CONSERVATION MEASURE 10-04 (2005)
Automated satellite-linked Vessel Monitoring Systems (VMS)

Species	all except krill
Area	all
Season	all
Gear	all

The Commission,

Recognising that in order to promote the objectives of the Convention and further improve compliance with the relevant conservation measures,

Convinced that illegal, unreported and unregulated (IUU) fishing compromises the objective of the Convention,

Recalling that Contracting Parties are required to cooperate in taking appropriate action to deter any fishing activities which are not consistent with the objective of the Convention,

Mindful of the rights and obligations of Flag States and Port States to promote the effectiveness of conservation measures,

Wanting to reinforce the conservation measures already adopted by the Commission,

Recognising the obligations and responsibilities of Contracting Parties under the Catch Documentation Scheme for *Dissostichus* spp. (CDS),

Recalling provisions as made under Article XXIV of the Convention,

Committed to take steps, consistent with international law, to identify the origins of *Dissostichus* spp. entering the markets of Contracting Parties and to determine whether *Dissostichus* spp. harvested in the Convention Area that is imported into their territories was caught in a manner consistent with CCAMLR conservation measures,

hereby adopts the following conservation measure in accordance with Article IX of the Convention:

1. Each Contracting Party shall ensure that its fishing vessels, licensed[1] in accordance with Conservation Measure 10-02, are equipped with a satellite-linked vessel monitoring device allowing for the continuous reporting of their position in the Convention Area for the duration of the licence issued by the Flag State. The vessel monitoring device shall automatically communicate at least every four hours to a land-based fisheries monitoring centre (FMC) of the Flag State of the vessel the following data:

   (i) fishing vessel identification;

   (ii) the current geographical position (latitude and longitude) of the vessel, with a position error which shall be less than 500 m, with a confidence interval of 99%; and

   (iii) the date and time (expressed in UTC) of the fixing of the said position of the vessel.

2. The implementation of vessel monitoring device(s) on vessels while participating only in a krill fishery is not currently required.

3. Each Contracting Party as a Flag State shall ensure that the vessel monitoring device(s) on board its vessels are tamper proof, i.e. are of a type and configuration that prevent the input or output of false positions, and that are not capable of being over-ridden, whether manually, electronically or otherwise. To this end, the on-board satellite monitoring device must:

   (i) be located within a sealed unit; and

   (ii) be protected by official seals (or mechanisms) of a type that indicate whether the unit has been accessed or tampered with.

4. In the event that a Contracting Party has information to suspect that an on-board vessel monitoring device does not meet the requirements of paragraph 3, or has been tampered with, it shall immediately notify the Secretariat and the vessel's Flag State.

5. Each Contracting Party shall ensure that its FMC receives Vessel Monitoring System (VMS) reports and messages, and that the FMC is equipped with computer hardware and software enabling automatic data processing and electronic data transmission. Each Contracting Party shall provide for backup and recovery procedures in case of system failures.

6. Masters and owners/licensees of fishing vessels subject to VMS shall ensure that the vessel monitoring device on board their vessels within the Convention Area is at all times fully operational as per paragraph 1, and that the data are transmitted to the Flag State. Masters and owners/licensees shall in particular ensure that:

   (i) VMS reports and messages are not altered in any way;

   (ii) the antennae connected to the satellite monitoring device are not obstructed in any way;

   (iii) the power supply of the satellite monitoring device is not interrupted in any way; and

   (iv) the vessel monitoring device is not removed from the vessel.

7. A vessel monitoring device shall be active within the Convention Area. It may, however, be switched off when the fishing vessel is in port for a period of more than one week, subject to prior notification to the Flag State, and if the Flag State so desires also to the Secretariat, and providing that the first position report generated following the repowering (activating) shows that the fishing vessel has not changed position compared to the last report.

8. In the event of a technical failure or non-functioning of the vessel monitoring device on board the fishing vessel, the master or the owner of the vessel, or their representative, shall communicate to the Flag State every six hours, and if the Flag State so desires also to the Secretariat, starting at the time that the failure or the non-functioning was

detected or notified in accordance with paragraph 12, the up-to-date geographical position of the vessel by electronic means (email, facsimile, telex, telephone message, radio).

9. Vessels with a defective vessel monitoring device shall take immediate steps to have the device repaired or replaced as soon as possible and, in any event, within two months. If the vessel during that time returns to port, it shall not be allowed by the Flag State to commence a further fishing trip in the Convention Area without having the defective device repaired or replaced.

10. When the Flag State has not received for 12 hours data transmissions referred to in paragraphs 1 and 8, or has reasons to doubt the correctness of the data transmissions under paragraphs 1 and 8, it shall as soon as possible notify the master or the owner or the representative thereof. If this situation occurs more than two times within a period of one year in respect of a particular vessel, the Flag State of the vessel shall investigate the matter, including having an authorised official check the device in question, in order to establish whether the equipment has been tampered with. The outcome of this investigation shall be forwarded to the CCAMLR Secretariat within 30 days of its completion.

11.[2,3] Each Contracting Party shall forward VMS reports and messages received, pursuant to paragraph 1, to the CCAMLR Secretariat as soon as possible:

(i) but not later than four hours after receipt for those exploratory longline fisheries subject to conservation measures adopted at CCAMLR-XXIII; or

(ii) but not later than 10 working days following departure from the Convention Area for all other fisheries.

12. With regard to paragraphs 8 and 11(i), each Contracting Party shall, as soon as possible but no later than two working days following detection or notification of technical failure or non-functioning of the vessel monitoring device on board the fishing vessel, forward the geographical positions of the vessel to the Secretariat, or shall ensure that these positions are forwarded to the Secretariat by the master or the owner of the vessel, or their representative.

13. Each Flag State shall ensure that VMS reports and messages transmitted by the Contracting Party or its fishing vessels to the CCAMLR Secretariat, are in a computer-readable form in the data exchange format set out in Annex 10-04/A.

14. Each Flag State shall in addition notify the CCAMLR Secretariat as soon as possible of each entry to, exit from and movement between subareas and divisions of the Convention Area by each of its fishing vessels in the format outlined in Annex 10-04/A.

15. Without prejudice to its responsibilities as a Flag State, if the Contracting Party so desires, it shall ensure that each of its vessels communicates the reports referred to in paragraphs 11 and 14 in parallel to the CCAMLR Secretariat.

16. Each Flag State shall notify the name, address, email, telephone and facsimile numbers, as well as the address of electronic communication of the relevant authorities of their FMC to the CCAMLR Secretariat before 1 January 2005 and thereafter any changes without delay.

17. In the event that the CCAMLR Secretariat has not, for 48 consecutive hours, received the data transmissions referred to in paragraph 11(i), it shall promptly notify the Flag State of the vessel and require an explanation. The CCAMLR Secretariat shall promptly inform the Commission if the data transmissions at issue, or the Flag State explanation, are not received from the Contracting Party within a further five working days.

18. The CCAMLR Secretariat and all Parties receiving data shall treat all VMS reports and messages received under paragraph 11 or paragraphs 19, 20, 21 or 22 in a confidential manner in accordance with the confidentiality rules established by the Commission as contained in Annex 10-04/B. Data from individual vessels shall be used for compliance purposes only, namely for:

    (i) active surveillance presence, and/or inspections by a Contracting Party in a specified CCAMLR subarea or division; or

    (ii) the purposes of verifying the content of a *Dissostichus* Catch Document (DCD).

19. The CCAMLR Secretariat shall place a list of vessels submitting VMS reports and messages pursuant to this conservation measure on a password-protected section of the CCAMLR website. This list shall be divided into subareas and divisions, without indicating the exact positions of vessels, and be updated when a vessel changes subarea or division. The list shall be posted daily by the Secretariat, establishing an electronic archive.

20. VMS reports and messages (including vessel locations), for the purposes of paragraph 18(i) above, may be provided by the Secretariat to a Contracting Party other than the Flag State without the permission of the Flag State only during active surveillance, and/or inspection in accordance with the CCAMLR System of Inspection and subject to the time frames set out in paragraph 11. In this case, the Secretariat shall provide VMS reports and messages, including vessel locations over the previous 10 days, for vessels actually detected during surveillance, and/or inspection by a Contracting Party, and VMS reports and messages (including vessel locations) for all vessels within 100 n miles of that same location. The Flag State(s) concerned shall be provided by the Party conducting the active surveillance, and/or inspection, with a report including name of the vessel or aircraft on active surveillance, and/or inspection under the CCAMLR System of Inspection, and the full name(s) of the CCAMLR inspector(s) and their ID number(s). The Parties conducting the active surveillance, and/or inspection will make every reasonable effort to make this information available to the Flag State(s) as soon as possible.

21. A Party may contact the Secretariat prior to conducting active surveillance, and/or inspection in accordance with the CCAMLR System of Inspection, in a given area and request VMS reports and messages (including vessel locations), for vessels in that area. The Secretariat shall provide this information only with the permission of the Flag State

for each of the vessels and according to the time frames set out in paragraph 11. On receipt of Flag State permission the Secretariat shall provide regular updates of positions to the Contracting Party for the duration of the active surveillance, and/or inspection in accordance with the CCAMLR System of Inspection.

22. A Contracting Party may request actual VMS reports and messages (including vessel locations) from the Secretariat for a vessel when verifying the claims on a DCD. In this case the Secretariat shall provide that data only with Flag State permission.

23. The CCAMLR Secretariat shall annually, before 30 September, report on the implementation of and compliance with this conservation measure to the Commission.

[1] Includes vessels licensed under French domestic law and vessels licensed under South African domestic law.

[2] This paragraph does not apply to vessels licensed under French domestic law in the EEZs surrounding Kerguelen and Crozet Islands.

[3] This paragraph does not apply to vessels licensed under South African domestic law in the EEZ surrounding Prince Edward Islands.

ANNEX 10-04/A

VMS DATA FORMAT
'POSITION', 'EXIT' AND 'ENTRY' REPORTS/MESSAGES

Data element	Field code	Mandatory/ Optional	Remarks
Start record	SR	M	System detail; indicates start of record.
Address	AD	M	Message detail; destination; 'XCA' for CCAMLR.
Sequence number	SQ	M[1]	Message detail; message serial number in current year.
Type of message	TM[2]	M	Message detail; message type, 'POS' as position report/ message to be communicated by VMS or other means by vessels with a defective satellite tracking device.
Radio call sign	RC	M	Vessel registration detail; international radio call sign of the vessel.
Trip number	TN	O	Activity detail; fishing trip serial number in current year.
Vessel name	NA	M	Vessel registration detail; name of the vessel.
Contracting Party internal reference number	IR	O	Vessel registration detail. Unique Contracting Party vessel number as ISO-3 Flag State code followed by number.
External registration number	XR	O	Vessel registration detail; the side number of the vessel.
Latitude	LA	M[3]	Activity detail; position.
Longitude	LO	M[3]	Activity detail; position.
Latitude (decimal)	LT	M[4]	Activity detail; position.
Longitude (decimal)	LG	M[4]	Activity detail; position.
Date	DA	M	Message detail; position date.
Time	TI	M	Message detail; position time in UTC.
End of record	ER	M	System detail; indicates end of the record.

[1] Optional in case of a VMS message.

[2] Type of message shall be 'ENT' for the first VMS message from the Convention Area as detected by the FMC of the Contracting Party, or as directly submitted by the vessel.
Type of message shall be 'EXI' for the first VMS message from outside the Convention Area as detected by the FMC of the Contracting Party or as directly submitted by the vessel, and the values for latitude and longitude are, in this type of message, optional. Type of message shall be 'MAN' for reports communicated by vessels with a defective satellite tracking device.

[3] Mandatory for manual messages.

[4] Mandatory for VMS messages.

ANNEX 10-04/B

PROVISIONS ON SECURE AND CONFIDENTIAL TREATMENT OF ELECTRONIC REPORTS AND MESSAGES TRANSMITTED PURSUANT TO CONSERVATION MEASURE 10-04

1. Field of Application

1.1 The provisions set out below shall apply to all VMS reports and messages transmitted and received pursuant to Conservation Measure 10-04.

2. General Provisions

2.1 The CCAMLR Secretariat and the appropriate authorities of Contracting Parties transmitting and receiving VMS reports and messages shall take all necessary measures to comply with the security and confidentiality provisions set out in sections 3 and 4.

2.2 The CCAMLR Secretariat shall inform all Contracting Parties of the measures taken in the Secretariat to comply with these security and confidentiality provisions.

2.3 The CCAMLR Secretariat shall take all the necessary steps to ensure that the requirements pertaining to the deletion of VMS reports and messages handled by the Secretariat are complied with.

2.4 Each Contracting Party shall guarantee the CCAMLR Secretariat the right to obtain as appropriate, the rectification of reports and messages or the erasure of VMS reports and messages, the processing of which does not comply with the provisions of Conservation Measure 10-04.

3. Provisions on Confidentiality

3.1 All requests for data must be made to the CCAMLR Secretariat in writing. Requests for data must be made by the main Commission Contact or an alternative contact nominated by the main Commission Contact of the Contracting Party concerned. The Secretariat shall only provide data to a secure email address specified at the time of making a request for data.

3.2 In cases where the CCAMLR Secretariat is required to seek the permission of the Flag State before releasing VMS reports and messages to another Party, the Flag State shall respond to the Secretariat as soon as possible but in any case within two working days.

3.3 Where the Flag State chooses not to give permission for the release of VMS reports and messages, the Flag State shall, in each instance, provide a written report within 10 working days to the Commission outlining the reasons why it chooses not to permit data to be released. The CCAMLR Secretariat shall place any report so provided, or notice that no report was received, on a password-protected part of the CCAMLR website.

3.4 VMS reports and messages shall only be released and used for the purposes stipulated in paragraph 18 of Conservation Measure 10-04.

3.5 VMS reports and messages released pursuant to paragraphs 20, 21 and 22 of Conservation Measure 10-04 shall provide details of: name of vessel, date and time of position report, and latitude and longitude position at time of report.

3.6 Regarding paragraph 21 each inspecting Contracting Party shall make available VMS reports and messages and positions derived therefrom only to their inspectors designated under the CCAMLR System of Inspection. VMS reports and messages shall be transmitted to their inspectors no more than 48 hours prior to entry into the CCAMLR, subarea or division where surveillance is to be conducted by the Contracting Party. Contracting Parties must ensure that VMS reports and messages are kept confidential by such inspectors.

3.7 The CCAMLR Secretariat shall delete all the original VMS reports and messages referred to in section 1 from the database at the CCAMLR Secretariat by the end of the first calendar month following the third year in which the VMS reports and messages have originated. Thereafter the information related to the movement of the fishing vessels shall only be retained by the CCAMLR Secretariat after measures have been taken to ensure that the identity of the individual vessels can no longer be established.

3.8 Contracting Parties may retain and store VMS reports and messages provided by the Secretariat for the purposes of active surveillance presence, and/or inspections, until 24 hours after the vessels to which the reports and messages pertain have departed from the CCAMLR subarea or division. Departure is deemed to have been effected six hours after the transmission of the intention to exit from the CCAMLR subarea or division.

4. Provisions on Security

4.1 Overview

4.1.1 Contracting Parties and the CCAMLR Secretariat shall ensure the secure treatment of VMS reports and messages in their respective electronic data processing facilities, in particular where the processing involves transmission over a network. Contracting Parties and the CCAMLR Secretariat must implement appropriate technical and organisational measures to protect reports and messages against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all inappropriate forms of processing.

4.1.2 The following security issues must be addressed from the outset:

- System access control:
  The system has to withstand a break-in attempt from unauthorised persons.

- Authenticity and data access control:
  The system has to be able to limit the access of authorised parties to a predefined set of data only.

- Communication security:
  It shall be guaranteed that VMS reports and messages are securely communicated.

- Data security:
  It has to be guaranteed that all VMS reports and messages that enter the system are securely stored for the required time and that they will not be tampered with.

- Security procedures:
  Security procedures shall be designed addressing access to the system (both hardware and software), system administration and maintenance, backup and general usage of the system.

4.1.3 Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing of the reports and the messages.

4.1.4 Security measures are described in more detail in the following paragraphs.

4.2 System Access Control

4.2.1 The following features are the mandatory requirements for the VMS installation located at the CCAMLR Data Centre:

- A stringent password and authentication system: each user of the system is assigned a unique user identification and associated password. Each time the user logs on to the system he/she has to provide the correct password. Even when successfully logged on the user only has access to those and only those functions and data that he/she is configured to have access to. Only a privileged user has access to all the data.

- Physical access to the computer system is controlled.

- Auditing: selective recording of events for analysis and detection of security breaches.

- Time-based access control: access to the system can be specified in terms of times-of-day and days-of-week that each user is allowed to log on to the system.

- Terminal access control: specifying for each workstation which users are allowed to access.

4.3 Authenticity and Data Access Security

4.3.1 Communication between Contracting Parties and the CCAMLR Secretariat for the purpose of Conservation Measure 10-04 shall use secure Internet protocols SSL, DES or verified certificates obtained from the CCAMLR Secretariat.

4.4 Data Security

4.4.1 Access limitation to the data shall be secured via a flexible user identification and password mechanism. Each user shall be given access only to the data necessary for their task.

4.5 Security Procedures

4.5.1 Each Contracting Party and the CCAMLR Secretariat shall nominate a security system administrator. The security system administrator shall review the log files generated by the software for which they are responsible, properly maintain the system security for which they are responsible, restrict access to the system for which they are responsible as deemed needed and in the case of Contracting Parties, also act as a liaison with the Secretariat in order to solve security matters.