31.
		Number of Segments	5	Total number of segments comprising the complete Trackline Report (Total = N+1). N = 0- 31.
		Search Point – Longitude	28	Longitude in 1/10,000 minute. (±180°) East = positive (as per 2's complement); West = negative (as per 2's complement); 181° = not available = default.
		Search Point – Latitude	27	Latitude in 1/10,000 minute (±90°) North = positive (as per 2's complement); South = negative (as per 2's complement); 91° = not available = default.
		Search Altitude	7	Altitude for search pattern in 50 ft increments. 0 = sea level; 50 – 6000 ft; 121 = not specified = default; 122 – 127 = reserved.
		Search Speed	9	Speed to execute the search pattern in 1kt increments. 0 = not specified = default; 1 – 500 kts; 501 – 510 = reserved; 511 – not to be used.
		Encryption Bit Padding	34	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (128). Set to 0.
	Checksum		16	16-bit CRC calculated as per EAIS Specification

Footer	Spare	4	Four extra bits added to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	224	2 Slot Binary Message

2.3.4 Message 8, FID 16 (Unencrypted) Format

Unencrypted Trackline Report Segment 1 (Message 8, Broadcast)

Parameter			# of Bits	Description
Standard Message Header	Message ID		6	Identifier for Message 8; always 8.
	Repeat Indicator		2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI		30	MMSI number of source station. Varies according to the transmitter ID.
	Spare		2	Not used. Set to zero.
Binary Data	Designated Area Code		10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
	Function Identifier		6	Function identifier. Set to 16.
	Application Data (unencrypted)	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID	10	Identifier for the SAR Pattern Report. This number uniquely identifies a search pattern sent from a given SMC (MMSI) and is used to connect additional information with the search. Source MMSI and this ID uniquely identify the event. Set to 1 - 1023 by message originator; 0 = not available.
		Message Segment	5	Number of this message segment; sequential number. Recipient will need to receive all segments and put in order sequentially. 0 – 31. Set to 0.
		Number of Segments	5	Total number of segments comprising the complete Trackline Report (Total = N+1). N = 0- 31.
		Pattern Type	2	Type of search pattern: 0 = Trackline Search Pattern or route = default; 1 = Polygon; 2-3 = reserved.
		Search Pattern Status	3	

Code	From MC	From Action SRU
0	Search plan to be executed	Search plan to be executed (concur w/ mission plan, and will take FORAC)
1	Reserved	Search plan started (time and search position updated to actual CST and CSP)
2	Reserved	Search plan completed. (time and point updated to reflect completion time and last position)
3	Search plan cancelled by SMC	Search plan aborted (time and point updated to reflect aborted time and position)
4	Directions to divert from search plan at this position, execute new search plan.	Indicates unit has diverted from search plan at this position
5	Direction to resume search plan at this position	Indicates the unit has resumed search plan at this position
6	Reserved	Reserved for future use
7	Reserved	Unable to execute search plan

Binary Data	Application Data (unencrypted)	Reference Time	UTC Day	5	UTC Day 1 – 31; 0 = UTC day not available = default.
			UTC Hour	5	UTC Hour. 0 – 23; 24 = UTC hour not available = default; 25 - 31 = reserved.
			UTC Min	6	UTC Minute. 0 – 59; 60 = UTC minute not available = default; 61 - 63 (reserved for future use).
		Action SRU MMSI		30	MMSI of the Action SRU. This varies according to the MMSI of the desired unit. 0 = unknown = default;
		Case ID Number		30	Case ID. Maximum 5 characters 6-bit ASCII as defined in ITU 1371-5, Table 47. "@@@@@" = not available = default. If less than 5 characters, the remainder of the parameter should be filled with "@" characters (set bits to 0); but, not shown on the presentation.
		Search Point	Longitude	28	Longitude in 1/10,000 minute. (±180°) East = positive (as per 2's complement); West = negative (as per 2's complement); 181° = not available = default.
			Latitude	27	Latitude in 1/10,000 minute (±90°) North = positive (as per 2's complement); South = negative (as per 2's complement); 91° = not available = default.
		Search Altitude		7	Altitude for search pattern in 50 ft increments. 0 = sea level; 50 – 6000 ft; 121 = not specified = default; 122 – 127 = reserved.
		Search Speed		9	Speed to execute the search pattern in 1kt increments. 0 = not specified = default; 1 – 500 kts; 501 – 510 = reserved; 511 – not to be used.
		Spare		1	Set to zero.
			Total bits	232	2 Slot Binary Message

Unencrypted SAR Trackline Report Segment 2-32 (Message 8, Broadcast)

Parameter				# of Bits	Description
Standard Message Header	Message ID			6	Identifier for Message 8; always 8.
	Repeat Indicator			2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI			30	MMSI number of source station. Varies according to the transmitter ID.
	Spare			2	Not used. Set to zero.
Binary Data	Designated Area Code			10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
	Function Identifier			6	Function identifier. Set to 16.
	Application Data (unencrypted)	Version		3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID		10	Identifier for the SAR Pattern Report. This number uniquely identifies a search pattern sent from a given SMC (MMSI) and is used to connect additional information with the search. Source MMSI and this ID uniquely identify the event. Set to 0-1023 by message originator; 0 = not available.
		Message Segment		5	Number of this message segment; sequential number. Recipient will need to receive all segments and put in order sequentially. 1 – 31.

Binary Data	Application Data (unencrypted)	Number of Segments		5	Total number of segments comprising the complete Trackline Report (Total = N+1). N = 0- 31.
		Search Point	Longitude	28	Longitude in 1/10,000 minute. (±180°) East = positive (as per 2's complement); West = negative (as per 2's complement); 181° = not available = default.
			Latitude	27	Latitude in 1/10,000 minute (±90°) North = positive (as per 2's complement); South = negative (as per 2's complement); 91° = not available = default.
		Search Altitude		7	Altitude for search pattern in 50 ft increments. 0 = sea level; 50 – 6000 ft; 121 = not specified = default; 122 – 127 = reserved.
		Search Speed		9	Speed to execute the search pattern in 1kt increments. 0 = not specified = default; 1 – 500 kts; 501 – 510 = reserved; 511 – not to be used.
		Spare		2	Set to zero.
		Total bits		152	1 Slot Binary Message

2.4 Text Message

DAC**: 366** FI**:** **17** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant update of the FID 0 message listed in the Oct 2014 EAIS IDD. It also replaces the DAC 366 FID 55 message from the same document.

There are AIS Message 6, 8 and 26 variants of this message, but only message 26 is implemented.

2.4.4 Introduction

This Message is used to send encrypted text messages.

2.4.5 Usage Notes

- The Message 26 Text Message format provides for both a broadcast and addressed text message. Message addressing, when required, shall be performed using the Destination Indicator and Destination ID fields inherent to the Message 26 structure.
- The text may be up to 142 6-bit ASCII characters (up to 852 bits).
- The addressed version of this message shall have the “ACK Flag” value set by the user. If an ACK is desired, see the Usage Notes of FID 9 for retry procedures.

2.4.6 Message 26 Addressed Format

Encrypted Text Message (Message 26, Addressed)

Parameter		# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 1 (addressed).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	30	MMSI number of destination station.
	Spare	2	Not used, Set to zero.

Binary Data	Designated Area Code		10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
	Function Identifier		6	Function identifier. Set to 17.
	Binary Encrypted Payload	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID	10	A source-specific random number, unique across recent binary messages equipped with Message Linkage ID. Used to connect the additional information in this Text Message with another ASM. The Message Linkage ID and the source MMSI uniquely identify the sent message. 1 – 1,023; 0 = not available.
		ACK Flag	1	Acknowledgement Flag; used to indicate acknowledgement status 0 = no acknowledgement requests = default; 1 = acknowledgement requested.
		Text length	8	Length of text message in characters. 0 – 142 characters; 143 = unknown = default; 144 – 255 = reserved.
		Text Message	0 – 852	User Text Message, 6-bit ASCII characters as per ITU 1371. 0 – 142 characters = 0 – 852 bits.
		Encryption Bit Padding	Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (128, 256, 384, 512, 640, 768, or 896). Set to 0.
	Checksum		16	16-bit CRC calculated as per EAIS Specification
Footer	Spare		4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector		1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State		19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits		256 – 1024	2 - 5 Slot Binary Message

2.4.7 Message 26 Broadcast Format

Encrypted Text Message (Message 26, Broadcast)

Parameter		# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 0 (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.

		Spare	0	Not used.
Binary Data		Designated Area Code	10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
		Function Identifier	6	Function identifier. Set to 17.
	Application Data (encrypted)	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID	10	A source-specific random number, unique across recent binary messages with Message Linkage ID. Used to connect the additional information in this Text Message with another ASM. The Message Linkage ID and the source MMSI uniquely identify the sent message. 1 – 1023; 0 = not available.
		ACK Flag	1	Acknowledgement Flag; used to indicate acknowledgement status 0 = no acknowledgement requests = default; 1 = acknowledgement requested.
		Text length	8	Length of text message in characters. 0 – 142 characters; 143 = unknown = default; 144 – 255 = reserved.
		Text Message	0 – 852	User Text Message, 6-bit ASCII characters as per ITU 1371. 0 – 142 characters = 0 – 852 bits.
		Encryption Bit Padding	Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (128, 256, 384, 512, 640, 768, or 896). Set to 0.
		Checksum	16	16-bit CRC calculated as per EAIS Specification
Footer		Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
		Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
		Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
		Total bits	224 - 992	2 - 5 Slot Binary Message

2.5 Target of Interest

DAC**: 366** FI**:** **18** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant update of the FID 1 message listed in the Oct 2014 EAIS IDD. It also replaces the DAC 366 FID 58 message from the same document.

There are AIS Message 6, 8 and 26 variants of this message, but only message 26 is implemented.

2.5.4 Introduction

The Target of Interest message is used to report contacts.

2.5.5 Usage Notes

- The Message 26 TOI Message format provides for both a broadcast and addressed TOI message variation. Addressing, when required, shall be performed using the Destination Indicator and Destination ID fields inherent to the Message 26 structure.
- The report is intended to be repeated every 15 seconds until cancelled locally. The PI shall not retransmit if an ACK is not received.
- 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.
- Cancellation messages repeat four (4) times, 15 seconds apart. The PI shall not retransmit the cancellation message if an ACK is not received.
- This message can be used to report either vessel or aircraft targets.

2.5.6 Message 26 Addressed Format

Encrypted Target of Interest (Message 26, Addressed)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 1 (addressed).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	30	MMSI number of destination station.
	Spare	2	Not used, Set to zero.

Designated Area Code			10	Designated area code (DAC). Set to 366.
Function Identifier			6	Function identifier. Set to 18.
Encrypted Payload	Version		3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
	Message Linkage ID		10	A source-specific random number, unique across recent binary messages with Message Linkage ID. Used to connect the additional information in this Text Message with another ASM. The Message Linkage ID and the source MMSI uniquely identify the sent message. 1 – 1023; 0 = not available.
	Target Acquisition Source		3	Type of Target. 0 = unknown = default; 1 = AIS, 2 = Radar, 3 = visual sighting; 4 = reported; 5 = other electronic surveillance, i.e. DSC, ECDIS, etc.; 6 -7 = reserved.
	Target ID		30	MMSI if type is Target Acquisition source=1 (AIS), Sender generated ID otherwise
	TOI Status		2	Designator for TOI Status 0 = cancel; 1 = active; 2 = being followed; 3 = being boarded.
	Target Type		3	Type of Target 0 = vessel = default; 1 = aircraft; 2 = submersible; 3-7 = reserved.
	Target Description and Cargo		8	Description of target type and cargo, see Appendix 3.
	Interest		8	Code to indicate what interest in vessel is. To be defined. Could be used as an 8-bit binary matrix, similar to ATON Status bits. TBD.
	Time of TOI Report	UTC Hour	5	UTC Hour of TOI report. 0 – 23; 24 = UTC hour not available = default; 25 - 31 = reserved.
		UTC Min	6	UTC Minute of TOI report. 0 – 59; 60 = UTC minute not available = default; 61 - 63 (reserved for future use).
		UTC Sec	6	UTC Second of TOI report. 0 – 59; 60 = UTC second not available = default; 61 - 63 (reserved).
	Longitude		28	Longitude in 1/10,000 min (+/-180 degrees, East = positive, West = negative - 2's complement). 181 degrees = not available = default.
	Latitude		27	Latitude in 1/10,000 min (+/-180 degrees, East = positive, West = negative - 2's complement). 91 degrees = not available = default.
	SOG		10	Speed over ground. Scale dependent on value of craft flag. Aircraft: 0 – 1000 kts (1 kt increments); 1001 = 1001 kts or higher; 1002 = not available = default; 1003 – 1023 = reserved. Vessel: 0 – 100.0 kts (0.1 kt increments); 1001 = 100.1 kts or higher; 1002 = not available = default; 1003 – 1023 = reserved.
	COG		12	Course over ground in 1/10 degree steps. 0 - 359.9 degrees; 3600 = not available = default; 3601 - 4095 = reserved.
	Encryption Bit Padding		95	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256). Set to zero.
Checksum			16	16-bit CRC calculated as per EAIS Specification

Footer	Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	384	2 Slot Binary Message

2.5.7 Message 26 Broadcast Format

Encrypted Target of Interest Message (Message 26, Broadcast)

Parameter			# of Bits	Description
Standard Message Header	Message ID		6	Identifier for Message 26; always 26.
	Repeat Indicator		2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI		30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator		1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag		1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID		0	MMSI number of destination station. Not used.
	Spare		0	Not used.
Binary Data	Designated Area Code		10	Designated area code (DAC). Set to 366.
	Function Identifier		6	Function identifier. Set to 18.
	Encrypted Payload	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID	10	A source-specific random number, unique across recent binary messages with Message Linkage ID. Used to connect the additional information in this Text Message with another ASM. The Message Linkage ID and the source MMSI uniquely identify the sent message. 1 – 1023; 0 = not available.
		Target Acquisition Source	3	Type of Target. 0 = unknown = default; 1 = AIS, 2 = Radar, 3 = visual sighting; 4 = reported; 5 = other electronic surveillance, i.e. DSC, ECDIS, etc.; 6 -7 = reserved.
		Target ID	30	MMSI if type is Target Acquisition source=1 (AIS), Sender generated ID otherwise
		TOI Status	2	Designator for TOI Status 0 = cancel; 1 = active; 2 = being followed; 3 = being boarded.
		Target Type	3	Type of Target 0 = vessel = default; 1 = aircraft; 2 = submersible; 3-7 = reserved.
		Target Description and Cargo	8	Description of target type and cargo, see Appendix 3.
		Interest	8	Code to indicate what interest in vessel is. To be defined. Could be used as an 8-bit binary matrix, similar to ATON Status bits. TBD.

	Binary Data	Encrypted Payload	Time of TOI Report	UTC Hour	5	UTC Hour of TOI report. 0 – 23; 24 = UTC hour not available = default; 25 - 31 = reserved.
				UTC Min	6	UTC Minute of TOI report. 0 – 59; 60 = UTC minute not available = default; 61 - 63 (reserved for future use).
				UTC Sec	6	UTC Second of TOI report. 0 – 59; 60 = UTC second not available = default; 61 - 63 (reserved).
			Longitude		28	Longitude in 1/10,000 min (+/-180 degrees, East = positive, West = negative - 2's complement). 181 degrees = not available = default.
			Latitude		27	Latitude in 1/10,000 min (+/-180 degrees, East = positive, West = negative - 2's complement). 91 degrees = not available = default.
			SOG		10	Speed over ground. Scale dependent on value of craft flag. Aircraft: 0 – 1000 kts (1 kt increments); 1001 = 1001 kts or higher; 1002 = not available = default; 1003 – 1023 = reserved. Vessel: 0 – 100.0 kts (0.1 kt increments); 1001 = 100.1 kts or higher; 1002 = not available = default; 1003 – 1023 = reserved.
			COG		12	Course over ground in 1/10 degree steps. 0 - 359.9 degrees; 3600 = not available = default; 3601 - 4095 = reserved.
			Encryption Bit Padding		95	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256). Set to zero.
		Checksum			16	16-bit CRC calculated as per EAIS Specification
	Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
		Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
		Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
				Total bits	352	2 Slot Binary Message

2.6 Change RSI Command

DAC**: 366** FI**:** **19** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Change RSI (Radio Set Identifier) Command.

This ASM only has an AIS Message 26 variant.

2.6.4 Introduction

This ASM implements the Project 25 OTAR Change Radio Set Identifier (RSI) message.

2.6.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio to support the changeover of an individual or key management group Radio Set Identifier.
- This message is broadcast as a non-addressed message, to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.
- The "Subsequent RSI Change" field is optional and unlimited per Project 25. In order to fix message size at 5 slots, the number of instructions is limited to 8 per message.

2.6.6 Message 26 Broadcast Format

Change RSI Command (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		DAC		10	Designated Area Code. Set to 366.
		Function Identifier		6	Function identifier. Set to 19.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 3 = Change RSI Command
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 31 - 87.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to "10"
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to "11" (Type 3 MAC)
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number for the KMF to prevent message playback. Binary number representing values from 0 – 65535.
		Change RSI Instruction Count		8	The number of Change-RSI instructions in this message Set to (decimal) 1 - 8.
		Old RSI		24	Identifies the individual or group identifier that is to be changed or deleted.
		New RSI		24	Identifies the individual or group identifier which is to be added.
		RSI Message Number		16	Initial value for the inbound and outbound message numbers for RSI transaction. This is a rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535. Set to all zeroes if RSI is being deleted.
		Subsequent Change-RSI Instructions		0 – 448	Subsequent items are 64 bits apiece, Old RSI, New RSI, RSI message Number repeated for each item.

Binary Data	Encrypted Payload	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (384, 512, 640, 768). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				592 – 976	3 - 5 Slot Binary Message

2.7 Change RSI Response

DAC**: 366** FI**:** **20** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Change RSI (Radio Set Identifier) Response.

2.7.4 Introduction

This ASM implements the Project 25 OTAR Change Radio Set Identifier (RSI) message.

2.7.5 Usage Notes

- This message is sent from the Mobile Radio to the Key Management Facility to respond to the changeover of an individual or key management group Radio Set Identifier.
- This message is broadcast as a non-addressed message, to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.
- The "Subsequent Response" field is optional and unlimited per Project 25. In order to fix message size at 5 slots, the number of instructions is limited to 10 per message.

2.7.6 Message 26 Broadcast Format

Change RSI Response (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		DAC		10	Designated Area Code. Set to 366.
		Function Identifier		6	Function identifier. Set to 20.
	KMM Preamble		Reserved	3	Reserved for future use. Set to 0.
			Version	5	Version of KMM Preamble Message Body. Set to 0.
			MFID	8	Manufacturer's ID, indicates conformance to standard. Set to 0.
			Algorithm ID	8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
			Key ID	16	Identifies the TEK used to encrypt the KMM.
			Message Indicator	72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload		OTAR Message ID	8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 4 = Change RSI Response
			Message Length	16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 30 - 93.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to "11" (Type 3 MAC)
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
			Destination RSI	24	Radio Set Identifier number
			Source RSI	24	Radio Set Identifier Number
			KMF Message Number	16	A rolling sequence number for the KMF to prevent message playback. Binary number representing values from 0 – 65535.
			Change RSI Response Count	8	The number of Change-RSI responses in this message. Set to (decimal) 1 - 10.
			Old RSI	24	Identifies the individual or group identifier that was changed or deleted.
			New RSI	24	Identifies the individual or group identifier which was added.
			Status	8	The result of the Change-RSI request. Defined by the Project 25 Primitive Field definitions, section 10.3.24 of TIA-102.AACA-A, September 2014.
			Subsequent Change-RSI Responses	0 - 504	Subsequent items are 56 bits apiece, Old RSI, New RSI, and Status repeated for each item.

Binary Data	Encrypted Payload	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (384, 512, 640, 768). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				592 – 976	3 - 5 Slot Binary Message

2.8 Changeover Command

DAC**: 366** FI**: 21** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Changeover Command.

This ASM only has an AIS Message 26 variant.

2.8.4 Introduction

This ASM implements the Project 25 OTAR Changeover Command message.

2.8.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio (MR) to support the change of the active keyset(s) at an MR or group of MR.
- This message instructs a MR to start using an already held keyset. Thus, this message must be preceded by a successful Modify Key transaction.
- This message is broadcast as a non-addressed message, to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.
- The "Subsequent Changeover" field is optional and unlimited per Project 25. In order to limit message size to 5 slots, the count of instructions is limited to 35 per message.

2.8.6 Message 26 Broadcast Format

Changeover Command (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		DAC		10	Designated Area Code. Set to 366.
		Function Identifier		6	Function identifier. Set to 21.
	KMM Preamble		Reserved	3	Reserved for future use. Set to 0.
			Version	5	Version of KMM Preamble Message Body. Set to 0.
			MFID	8	Manufacturer's ID, indicates conformance to standard. Set to 0.
			Algorithm ID	8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
			Key ID	16	Identifies the TEK used to encrypt the KMM.
			Message Indicator	72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload		OTAR Message ID	8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 5 = Changeover Command
			Message Length	16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 25 - 93.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to "10"
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to "11" (Type 3 MAC)
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
			Destination RSI	24	Radio Set Identifier number
			Source RSI	24	Radio Set Identifier Number
			KMF Message Number	16	A rolling sequence number for the KMF to prevent message playback. Binary number representing values from 0 – 65535.
			Changeover Count	8	Number of changeover instructions in this message. Set to (decimal) 1 - 35.
			Superceded Keyset ID	8	Identifies the keyset which is superceded and must be deactivated. 1-255
			Activated Keyset ID	8	Identifies the keyset which must be activated. 1-255
			Subsequent Changeover Instructions	0 - 544	Subsequent items are 16 bits apiece, Superceded Keyset ID, and Activated Keyset ID repeated for each item.

Binary Data	Encrypted Payload	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256, 384, 512). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				464 – 976	3 – 5 Slot Binary Message

2.9 Changeover Response

DAC**: 366** FI**:** **22** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Changeover Response.

This ASM only has an AIS Message 26 variant.

2.9.4 Introduction

This ASM implements the Project 25 OTAR Changeover Command message.

2.9.5 Usage Notes

- This message is sent from the Mobile Radio (MR) to the Key Management Facility to the indicate the result of an instruction to change the active keyset(s) at an MR or group of MR.
- This message is broadcast as a non-addressed message, to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.
- The "Subsequent Changeover" field is optional and unlimited per Project 25. In order to limit message size to 5 slots, the count of instructions is limited to 35 per message

2.9.6 Message 26 Broadcast Format

Changeover Response (Message 26, broadcast)

Parameter		# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		DAC		10	Designated Area Code. Set to 366.
		Function Identifier		6	Function identifier. Set to 22.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 6 = Changeover Response
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 25 - 93.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Changeover Responses Count		8	The number of changeover responses in this message. Set to 1 - 35.
		Superceded Keyset ID		8	Identifies the keyset which is superceded and was deactivated. Value of 0 indicates specified keyset was not active (already changed over or nor present)
		Activated Keyset ID		8	Identifies the keyset which was activated. Value of 0 indicates that the specified keyset was not activated (keyset not present).
		Subsequent Changeover Responses		0 - 544	Subsequent items are 16 bits apiece, Superceded Keyset ID, and Activated Keyset ID repeated for each item.

Binary Data	Encrypted Payload	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256, 384, 512, 640, 768). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				464 – 976	3 - 5 Slot Binary Message

2.10 Hello

DAC**: 366** FI**:** **23** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Hello.

This ASM only has an AIS Message 26 variant.

2.10.4 Introduction

This ASM implements the Project 25 OTAR Hello message.

2.10.5 Usage Notes

- This message is sent from either the Mobile Radio (MR) or the Key Management Facility to provide simple identification.
- This message is also sent from the MR to the Key Management Facility to request rekey.
- This message is broadcast as a non-addressed message, to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.10.6 Message 26 Broadcast Format

Hello (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data	DAC			10	Designated Area Code. Set to 366.
	Function Identifier			6	Function identifier. Set to 23.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 7 = Hello
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 8.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 00
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 00 = No MAC
			Spare	1	Always zero.
			Done	1	Indicates if subsequent KMM messages are expected. 1=NOT DONE (more to follow), 0=DONE=default.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		Hello Flag		8	(hex) 00 = Identification Only, (hex) 01 = Rekey Request (UKEK exists) (hex) 02 = Rekey request (UKEK does not exist), (hex) 03-FF = Reserved.
		Encryption Bit Padding		40	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (128). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
			Total bits	336	2 Slot Binary Message

2.11 Modify Key Command

DAC**: 366** FI**:** **24** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Modify Key Command.

This ASM only has an AIS Message 26 variant.

2.11.4 Introduction

This ASM implements the Project 25 OTAR Modify Key Command message.

2.11.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio (MR) to modify one or more keys in the keyset.
- This message is broadcast as a non-addressed message, to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.
- The "Number of Keys" field is set at two per message, in order to reduce and fix message size within AIS slot count limits.

2.11.6 Message 26 Broadcast Format

Modify Key Command (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		DAC		10	Designated Area Code. Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 24.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 19 = Modify Key Command
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 59 - 88.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Decryption Instruction Format	Reserved Bit	1	Set to zero (not used).
			Message Indicator Block	1	Set to zero (not used).
			Spare	6	Always zero.
		KEK Algorithm ID		8	The algorithm ID is used in conjunction with the KeyID to uniquely select a KEK. Set to (hex) 85 = AES-128
		KEK Key ID		16	Identifies the Key ID for the KEK.
		Message Indicator		0	Optional, not used for AES-ECB wrapped keys.
		Keyset ID		8	The Keyset ID to be modified.

Binary Data	Encrypted Payload	Algorithm ID		8	The algorithm to be used for the keyset. Set to (hex) 85 = AES-128
		Key Length		8	The number of octets to transfer the key. Set to (decimal) 16.
		Number of Keys		8	The number of keys in this sequence. Set to (decimal) 1 - 2.
		Key Format	Key Type	1	0 = TEK, 1 = KEK
			Spare	1	Not used, set to zero.
			Delete/Rekey	1	0 = rekey (add new or change existing key), 1 = delete existing key
			Key Name Size	5	Defined the length in octets of the key name field. Set to (decimal) 8.
		Storage Location Number		16	Identifies one of 65536 possible storage location indices.
		Key ID		16	The Key ID of the key being modified.
		Key		128	The key, either a KEK or a TEK.
		Key Name	Function	16	Functional name or purpose of key. This will be a logical representation of the key (KEK, MAC key or TEK), as well as organization (USCG, NAVY, etc.)
			Month	16	Month identifier, typically of the publish date. (8 bit ASCII) 1-12
			Day	16	Day identifier, typically of the publish date. (8 bit ASCII) 1-31
			Year	16	Year (century agnostic) identifier, typically of the publish date. (8 bit ASCII) 0-99.
		Subsequent Key Items		0 - 232	Subsequent items are 232 bits apiece, Key Format to Key Name, inclusive repeated for each item.
		Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (512, 768). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification

Footer	Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	720 – 976	4 - 5 Slot Binary Message

2.12 Negative Acknowledgement

DAC**: 366** FI**:** **25** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Negative Acknowledgement Message.

This ASM only has an AIS Message 26 variant.

2.12.4 Introduction

This ASM implements the Project 25 OTAR Negative Acknowledgement message.

2.12.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio (MR) to respond to a Respond Kind 3 message which the receiving end does not understand, or has invalid message attributes (ID, number or MAC).
- When this response is received, it is assumed it refers to the most recent message sent.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.12.6 Message 26 Broadcast Format

Negative Acknowledgement (Message 26, broadcast)

Parameter		# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		DAC		10	Designated Area Code. Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 25.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 27 = Negative Acknowledge
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 26.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Message ID		8	Message ID that is being negatively acknowledged (if known), otherwise zero.
		Message Number		16	The KMF Message number of the last valid received command. This allows the KMF to determine if the Mobile Radio's MN is out of synchronization.
		Status		8	The reason for the negative acknowledgment. See Appendix 4.

Binary Data	Encrypted Payload	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		24	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				464	3 Slot Binary Message

2.13 Rekey Acknowledgement

DAC**: 366** FI**:** **26** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Rekey Acknowledgement Message.

This ASM only has an AIS Message 26 variant.

2.13.4 Introduction

This ASM implements the Project 25 OTAR Rekey Acknowledgement message.

2.13.5 Usage Notes

- This message is sent from the Mobile Radio (MR) to the Key Management Facility to respond to a Modify Key, Rekey or Warm Start command.
- The "Subsequent Key Status" field is limited in order to reduce and fix message size at 5 slots. A maximum of 17 Rekey Acknowledgements may be sent in a single message.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.13.6 Message 26 Broadcast Format

Rekey Acknowledgment (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		DAC		10	Designated Area Code. Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 26.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 29 = Rekey Acknowledge
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 28 - 92.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Message ID		8	Message ID that is being acknowledged.
		Number of Rekey Statuses		8	The number of key statuses in this acknowledgement. Set to (decimal) 1 - 17.
		Algorithm ID		8	Algorithm code is used in conjunction with Key ID to uniquely select a key. Set to (hex) 85 = AES-128.
		Key Id		16	The subject Key ID of the rekey operation.
		Status		8	The status of the rekey. See Appendix 4.
		Subsequent Key Status		0 - 512	Subsequent items are 32 bits apiece, Algorithm ID to Status, inclusive repeated for each item.

Binary Data	Encrypted Payload	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256, 384, 512, 640, 768). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				464 – 976	3 - 5 Slot Binary Message

2.14 Rekey Command

DAC**: 366** FI**:** **27** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Rekey Command Message.

This ASM only has an AIS Message 26 variant.

2.14.4 Introduction

This ASM implements the Project 25 OTAR Rekey Command message.

2.14.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio (MR) to add or modify keysets, or to add or modify keys in a keyset.
- The “Number of Keyset” field is set at the Project 25 minimum, one per message, in order to reduce and fix message size. Likewise, a max of one key can be sent per keyset, based on AIS message length limits.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.14.6 Message 26 Broadcast Format

Rekey Command (Message 26, broadcast)

Parameter		# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		DAC		10	Designated Area Code. Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 27.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 30 = Rekey Command
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 74.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Decryption Instruction Format	Reserved Bit	1	Set to zero (not used).
			Message Indicator Block	1	Set to zero (not used).
			Spare	6	Always zero.
		KEK Algorithm ID		8	The algorithm is used in conjunction with the KeyID to uniquely select a KEK. Set to (hex) 85 = AES-128
		KEK Key ID		16	Identifies the Key ID for the KEK.
		Message Indicator		0	Optional, not used for AES-ECB wrapped keys.
		Number of Keysets		8	The number of keysets in this sequence. Set to (decimal) 1.

Binary Data	Encrypted Payload	Keyset Format	Keyset Type	1	0 = TEK, 1 = KEK
			Reserved	1	Indicates if 24 bit "reserved" block is used. Set to zero = not used.
			DT	1	Date/Time. Indicates if the 40 bit Date and Time block is included in the keyset block. Set to one = used.
			Keyset Name Size	5	The length in octets (ASCII chars) of the keyset name field. Set to (decimal) 8.
		Keyset ID		8	The Keyset ID to be modified/added.
		Algorithm ID		8	The algorithm to be used for the keyset. Set to (hex) 85 = AES-128
		Reserved		0	Not used.
		Date	Month	4	The month (UTC) the keyset becomes active. 1-12
			Day	5	The day (UTC) the keyset becomes active. 1 – 31
			Year	7	The year (UTC) the keyset becomes active. 0 – 99 (century is assumed)
		Time		24	The time (UTC) when the keyset becomes active. See Appendix 4 for format.
		Keyset Name	Function	16	Functional name or purpose of key. This will be a logical representation of the key (KEK, MAC key or TEK), as well as organization (USCG, NAVY, etc.)
			Month	16	Month identifier, typically of the publish date. (8 bit ASCII) 1-12
			Day	16	Day identifier, typically of the publish date. (8 bit ASCII) 1-31
			Year	16	Year (century agnostic) identifier, typically of the publish date. (8 bit ASCII) 0-99.
		Key Length		8	The number of octets to transfer the key. Set to (decimal) 16.
		Number of Keys		8	The number of keys in this sequence. Set to (decimal) 1.
		Key Format	Key Type	1	0 = TEK, 1 = KEK
			Spare	1	Not used, set to zero.
			Delete/Rekey	1	0 = rekey (add new or change existing key), 1 = delete existing key
			Key Name Size	5	Defined the length in octets of the key name field. Set to (decimal) 8.
		Storage Location Number		16	Identifies one of 65536 possible storage location indices.
		Key ID		16	The Key ID of the key being modified.
		Key		128	The key, either a KEK or a TEK.

Binary Data	Encrypted Payload	Key Name	Function	16	Functional name or purpose of key. See Appendix 5.
			Month	16	Month identifier, typically of the publish date. (8 bit ASCII) 1-12
			Day	16	Day identifier, typically of the publish date. (8 bit ASCII) 1-31
			Year	16	Year (century agnostic) identifier, typically of the publish date. (8 bit ASCII) 0-99.
		Subsequent Key Items		0	Subsequent items are 232 bits apiece, Key Format to Key Name, inclusive repeated for each item. Not used.
		Subsequent Keyset Items		0	Not used.
		Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		24	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (640). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				848	5 Slot Binary Message

2.15 Warm-Start Command

DAC**: 366** FI**:** **28** (Unencrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Warm Start Command Message.

This ASM only has an AIS Message 26 variant.

2.15.4 Introduction

This ASM implements the Project 25 OTAR Warm Start Command message.

2.15.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio to provide TEKS when the MR has a valid KEK but no TEKs.
- Complying with NIST requirements for a separate (non-derived) key for computing the MAC is impossible, as the Project 25 standard calculates the MAC of a Warm Start Message using a key derived from the received TEK.
- This message is broadcast as a non-addressed message, with repeat disabled, to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.15.6 Message 26 Broadcast Format

Warm Start Command (Message 26, broadcast)

Parameter		# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to one (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Application Data (unencrypary Datae)	Designated Area Code		10	Designated area code (DAC). This code is based on the maritime identification digits (MID). Set to 366.
	Function Identifier		6	Function identifier. Set to (decimal) 28.
	KMM Preamble	Reserved	3	Reserved for future use. Set to 0.
		Version	5	Version of KMM Preamble Message Body. Set to 0.
		MFID	8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID	8	Identifies the payload encryption algorithm. Set to (hex) 80 = unencrypted.
		Key ID	16	Identifies the TEK used to encrypt the KMM. Set to 0.
		Message Indicator	72	Provides the message indicator to synchronize the encryption of the OTAR KMM. Set to zero.
	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 32 = Warm Start Command
	Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 49.
	Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
		MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
		MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
		Spare	1	Set to zero.
		Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
	Destination RSI		24	Radio Set Identifier number
	Source RSI		24	Radio Set Identifier Number
	KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
	Decryption Instruction Format	Reserved Bit	1	Set to zero (not used).
		Message Indicator Block	1	Set to zero (not used).
		Spare	6	Always zero.
	KEK Algorithm ID		8	The algorithm is used in conjunction with the KeyID to uniquely select the KEK. Set to (hex) 85 = AES-128
	KEK Key ID		16	Identifies the Key ID for the KEK used.
	Message Indicator		0	Optional, not used for AES-ECB wrapped keys.

	Key Length		8	The number of octets to transfer the key. Default = (decimal) 16, however, can be any value.
	Algorithm ID		8	The algorithm to be used for the keyset. Set to (hex) 85 = AES-128
	Key Format	Key Type	1	Set to 0 = TEK
		Spare	1	Not used, set to zero.
		Delete/Rekey	1	Set to 0 = rekey (add new key)
		Key Name Size	5	Set to zero.
	Storage Location Number		16	Identifies one of 65536 possible storage location indices.
	Key ID		16	The Key ID of the warm start TEK.
	Key		128	The warm start TEK, encrypted with already held KEK.
	Key Name		0	Not used.
	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
		MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
		MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
		MAC Key ID	16	Identifies the Key to be used to compute the MAC. Set to zero.
		T	1	Not used. Set to zero.
		D	1	Derived Key. Set to one = Derived MAC Key
		R	1	Reserved for future use. Set to zero.
		Version	5	Defines the version of the MAC message body. Set to zero.
Footer	Spare		4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector		1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State		19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
		Total bits	608	3 Slot Binary Message

2.16 Zeroize Command

DAC**: 366** FI**:** **29** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Zeroize Command Message.

This ASM only has an AIS Message 26 variant.

2.16.4 Introduction

This ASM implements the Project 25 OTAR Zeroize Command message.

2.16.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio to zeroize all keys and keysets on the MR.
- There is no information contained in the message body.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.16.6 Message 26 Broadcast Format

Zeroize Command (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		Designated Area Code		10	Designated area code (DAC). Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 29.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 33 = Zeroize Command
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 22.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		56	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256). Set to zero.

	Checksum	16	16-bit CRC calculated as per EAIS Specification
Footer	Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	464	3 Slot Binary Message

2.17 Zeroize Response

DAC**: 366** FI**:** **30** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Zeroize Response Message.

This ASM only has an AIS Message 26 variant.

2.17.4 Introduction

This ASM implements the Project 25 OTAR Zeroize Response message.

2.17.5 Usage Notes

- This message is sent from the Mobile Radio to the Key Management Facility in response to a Zeroize Command. This provides confirmation of message receipt.
- There is no information contained in the message body.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.17.6 Message 26 Broadcast Format

Zeroize Response (Message 26, broadcast)

Parameter		# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		Designated Area Code		10	Designated area code (DAC). Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 30.
	KMM Preamble		Reserved	3	Reserved for future use. Set to 0.
			Version	5	Version of KMM Preamble Message Body. Set to 0.
			MFID	8	Manufacturer's ID, indicates conformance to standard. Set to 0.
			Algorithm ID	8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
			Key ID	16	Identifies the TEK used to encrypt the KMM.
			Message Indicator	72	Provides the message indicator to synchronize the encryption of the OTAR KMM
	Encrypted Payload		OTAR Message ID	8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 34 = Zeroize Response
			Message Length	16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 22.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
			Destination RSI	24	Radio Set Identifier number
			Source RSI	24	Radio Set Identifier Number
			KMF Message Number	16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
			Encryption Bit Padding	56	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256). Set to zero.

	Checksum	16	16-bit CRC calculated as per EAIS Specification
Footer	Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	464	3 Slot Binary Message

2.18 Delete Key Command

DAC**: 366** FI**:** **31** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Delete Key Command Message.

This ASM only has an AIS Message 26 variant.

2.18.4 Introduction

This ASM implements the Project 25 OTAR Delete Key Command message.

2.18.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio to delete keys on the MR.
- The “Number of Unique Key IDs” field is limited to 23 per message, in order to remain within the AIS limit of five slot messages.
- This message is broadcast as a non-addressed message, with repeat disabled, to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.18.6 Message 26 Broadcast Format

Delete Key Command (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		Designated Area Code		10	Designated area code (DAC). Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 31.
	KMM Preamble		Reserved	3	Reserved for future use. Set to 0.
			Version	5	Version of KMM Preamble Message Body. Set to 0.
			MFID	8	Manufacturer's ID, indicates conformance to standard. Set to 0.
			Algorithm ID	8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
			Key ID	16	Identifies the TEK used to encrypt the KMM.
			Message Indicator	72	Provides the message indicator to synchronize the encryption of the OTAR KMM.
	Encrypted Payload		OTAR Message ID	8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 8 = Delete Key Command
			Message Length	16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. (decimal) 26 – 92.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
			Destination RSI	24	Radio Set Identifier number
			Source RSI	24	Radio Set Identifier Number
			KMF Message Number	16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
			Number of Unique Key IDs	8	Number of keys to be deleted. (decimal) 1 – 23.
			Algorithm ID	8	The algorithm is used in conjunction with the KeyID to uniquely select a key. Set to (hex) 85 = AES-128
			Key ID	16	Identifies the Key ID to be deleted.
			Subsequent Key Items	0 - 528	Subsequent items are 24 bits apiece, Algorithm ID and Key ID repeated for each item.

Binary Data	Encrypted Payload	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256, 384, 512, 640, 768). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				464 – 976	3 - 5 Slot Binary Message

2.19 Delete Key Response

DAC**: 366** FI**:** **32** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Delete Key Response Message.

This ASM only has an AIS Message 26 variant.

2.19.4 Introduction

This ASM implements the Project 25 OTAR Delete Key Response message.

2.19.5 Usage Notes

- This message is sent from the Mobile Radio to the Key Management Facility in response to a Delete Key Command message.
- The "Number of Key Statuses" field is limited to 17 per message, in order remain within the AIS limit of five slot messages.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.19.6 Message 26 Broadcast Format

Delete Key Response (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data	Designated Area Code			10	Designated area code (DAC). Set to 366.
	Function Identifier			6	Function identifier. Set to (decimal) 32.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM.
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 9 = Delete Key Response
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. (decimal) 27 – 91.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Number of Unique Key IDs		8	Number of keys deleted. (decimal) 1 – 17.
		Algorithm ID		8	The algorithm is used in conjunction with the KeyID to uniquely select a key. Set to (hex) 85 = AES-128
		Key ID		16	Identifies the Key ID to be deleted.
		Status		8	The status of the rekey. See Appendix 4.
		Subsequent Key Items		0 - 512	Subsequent items are 32 bits apiece, Algorithm ID, Key ID and Status repeated for each item.

Binary Data	Encrypted Payload	Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256, 384, 512, 640, 780). Set to zero.
	Checksum			16	16-bit CRC calculated as per EAIS Specification
Footer	Spare			4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector			1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State			19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits				464 – 976	3 - 5 Slot Binary Message

2.20 Registration Command

DAC**: 366** FI**:** **33** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Registration Command Message.

This ASM only has an AIS Message 26 variant.

2.20.4 Introduction

This ASM implements the Project 25 OTAR Registration Command message.

2.20.5 Usage Notes

- This message is sent from the Mobile Radio to the Key Management Facility to indicate the MR is on the system and available for OTAR service..
- The OTAR portion of this message is variable length, depending if a reverse warm start is attempted. Optional fields are indicated by the light purple color.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.20.6 Message 26 Broadcast Format

Registration Command (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data	Designated Area Code			10	Designated area code (DAC). Set to 366.
	Function Identifier			6	Function identifier. Set to (decimal) 33.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM.
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 37 = Registration Command
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. (decimal) 49 or 53.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Body Message Format	T	1	TEK Included. 0 = message only contains message subheader, 1 = a Reverse Warm Start TEK segment exists.
			K	1	KEK Exists. 0 = KEK exists, 1 = KEK does not exist.
			Spare	6	Always zero.
		KMF RSI		24	Radio Set Identifier for the Key Management Facility
		Decryption Instruction Format	Reserved Bit	1/0	Set to zero (not used).
			Message Indicator Block	1/0	Set to zero (not used).
			Spare	6/0	Always zero.
		Reverse Warm Start Algorithm ID		8/0	The algorithm is used in conjunction with the KeyID to uniquely select a KEK. Set to (hex) 85 = AES-128

Binary Data	Encrypted Payload	Reverse Warm Start Key ID			16/0	Identifies the Key ID for the TEK.
		Message Indicator			0	Optional, not used for AES-ECB wrapped keys.
		Key Length			8	The number of octets to transfer the key. Set to (decimal) 16.
		Algorithm ID			8	The algorithm of the KEK used to encrypt the TEK. Set to (hex) 85 = AES-128
		Key Format	Key Type		1	Set to 0 = TEK.
			Spare		1	Not used, set to zero.
			Delete/Rekey		1	0 = rekey (add new or change existing key), 1 = delete existing key
			Key Name Size		5	Defined the length in octets of the key name field. Set to (decimal) 0.
		Storage Location Number			16	Set to zero.
		Key ID			16	The Key ID of the key being sent.
		Key			128	The TEK.
		Key Name			0	Not used.
		Message Authentication Code	MAC		64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length		8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID		8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID		16	Identifies the Key to be used to compute the MAC
			T		1	Not used. Set to zero.
			D		1	Derived Key. Set to zero = Dedicated MAC Key
			R		1	Reserved for future use. Set to zero.
			Version		5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding			Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (512). Set to zero.
	Checksum				16	16-bit CRC calculated as per EAIS Specification
Footer	Spare				4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector				1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State				19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits					720	4 Slot Binary Message

2.21 Registration Response

DAC**: 366** FI**:** **34** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Registration Response Message.

This ASM only has an AIS Message 26 variant.

2.21.4 Introduction

This ASM implements the Project 25 OTAR Registration Response message.

2.21.5 Usage Notes

- This message is sent from the Key Management Facility to the Mobile Radio to indicate the receipt and success or failure of request.
- Project 25 dictates that if a Registration Request has a MAC, then the Response must also have a MAC.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.21.6 Message 26 Broadcast Format

Registration Response (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to one (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data	Designated Area Code			10	Designated area code (DAC). Set to 366.
	Function Identifier			6	Function identifier. Set to (decimal) 34.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM.
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 38 = Registration Response
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. Set to (decimal) 23.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Status		8	The status of the rekey. See Appendix 4.
		Message Authentication Code	MAC	64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length	8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID	8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID	16	Identifies the Key to be used to compute the MAC
			T	1	Not used. Set to zero.
			D	1	Derived Key. Set to zero = Dedicated MAC Key
			R	1	Reserved for future use. Set to zero.
			Version	5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding		48	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256). Set to zero.

	Checksum	16	16-bit CRC calculated as per EAIS Specification
Footer	Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	464	3 Slot Binary Message

2.22 Unable to Decrypt Response

DAC**: 366** FI**:** **35** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant implementation of the Project 25 OTAR Unable to Decrypt Response Message.

This ASM only has an AIS Message 26 variant.

2.22.4 Introduction

This ASM implements the Project 25 OTAR Unable to Decrypt Response message.

2.22.5 Usage Notes

- This message is sent from the Mobile Radio (MR) to the Key Management Facility when a Key Management Message cannot be decrypted by the MR.
- When the KMF receives this message, it is assumed that it refers to the most recently transmitted message.
- This message is broadcast as a non-addressed message to reduce the message size, and to avoid issues from a relocated RSI to a different MMSI.

2.22.6 Message 26 Broadcast Format

Unable to Decrypt Response (Message 26, broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always (decimal) 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to zero (broadcast).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not used.
	Spare	0	Not used.

Binary Data		Designated Area Code		10	Designated area code (DAC). Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 35.
	KMM Preamble	Reserved		3	Reserved for future use. Set to 0.
		Version		5	Version of KMM Preamble Message Body. Set to 0.
		MFID		8	Manufacturer's ID, indicates conformance to standard. Set to 0.
		Algorithm ID		8	Identifies the algorithm used to encrypt payload. Set to (hex) 85 = AES-128.
		Key ID		16	Identifies the TEK used to encrypt the KMM.
		Message Indicator		72	Provides the message indicator to synchronize the encryption of the OTAR KMM.
	Encrypted Payload	OTAR Message ID		8	Identifies the Project 25 "Message ID" type. One of 255 possible values assigned as the message type. Set to (decimal) 39 = Unable to Decrypt
		Message Length		16	A 16 bit binary number that defines the length (in octets) of the subsequent OTAR fields, including MAC. (decimal) 51 or 55.
		Message Format	RSP	2	Response Kind defines acknowledgment to be returned to the sender of the KMM. 00 =Rsp Kind 1, 01 = Rsp Kind 2, 10 = Rsp Kind 3 and 11 is undefined.
			MN	2	Message Number defines the size of the Message Number field in the KMM. 00 = no message number, 10 = a 2 octet message number. Set to (binary) 10
			MAC Processing	2	Defines the type of MAC processing performed over the entire KMM. Set to (binary) 11 = Type 3 MAC
			Spare	1	Set to zero.
			Done	1	Indicates if KMM is last in a series. 1 = More to follow (Not Done), 0 = done.
		Destination RSI		24	Radio Set Identifier number
		Source RSI		24	Radio Set Identifier Number
		KMF Message Number		16	A rolling sequence number to prevent message playback. Binary number representing values from 0 – 65535.
		Body Message Format	T	1	TEK Included. 0 = message only contains message subheader, 1 = a Reverse Warm Start TEK segment exists.
			K	1	KEK Exists. 0 = KEK exists, 1 = KEK does not exist.
			Spare	6	Always zero.
		ESYNC MFID		8	MFID used in original message which could not be decrypted
		ESYNC Algorithm ID		8	Alg ID used in the original message which could not be decrypted.
		ESYNC Key ID		16	Key ID of original message which could not be decrypted
		Status		8	Reason for the failed decryption. See Appendix 4.

Binary Data	Encrypted Payload	Decryption Instruction Format	Reserved Bit		1/0	Set to zero (not used).
			Message Indicator Block		1/0	Set to zero (not used).
			Spare		6/0	Always zero.
		Reverse Warm Start Algorithm ID			8/0	The algorithm is used in conjunction with the KeyID to uniquely select a KEK. Set to (hex) 85 = AES-128
		Reverse Warm Start Key ID			16/0	Identifies the Key ID for the TEK.
		Message Indicator			0	Optional, not used for AES-ECB wrapped keys.
		Key Length			8	The number of octets to transfer the key. Set to (decimal) 16.
		Algorithm ID			8	The algorithm of the KEK used to encrypt the TEK. Set to (hex) 85 = AES-128
		Key Format	Key Type		1	Set to 0 = TEK.
			Spare		1	Not used, set to zero.
			Delete/Rekey		1	0 = rekey (add new or change existing key), 1 = delete existing key
			Key Name Size		5	Defined the length in octets of the key name field. Set to (decimal) 0.
		Storage Location Number			16	Set to zero.
		Key ID			16	The Key ID of the key being sent.
		Key			128	The TEK.
		Key Name			0	Not used.
		Message Authentication Code	MAC		64	OTAR Message authentication code, concatenated to key length/2. Calculated per paragraph 13.5.2 of TIA 102.AACA-A, September 2014.
			MAC Length		8	Length of message authentication code in octets. Set to (decimal) 8
			MAC Algorithm ID		8	Used with MAC Key ID to uniquely determine key to used to produce MAC. Set to (hex) 85 = AES-128.
			MAC Key ID		16	Identifies the Key to be used to compute the MAC
			T		1	Not used. Set to zero.
			D		1	Derived Key. Set to zero = Dedicated MAC Key
			R		1	Reserved for future use. Set to zero.
			Version		5	Defines the version of the MAC message body. Set to zero.
		Encryption Bit Padding			variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (512). Set to zero.
	Checksum				16	16-bit CRC calculated as per EAIS Specification

Footer	Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits	720	4 Slot Binary Message

2.23 Area Notice

DAC**: 366** FI**: 36** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:

This is an encrypted version of IMO Circ. 289 DAC:001 FI: **22** and **23** listed on IALA ASM collection.

This ASM only has a Message 26 variant.

2.23.4 Introduction

This message provides encrypted dynamic information concerning a specified geographic area, polyline or positions.

2.23.5 Usage Notes

- This Message 26 Area Notice provides for both a broadcast and addressed messages. Message addressing, when required, shall be performed using the Destination Indicator and Destination ID fields inherent to the Message 26 structure.
- There can be from up to 9 sub-areas associated with each notice.
- This message can be used to convey advisory lines or tracks, but Route Information should be used recommended or directed route.
- The PI shall expect an ACK for the addressed form of the message, and shall retransmit according to the Usage Notes of FID 9 if it does not receive one.

2.23.6 Message 26 Addressed Format

Encrypted Area Notice Message (Message 26, Addressed)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 1 (addressed).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	30	MMSI number of destination station.
	Spare	2	Not used, Set to zero.

Binary Data	Designated Area Code				10	Designated area code (DAC). Set to 366.
	Function Identifier				6	Function identifier. Set to (decimal) 36.
	Encrypted Payload	Version			3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID			10	A source-specific random number, unique across recent binary messages with Message Linkage ID. Used to connect the additional information in this Area Notice Message with another ASM. The Message Linkage ID and the source MMSI uniquely identify the sent message. 1 – 1,023; 0 = not available.
		Notice Description			7	Notice Description as defined in Table 11.11. Set to 0-127 according to description. If = 127 there must be associated text (reference Table 11.10 & Table 11.11 of IALA ASM DAC=001, FI=23)
		Start date and time of Area	UTC Month		4	Start UTC month of the Area notice. 1 -12 0 = not available = default 13 -15 = reserved for future use
			UTC Day		5	Start UTC day of the Area notice. 1 -31 0 = not available = default
			UTC Hour		5	Start UTC hour of the Area notice. 0 – 23 24 = not available = default 25- 31 = reserved for future use
			UTC Minute		6	Start UTC Minute of the Area notice 0 – 59 60 = not available = default 61-63 reserved for future use
		Duration			18	Minutes until end of Area notice. Measured from start date and time of Area Notice. 0 = cancel Area Notice 262,143 = undefined = default Maximum duration is 262,142 minutes (182.04 days).
		Number of Sub-areas			4	1 – 9
		Sub- areas			Max 783	From 1 to 9 sub-areas, each structured as in Tables 11.4 - 11.9 of IALA ASM DAC=001, FI=22. A short text description may be associated with the areas using Sub-area 5: Associated text (see Table 11.10). Each sub-area is 87 bits.
		Encryption Bit Padding			Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (128, 256, 384, 512, 640, 768, or 896). Set to 0.
	Checksum				16	16-bit CRC calculated as per EAIS Specification
Footer	Spare				4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector				1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State				19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
	Total bits				384 – 1024	2 - 5 Slot Binary Message

2.23.7 Message 26 Broadcast Format

Encrypted Area Notice Message (Message 26, Broadcast)

Parameter				# of Bits	Description
Standard Message Header	Message ID			6	Identifier for Message 26; always 26.
	Repeat Indicator			2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI			30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator			1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 0 (broadcast).
	Binary Data Flag			1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID			0	MMSI number of destination station. Not used.
	Spare			0	Not used.
Binary Data	Designated Area Code			10	Designated area code (DAC). Set to 366.
	Function Identifier			6	Function identifier. Set to 36.
	Encrypted Payload	Version		3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID		10	A source-specific random number, unique across recent binary messages with Message Linkage ID. Used to connect the additional information in this area notice Message with another ASM. The Message Linkage ID and the source MMSI uniquely identify the sent message. 1 – 1,023; 0 = not available.
		Notice Description		7	Notice Description as defined in Table 11.11. Set to 0-127 according to description. If = 127 there must be associated text (reference Table 11.10 and 11.11 of IALA ASM DAC=001, FI=23)
		Start date and time of Area	UTC Month	4	Start UTC month of the Area notice. 1 -12 0 = not available = default, 13 -15 = reserved for future use
			UTC Day	5	Start UTC day of the Area notice. 1 -31 0 = not available = default
			UTC Hour	5	Start UTC hour of the Area notice. 0 – 23 24 = not available = default, 25- 31 = reserved for future use
			UTC Minute	6	Start UTC Minute of the Area notice. 0 – 59 60 = not available = default, 61-63 reserved for future use
		Duration		18	Minutes until end of Area notice. Measured from start date and time of Area Notice. 0 = cancel Area Notice, 262,143 = undefined = default Maximum duration is 262,142 minutes (182.04 days).
		Number of Sub-areas		4	Total count of sub-areas. 1 – 9
		Sub- areas		Max 783	From 1 to 9 sub-areas, each structured as in Tables 11.4 - 11.9 of IALA ASM DAC=001, FI=22. A short text description may be associated with the areas using Sub-area 5: Associated text (see Table 11.10). Each sub-area is 87 bits.
		Encryption Bit Padding		Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256, 384, 512, 640, 768, or 896). Set to 0.

	Checksum	16	16-bit CRC calculated as per EAIS Specification
Footer	Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
Total bits		352 – 992	2 - 5 Slot Binary Message

2.24 Route Information

DAC**: 366** FI**:** **37** (Encrypted)

Published**: 12 May 2016** Version**: 0**

Summary of changes:

Version 0:
This is an encrypted version of Route information IMO Circ. 289 DAC:001 FI: 27 and 28 listed in IALA ASM collection.

This ASM only has a Message 26 variant.

2.24.4 Introduction

This message provides encrypted information concerning a route.

2.24.5 Usage Notes

- This Message 26 Route Information provides for both broadcast and addressed messages. Message addressing, when required, shall be performed using the Destination Indicator and Destination ID fields inherent to the Message 26 structure.
- The route may contain up to 14 waypoints, to keep maximum message size parity with other STEDS messages.
- The PI shall expect an ACK for the addressed form of the message, and shall retransmit according to the Usage Notes of FID 9 if it does not receive one.

2.24.6 Message 26 Addressed Format

Encrypted Route Information Message (Message 26, Addressed)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 1 (addressed).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	30	MMSI number of destination station.
	Spare	2	Not used, Set to zero.

Binary Data		Designated Area Code		10	Designated area code (DAC). Set to 366.
		Function Identifier		6	Function identifier. Set to (decimal) 37.
	Encrypted Payload	Version		3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID		10	A source-specific random number, unique across recent binary messages with Message Linkage ID. Used to connect the additional information in this Route Message with another ASM. The Message Linkage ID and the source MMSI uniquely identify the sent message. 1 – 1,023; 0 = not available.
		Sender Classification		3	0 = ship = default, 1 = authority, 2 - 7 (reserved for future use)
		Route Type		5	0 = not available = default 1 = mandatory route 2 = recommended route 3 = alternative route 4 = recommended route through ice 5 = ship route plan 6 - 30 (reserved for future use) 31 = cancellation (cancel route as identified by Message Linkage ID)
		Start date and time of route	UTC Month	4	Start UTC month of the Area notice. 1 -12 0 = not available = default, 13 -15 = reserved for future use
			UTC Day	5	Start UTC day of the Area notice. 1 -31 0 = not available = default
			UTC Hour	5	Start UTC hour of the Area notice. 0 – 23 24 = not available = default, 25- 31 = reserved for future use
			UTC Minute	6	Start UTC Minute of the Area notice 0 – 59 60 = not available = default, 61-63 reserved for future use
		Duration		18	Minutes until end of Validity Route. Measured from start date and time of Route Information. 0 = cancel route, 262,143 = undefined = default Maximum duration is 262,142 minutes (182.04 days).
		Number of waypoints		5	Number of waypoints. 1 – 14 0 = no waypoint = default, 15 - 31 (not used)
		Waypoints		Max 770	Variable number of waypoints 1 - 14 (55 bit each), reference Table 13.3, IALA ASM DAC=001, FI=28). The number of waypoints is determined by the length of the message.
		Encryption Bit Padding		Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (256, 384, 512, 640, 768, or 896). Set to 0.
		Checksum		16	16-bit CRC calculated as per EAIS Specification
Footer		Spare		4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
		Communications State Selector		1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
		Communications State		19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
			Total bits	256 – 1024	2 - 5 Slot Binary Message

2.24.7 Message 26 Broadcast Format

Encrypted Route Information Message (Message 26, Broadcast)

Parameter				# of Bits	Description
Standard Message Header	Message ID			6	Identifier for Message 26; always 26.
	Repeat Indicator			2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI			30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator			1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 0 (broadcast).
	Binary Data Flag			1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID			0	MMSI number of destination station. Not used.
	Spare			0	Not used.
Binary Data	Designated Area Code			10	Designated area code (DAC). Set to 366.
	Function Identifier			6	Function identifier. Set to 37.
	Encrypted Payload	Version		3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Message Linkage ID		10	A source-specific random number, unique across recent binary messages with Message Linkage ID. Used to connect the additional information in this Route Message with another ASM. The Message Linkage ID and the source MMSI uniquely identify the sent message. 1 – 1,023; 0 = not available.
		Sender Classification		3	0 = ship = default, 1 = authority, 2 - 7 (reserved for future use)
		Route Type		5	0 = not available = default 1 = mandatory route 2 = recommended route 3 = alternative route 4 = recommended route through ice 5 = ship route plan 6 - 30 (reserved for future use) 31 = cancellation (cancel route as identified by Message Linkage ID)
		Start date and time of Route	UTC Month	4	Start UTC month of the Area notice. 1 -12 0 = not available = default, 13 -15 = reserved for future use
			UTC Day	5	Start UTC day of the Area notice. 1 -31 0 = not available = default
			UTC Hour	5	Start UTC hour of the Area notice. 0 – 23 24 = not available = default, 25- 31 = reserved for future use
			UTC Minute	6	Start UTC Minute of the Area notice. 0 – 59 60 = not available = default, 61-63 reserved for future use

		Duration	18	Minutes until end end of route validity. Measured from start date and time of Route Information. 0 = cancel Area Notice, 262,143 = undefined = default Maximum duration is 262,142 minutes (182.04 days).
		Number of waypoints	5	Number of waypoints. 1 - 14 0 = no waypoint = default, 15 - 31 (not used)
		Waypoints	Max 770	Variable number of waypoints 1 - 14 (55 bit each), reference Table 13.3 of IALA ASM DAC=001, FI=28. The number of waypoints is determined by the length of the message.
		Encryption Bit Padding	Variable	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption (128, 256, 384, 512, 640, 768, or 896). Set to 0.
	Checksum		16	16-bit CRC calculated as per EAIS Specification
Footer	Spare		4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
	Communications State Selector		1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
	Communications State		19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
		Total bits	224 – 992	2 - 5 Slot Binary Message

2.25 Situation Report (SITREP) for Vessels and Aircraft

DAC**: 366** FI**:** **38** (Encrypted)

Published**: 21 Apr 2017** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant update of the FID 0 Message 25 listed in the Oct 2014 EAIS IDD. It also replaces the DAC 366, FI 56 Position Report from the same document.

2.25.1 Introduction

The Situation Report Message is used to send the equivalent information to AIS Message 1 but removes less essential data to compress message size.

2.25.2 Usage Notes

- This same report can be used for both vessels and aircraft.

Note: Only aircraft engaged in SAR (using SAR transponder) may transmit AIS.

- The 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. Aircraft should transmit at 10-second intervals..

2.25.3 Message 26 Format

Encrypted Situation Report (Message 26, Broadcast)

Parameter		# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 1 (addressed).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not Used.
	Spare	0	Not used.

Binary Data		Designated Area Code	10	Designated area code (DAC). Set to 366.
		Function Identifier	6	Function identifier. Set to (decimal) 38.
	Encrypted Payload	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Time of Position - UTC Min	6	UTC Minute of the position. 0 – 59; 60 = UTC minute not available = default; 61 - 63 (reserved for future use).
		Time of Position - UTC Sec	3	UTC Seconds of the position; 10-second resolution. 0 = 0 sec; 1 =10 sec; 2 = 20 sec; 3 = 30 sec; 4 = 40 sec; 5 = 50 sec; 6 = unknown = default; 7 = (reserved for future use).
		Craft Flag	1	Indicates whether report is from a vessel or aircraft. 0 = vessel = default; 1 = aircraft.
		Longitude	28	Longitude in 1/10,000 min (±180 degrees, East = positive, West = negative. 181 degrees = not available = default). Negative in 2's complement.
		Latitude	27	Latitude in 1/10,000 min (±90 degrees, North = positive, South = negative, 91 degrees = not available = default). Negative in 2's complement.
		Altitude	12	Altitude above sea level in 1m increments. Set to 0 for vessels. 0-4,000 m; 4001 = 4,001 m or higher; 4,002 = unknown = default.
		COG	12	Course over ground in 1/10° increments. 0-359.9 degrees; 3,600 = not available = default; 3,601 – 4095 = reserved.
		SOG	10	Speed over ground. Scale dependent on value of craft flag. Aircraft: 0 – 1000 kts (1 kt increments); 1001 = 1001 kts or higher; 1002 = not available = default; 1003 – 1023 = reserved.
		Operational Status	4	Operational status of the craft reporting. 0 = unknown = default 1 = ops normal 2 = on scene as directed 3 = returning to port/land 4 = awaiting instructions 5 = Bravo at home port 6 = Bravo at port other than home 7 = Charlie, homeport 8 = Charlie, in repair 9-15 reserved.
		Encryption Bit Padding	22	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption. Set to 0.
		Checksum	16	16-bit CRC calculated as per EAIS Specification
Footer		Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
		Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
		Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
		Total bits	224	2 Slot Binary Message

2.26 Static Data Report

DAC**: 366** FI**:** **39** (Encrypted)

Published**: 21 Apr 2017** Version**: 0**

Summary of changes:

Version 0:

This is an RTCM compliant update of the FID 1 message listed in the Oct 2014 EAIS IDD. It also replaces the DAC 366, FI 57 Static Data Report from the same document.

2.26.1 Introduction

The Static Data Message is used to send the equivalent information to AIS Message 5 but removes less essential data to compress message size.

2.26.2 Usage Notes

- The FID 11 static data report shall be transmitted once every 6 minutes.
- The data is matched by MMSI to the corresponding FID 10 message to provide additional information.

2.26.3 Message 26 Format

Encrypted Situation Report (Message 26, Broadcast)

	Parameter	# of Bits	Description
Standard Message Header	Message ID	6	Identifier for Message 26; always 26.
	Repeat Indicator	2	Indicates how many times a message has been repeated. 0 – 3; 0 = default; 3 = do not repeat any more. Set to zero (default).
	Source MMSI	30	MMSI number of source station. Varies according to the transmitter ID.
	Destination Indicator	1	0 = broadcast (no Destination ID field) 1 = Addressed (30 bit Destination ID field). Set to 1 (addressed).
	Binary Data Flag	1	0 = unstructured binary data (no Application Identifier bits used) 1 = binary data coded as defined by the 16-bit AI. Set to 1 (structured).
	Destination ID	0	MMSI number of destination station. Not Used.
	Spare	0	Not used.

Binary Data		Designated Area Code	10	Designated area code (DAC). Set to 366.
		Function Identifier	6	Function identifier. Set to (decimal) 39.
	Encrypted Payload	Version	3	Sequential number used to indicate the message version in steps of 1. 0 = test message = default; 1 – 7 = message version. Set to zero.
		Asset Name	90	Maximum 15 characters 6-bit ASCII as per ITU 1371. "@@@@@@@@@@@@@@@@" = not available = default. The Name should be as shown on the station radio license.
		Asset Type	10	Asset Type as per Appendix 1 of this VDL.
		DTE	1	Data terminal equipment (DTE) ready. 0 = available, 1 = not available = default.
		Encryption Bit Padding	24	Sufficient spare bits to ensure that the binary data is a multiple of 128 bits for block encryption. Set to 0.
		Checksum	16	16-bit CRC calculated as per EAIS Specification
Footer		Spare	4	Four extra bits to ensure the message ends on a byte boundary. Set to zero.
		Communications State Selector	1	0 = SOTDMA communication state follows 1 = ITDMA communication state follows
		Communications State	19	SOTDMA communication state (see ITU 1371-5 § 3.3.7.2.1, Annex 2), if communication state selector flag is set to 0, or ITDMA communication state (§ 3.3.7.3.2, Annex 2), if communication state selector flag is set to 1.
		Total bits	224	2 Slot Binary Message

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

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

1.4.1. 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

1.4.2. 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

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

PUCG,STEDS STEDS 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.

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

1.3.1. 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

1.3.2. 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

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

USCG STEDS Configuration Command/Report — PGN: 065535 hex: FFFF

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.

The PGN is a USCG proprietary destination global fast packet PGN.

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

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

When sent as a query from the Presentation Interface to a device, the Command/Report/Query field must be set to "2" meaning that this is a request or query for the current configuration from a device.

Required Behavior:
When sent on the network as a command(field 6 = 0), the receiving device shall respond with this PGN as report (field 6 = 1), containing all configuration information as a consequence of receiving this PGN. This enables the Presentation Interface sending this PGN as a command to determine success or failure of the intended configuration. When sent as a query (field 6 = 2) to a device, the receiving device shall responsd with this PGN as a report (field 6 = 1), containing all the existing configuration information as a consequence of receiving this PGN.

This PGN shall be sent as a report (Field 6 = 1) in response to either an ISO Request PGN 059904 or Request Group Function PGN 126208.

If a receiving device is unable to properly process the command or query, the response will be sent with field 6 = 6 to indicate an error and the other fields containing all existing information.

Single Frame:	Yes	*Priority Default:*	6	*Default Update Rate:*	milliseconds	*Frequency:*	NA cycles per second
Destination:	Global Pr	*Query Support:*	Required	*Command Support:*	Optional	*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.						

USCG STEDS Configuration Command/Report

PGN: 065535
hex: FFFF

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

4	**USCG PGN ID**	*Byte Field Size:*		*Request Parameter*	Required
		Bit Field Size:	8	*Command Parameter:*	Optional

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 / Query Indicator**	*Byte Field Size:*		*Request Parameter*	Optional
		Bit Field Size:	3	*Command Parameter:*	Optional

DD376 Command / Report / Query

0 = Command
1 = Report
2 = Query
3 – 5 = Reserved
6 = Error
7 = Data not available

DF52 Bit field **bit(n)** *Range:* Variable *Resolution:* 1 Used to construct bit fields

USCG STEDS Configuration Command/Report — PGN: 065535 hex: FFFF

7 Transmit Mode of Operation

Byte Field Size: *Request Parameter* Optional
Bit Field Size: 3 *Command Parameter:* Optional

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* Optional
Bit Field Size: 3 *Command Parameter:* Optional

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* Optional
Bit Field Size: 3 *Command Parameter:* Optional

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

Version 2.001A
Printed: 31-Mar-17 10:43

USCG STEDS Configuration Command/Report
PGN: 065535

USCG STEDS Configuration Command/Report

PGN: 065535
hex: FFFF

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*	Optional
			Bit Field Size:	3	*Command Parameter:*	Optional
	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	**Unit Type**		*Byte Field Size:*		*Request Parameter*	Optional
			Bit Field Size:	10	*Command Parameter:*	Optional
	DD382 Unit Type		0 = Unknown 1 – 299 = Conforms to Unit Types enumerated in Annex 5 of the EAIS Interface Design Description 300 – 1021 = Reserved for future assignments 1022 = Error 1023 = 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 11	*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.					

Version 2.001A
Printed: 31-Mar-17 10:43

USCG STEDS Configuration Command/Report
PGN: 065535

ANNEX 5

The implementation for OTAR in this VDL is based on the guidance contained in the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Special Publication 800-57, Part 3. The recommendations contained in this document apply to all Federal entities, and specify that the Project25 implementation of OTAR shall be the key management protocol used for over-the-air rekeying of digital radios. However, NIST specifies that separate keys must be used for traffic and key encryption and message authentication, and only 3DES and AES may be used. This VDL implements all these requirements, and implements AES for all encryption operations.

Based on the NIST guidance, this VDL is based on the Project25 Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures, TIA-102.AACA-A of September 2014. Specifically, the Data Link Independent methods described in Section 6 of that document, wherein encryption and decryption are conducted at the application layer.

For STEDS, the Radio Station Identifier (RSI) is an OTAR-specific identifier for the encrypting device, regardless of the MMSI used to deliver OTAR data. Individual RSIs can be assigned to a particular presentation interface device, such as an ECDIS or multi-function display. Additionally, an encrypting device can be assigned a Group RSI, to simplify and minimize OTAR traffic.

As part of this IDD, the PI must implement all Project25 RSI functionalities and procedures supported by the OTAR ASMs listed in Annex 2. This involves the necessary user interfaces for all data input, message and function selection. The PI must allow manual entry of keyset and passphrase data.

Appendix 1 - Asset Type List for Encrypted AIS

#	Type	STEDS ABBREVIATION
USCG - CUTTERS		**(max. 5 characters)**
1	USCG 418 WMSL	WMSL
2	Maritime Security Cutter Medium	WMSM
3	USCG 154 WPC	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

#	Type	STEDS ABBREVIATION
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	SPECIAL PURPOSE CRAFT – AIR	SPC-AIR
75	USCG-CB-ATON-L	CB-ATON-L
76	USCG RB-S II	RB-S II
77	SPECIAL PURPOSE CRAFT – BOARDING	SPC-BTD
78	SPECIAL PURPOSE CRAFT – TRAINING	SPC-TB
79	USCG RB-M	RB-M
80	USCG CB-ATON-M	CB-ATON-M
81	SPECIAL PURPOSE CRAFT – SCREENING	SPC-SV
82-99	Reserved for future CG boat types	
USCG - AIRCRAFT		
100	Vertical takeoff Unmanned Aerial Vehicle	VUAV
101	High Altitude Endurance Unmanned Aerial 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	

#	Type	STEDS ABBREVIATION
OTHER GOVERNMENT AGENCIES		
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	
300-1021	Reserved for future use	

Appendix 2 – Search Definitions

2.1 Search Pattern Nomenclature

Commence Search Point (CSP) is the location in the search pattern where the SRU begins searching. Specifying the CSP allows the SRU to efficiently plan the en route track, and ensures that SRUS are separated and that the SRU begins search at the desired point.

Commence Search Time (CST) is the time that the SRU should start execution of the search pattern. Specifying the CST ensures that the SRU begins the search at the desired time.

Search Leg is the long leg along the track of any pattern.

Cross Leg is the connection between two search legs.

Creep is the general direction in which an SRU moves through a rectangular or square area, normally the same direction as the cross legs.

2.2 Search Pattern Designation

A coded system of letters is used to designate search patterns by type. The first letter designates the major pattern characteristic. The second letter denotes SRU number ("S" is a single-unit search; "M" is a multi-unit search). The third letter designates specialized SRU patterns or instructions.

Square Patterns (S) are used to search a small area when some doubt exists about the distress position. They provide more uniform coverage than a sector search and may be expanded. Square searches are referred to as expanding square searches beginning at datum and expanding outward. If datum is a line instead of a point, the pattern may be changed to an expanding rectangle. The first leg is usually directly into the wind or current to minimize navigation errors. A precise pattern, it requires the full attention of the navigator. If two aircraft (the maximum that should be used) are assigned to the same area, they must fly their individual patterns at different altitudes on tracks, which differ by 45°.

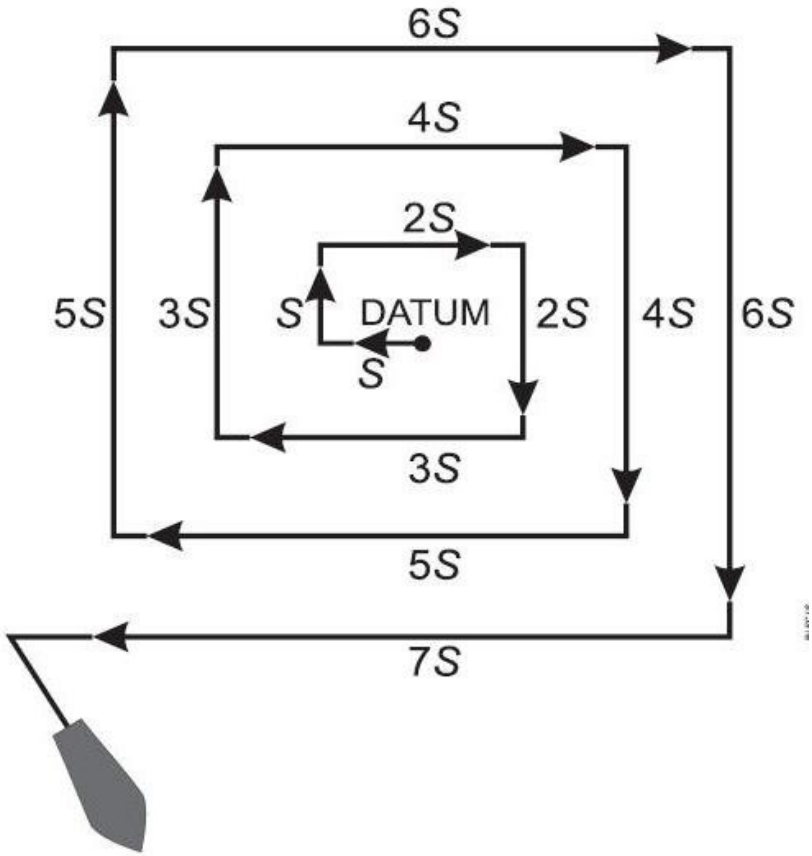

Figure 2: Expanding Square Single Unit (ES) (S = track spacing)

Sector Patterns (V) These patterns may be used when datum is established within close limits, a very high coverage is desired in the immediate vicinity of datum, and the area to be searched is not extensive. The patterns resemble the spokes of a wheel and cover circular search areas. Datum is located at the center of the wheel and should be marked with a suitable floating marker. By marking datum, the SRU has a navigation check each time the SRU passes through the center of the search area. While there are many types of sector search patterns, a six-sector pattern is usually used. It consists of three equilateral triangles with one corner of each triangle at datum.

The search radius is also the length of every leg. This search pattern can be used in both single and multi- unit searches. An average coverage for sector patterns can be determined by using the mid-leg track spacing or, equivalently, twice the sweep width divided by the radius of the pattern. Sector searches have high Probability of Success (POS) near datum assuming the object is in the search area. Generally, aircraft sector search areas do not have a radius greater than 20 to 30 miles, while marine craft use a maximum radius of 5 miles. Because only a small area is covered, datum should be recomputed on every search to allow for drift. If the search is oriented over a marker, adjustment for total water current (TWC) will occur automatically, and only leeway must be considered. For standardization, all turns should be made to the right.

Sector Search Pattern: Single Unit -- Victor Sierra (VS) searches six-sector patterns are most commonly used. See Figure 6. When practical, the first leg of the search is normally in the direction of search object drift. All turns in this pattern are 120° to the right. All legs of the search pattern are equal to the chosen radius. Upon completion of the pattern, a second pattern is started with the heading of the new first leg 30° to the right of the final course of the first pattern.

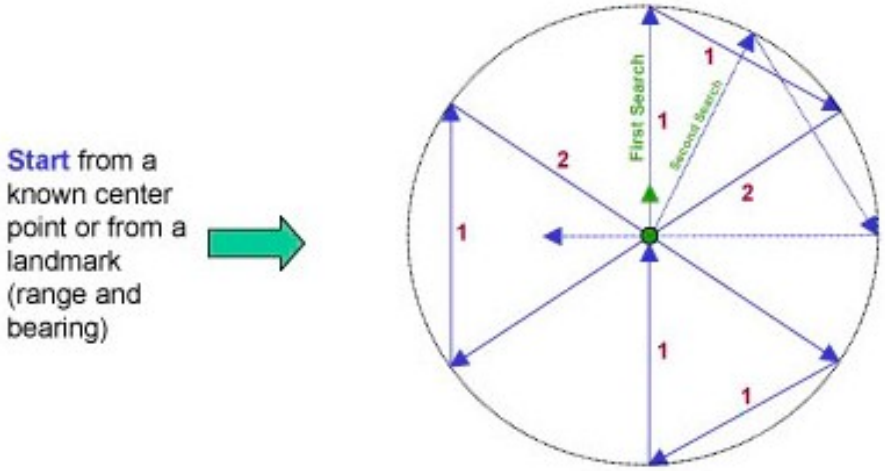

Figure 3: Single Unit Sector Search (VS)

Parallel Patterns (P) are best adapted to rectangular or square areas and have straight search legs that are usually aligned parallel to the major axis. Parallel patterns are normally used for large, fairly level search areas, where only approximate initial position is known, and when uniform cover-age is desired.

Parallel Track Single-Unit (PS) is used by single SRUs for searching rectangular areas and is mostly used by fixed-wing aircraft. Search legs are oriented along the major axis, providing longer legs and fewer turns. See Figure 4.

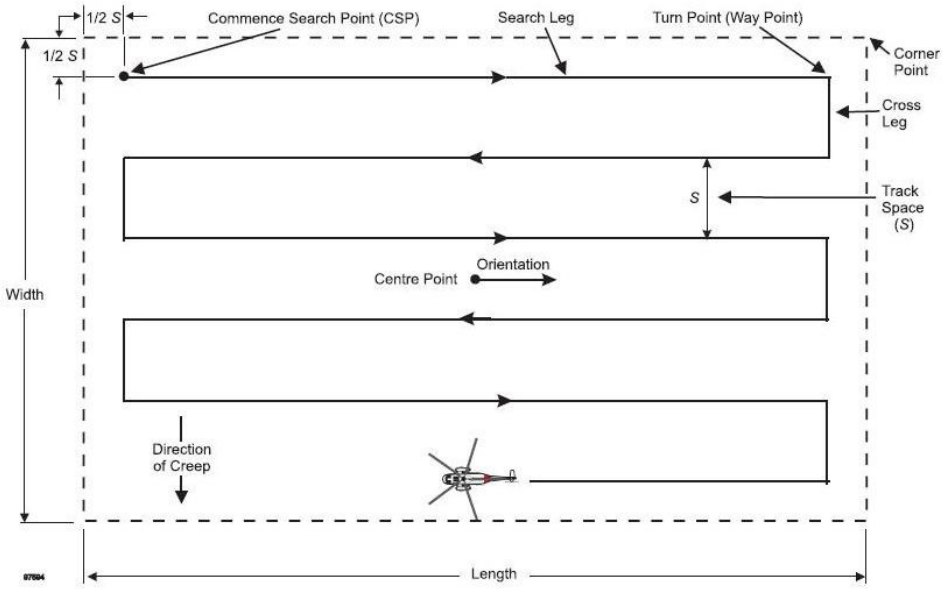

Figure 4: Parallel Track Single Unit (PS)

Creeping Line Patterns (C) are a specialized type of parallel pattern where the direction of creep is along the major axis, unlike the usual parallel (P) pattern. They are used to cover one

end of an area first, or to change direction of the search legs where sun glare or swell direction makes this necessary.

Creeping Line Single-Unit (CS). The CSP is located 1/2 track spacing inside the corner of the search area. See Figure 5.

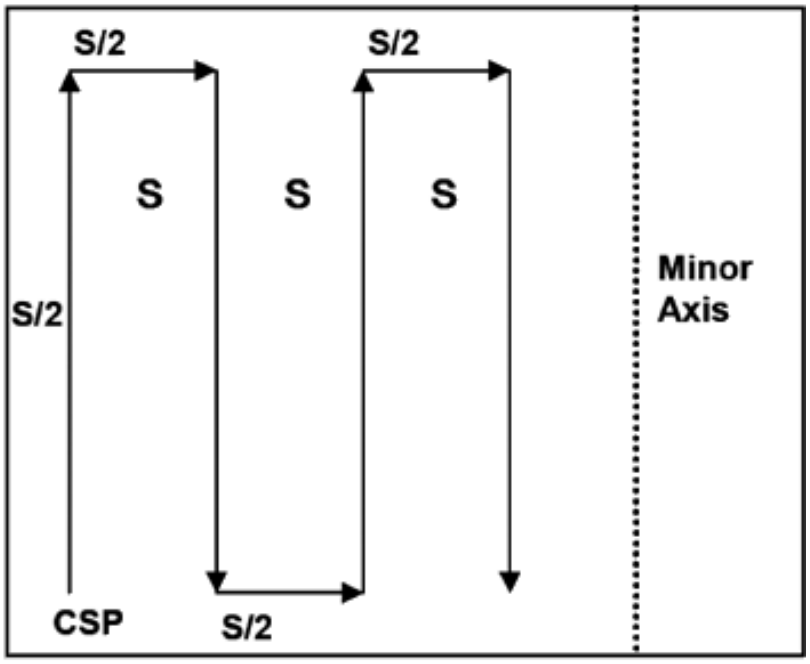

Figure 5: Creeping Line Single Unit (CS)

Trackline Patterns (T) are used when the intended route of the search object is known. A route search is usually the first search action since it is assumed that the target is near track, and that either it will be easily seen or the survivors will signal. The trackline pattern is a rapid and reasonably thorough coverage of the missing craft's proposed track and area immediately adjacent, such as along a datum line.

Trackline Single-Unit Non-Return (TSN) search is made along the track or datum line. The letter "N" in the third position indicates that the pattern makes one or more searches along the track, but the search terminates at the opposite end of track from where it began. See Figure 6.

Trackline Single-Unit Return (TSR) has the CSP offset 1⁄2-search track spacing from the trackline or datum. The SRU runs up one side and down the other, ending one-track space from where it began. See Figure 7.

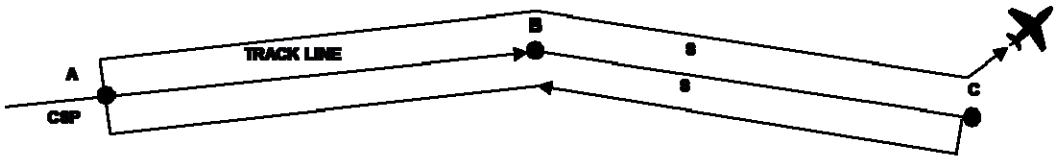

Figure 6: Trackline Single-Unit Non-Return (TSN)

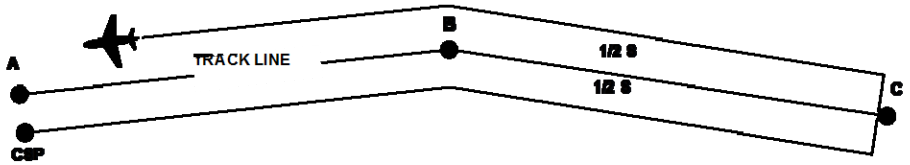

Figure 7: Trackline Single-Unit Return (TSR)

Appendix 3 – Vessel, Aircraft, and Submarine Target Descriptions

Three letter codes correspond to current USCG vessel query sheet, form CG-4100 (Rev 5-15), and the associated Maritime Law Enforcement Academy Job Aid.

#	VESSEL TYPE	
COMMERCIAL FISHING		
1	CLAM DREDGE	FCD
2	CHARTER/PARTY/HEAD BOAT	FCH
3	FACTORY SHIP	FFS
4	GILLNETTER	FGN
5	HARPOONER	FHP
6	LONGLINER	FLL
7	POT OR TRAP BOAT	FPB
8	RESEARCH VESSEL	FRV
9	SCALLOPER	FSC
10	SHRIMPER	FSH
11	SUPPORT SHIP	FSP
12	SEINER SIDE CUTE	FSS
13	SEINER STERN CHUTE	FST
14	TRAWLER SIDE EASTERN	FTE
15	TRAWLER STERN	FTS
16	TRAWLER SIDE WESTERN	FTW
17	TROLLER	FTO
18	WHALER	FWL
19-29	RESERVED FOR FUTURE USE	
POWER (RECREATIONAL)		
30	CABIN CRUISER	PCC
31	SPORT FISHER	PFS
32	HOUSEBOAT	PHB
33	HIGH PERFORMANCE	PHP
34	POWER, OTHER	POO
35	RUNABOUT	PRA
36	YACHT, LUXURY MOTOR	PYM
37	YACHT, TRAWLER TYPE	PYT
38-49	RESERVED FOR FUTURE USE	
SAIL (RECREATIONAL)		
50	CATAMARAN	PSC
51	KETCH	PSK
52	SLOOP	PSL
53	MOTORSAIL	PSM
54	SAIL, OTHER	PSO
55	SCHOONER	PSS
56	TRIMARAN	PST
57-69	RESERVED FOR FUTURE USE	
MERCHANT (COMMERCIAL)		

70	BARGE	MBG
71	FREIGHTER, COASTAL	MFC
72	FREIGHTER, OCEAN GOING	MFO
73	FERRY	MFY
74	LNG CARRIER	MNG
75	OIL CREW BOAT	MOC
76	MERCHANT, OTHER	MOO
77	OIL RIG BOAT	MOR
78	PASSENGER LINE	MPL
79	RESEARCH VESSEL	MRV
80	TUG AND TOW	MTB
81	TANKER, COASTAL	MTC
82	TUG	MTG
83	TANKER, OCEAN GOING	MTO
84-99	RESERVED FOR FUTURE USE	
OTHER		
100-255	RESERVED FOR FUTURE USE	

Appendix 4 – OTAR Primitive Field Descriptions

These data fields are defined by the Project 25 Primitive Field definitions, section 10.3 of TIA-102.AACA-A, September 2014.

4.1 Status

Value (Hex)	Status	Reason
$00	Command was performed	Command was executed successfully
$01	Command not performed	Command could not be performed due to an unspecified reason
$02	Item does not exist	Key / Keyset needed to perform the operation does not exist
$03	Invalid Message ID	Message ID invalid/unsupported
$04	Invalid MAC	MAC is invalid
$05	Out of Memory	Memory unavailable to process the command/message
$06	Could not decrypt the message	KEK does not exist
$07	Invalid Message Number	Message number is invalid
$08	Invalid Key ID	Key ID is invalid or not present
$09	Invalid Algorithm ID	ALGID is invalid or not present
$0A	Invalid MFID	MFID is invalid
$0B	Module Failure	Encryption Hardware failure
$0C	MI all zeros	Received MI was all zeros
$0D	Keyfail	Key identified by ALGID/Key ID is erased
$0E - $FE	Reserved for Future Use	Reserved
$FF	Unknown	Unknown

4.2 RSI

RSI	Value (Decimal)	Value (Hex)
Reserved “No One”	0	$000000
Individual Address	1 – 9,999,998	$000001 - $98967E
Default KMF RSI	9,999,999	$98967F
Group Addresses	10,000,000 – 16,777,214	$989680 - $FFFFFE
Designates Everyone	16,777,215	$FFFFFF

4.3 Time

Time	Hours	5	Hour in 24 hour notation. 0 – 23
	Minutes	6	Minutes of the time. 0 – 59
	Seconds	6	Seconds of the time. 0 – 59
	Spare	7	Not used. Set to zero.

Appendix 5 – Key Name Codes

The Project25 OTAR standard specifies that a key's name may use a series of 8 bit ASCII characters to form a Key Name. This VDL will use this data field to assist with troubleshooting and key administration, as seen below:

Key Name	Function	16	Functional name or purpose of key.
	Month	16	Month identifier, typically of the publish date. (8 bit ASCII) 1-12
	Day	16	Day identifier, typically of the publish date. (8 bit ASCII) 1-31
	Year	16	Year (century agnostic) identifier, typically of the publish date. (8 bit ASCII) 0-99.

The first (most significant) character of the "Function" field represents the key's type and function.

First Character	Key Type
K	Key Encryption Key
T	Traffic Encryption Key
M	MAC Encryption Key
(all others)	Reserved for Future Use

The second (least significant) character of the "Function" field represents the key's organization.

Second Character	Organization
C	US Coast Guard
N	US Navy
O	National Oceanographic & Atmospheric Administration
(all others)	Reserved for Future Use