a) planning for active surveillance operations and/or inspections at sea;
b) active surveillance operations and/or inspections at sea;
c) supporting search and rescue activities undertaken by a competent Maritime Rescue Coordination Centre (MRCC) subject to the terms of an Arrangement between the Secretariat and the competent MRCC.

24. For the purpose of implementing Paragraph 23 a) and b):

a) Inspections at sea will be undertaken solely by SPRFMO Members in accordance with CMM 11-2015;
b) each Member or CNCP as applicable shall only make available such VMS data to their authorised inspectors, and any other government officials for whom it is deemed necessary to access the data;
c) VMS data shall be transmitted by the VMS Point of Contact of the Member or CNCP as applicable to the inspectors and government officials in charge of the operations referred to in paragraph 23 a) and b);
d) Members and CNCPs as applicable shall ensure that such inspectors and government officials keep the data confidential and only use the data for the purposes described in paragraph 23 a) and b);
e) Members may retain VMS data provided by the Secretariat for the purposes described in paragraph 23 a) and b) until 24 hours after the vessels to which the VMS data pertain have departed from the SPRFMO Convention Area. Except in the circumstances outlined in paragraph 24 f), Members shall submit a written confirmation of the deletion of the VMS data immediately after the 24 hours' period;
f) Members and CNCPs' authorised inspectors and government officials authorities may retain VMS data provided by the Secretariat for the purposes described in paragraph 23 a) and b) for longer than the periods specified in paragraph 24 e) only if it is part of an investigation, judicial or administrative proceeding of an alleged violation of the provisions of the Convention, any conservation and management measures or decisions adopted by the Commission, or domestic laws and regulations. Members shall inform the Secretariat of the purposes and expected timing of the additional period of data retention.

25. For the purpose of paragraph 23 a), Members requesting VMS data shall provide the Secretariat the geographic area of the planned surveillance and/or inspection activity. In this case, Members and CNCPs authorised inspectors and government officials shall advise the Secretariat at least 48 hours in advance of the commencement of MCS activities in the notified geographic area of the high seas areas of the Convention Area. In the event that the MCS activities will no longer take place or if the notified geographic area of the high seas has changed, the Secretariat will be notified at least 48 hours in advance.

26. For the purpose of paragraph 23 b), the Secretariat shall provide VMS data from the previous ten days, for vessel detected during surveillance, and/or inspection activity, and contemporaneous VMS data for all vessels within approximately 100nm[2] of the surveillance and/or inspection activity location. Members conducting the active surveillance and/or inspection activity shall provide the Secretariat with a report including the name of the vessel or aircraft on active surveillance and/or inspection activity. This information shall be made available without undue delay after the surveillance and/or inspection activities are complete.

27. For the purpose of paragraph 23 c), upon the request of a Member or CNCP, the Secretariat shall provide VMS data without the permission of the flag Member or CNCP for the purposes of supporting search and rescue activities undertaken by a competent Maritime Rescue Coordination Centre (MRCC) subject to the terms of an arrangement between the Secretariat

[2] The Secretariat and/or VMS provider will shape these temporary patrol zone boundaries to the nearest longitude and latitude degree intersections practical for implementing this requirement.

and the competent MRCC. The Member or CNCP requesting the information shall ensure that the data will only be used only for the purposes described in this paragraph.

28. Paragraphs 23 to 27 shall be reviewed by the Commission when the Commission adopts a specific SPRFMO high seas inspection regime.

REVIEW

29. At each annual meeting of the Commission, the Secretariat shall provide the Commission with a report on the implementation and operation of the Commission VMS.

30. The Commission shall conduct a review of the implementation of the Commission VMS at its annual meeting in 2019 and shall consider its efficiency and effectiveness and consider further improvements to the system as required.

FINAL PROVISIONS

31. Section 3 on Vessel Monitoring System data of CMM 02-2017 is deleted.

Formatted: Indent: Left: 0.63 cm, Space Before: 0 pt, After: 0 pt, No bullets or numbering

Formatted: Space Before: 0 pt, After: 0 pt

Annex 1

Minimum Standards for Automatic Location Communicators (ALCs) used in the Commission Vessel Monitoring System

1. The ALC shall continuously, automatically and independently of any intervention by the vessel communicate the following data when operating in the area defined in paragraph 2 of this CMM with at least the level of accuracy specified at paragraph 7 of this Annex and obtained by a satellite-based positioning system:

Category	Data Element	Remarks
Vessel registration	Static unique vessel identifier	For example, country code followed by national vessel registration number
Activity detail	Latitude	Position latitude
Activity detail	Longitude	Position longitude
Message detail	Date	Position date in UTC
Message detail	Time	Position time in UTC

2. ALCs fitted to fishing vessels must be capable of transmitting data at least every 15 minutes.
3. The flag Member or CNCP shall ensure that its FMC receives VMS positions at least with the frequency adopted according to this CMM and shall be able to request the VMS information at a higher frequency.
4. The flag Member or CNCP shall maintain a record of all vessel position information reported while these vessels are operational in the Convention Area, such that this information may be used to document vessel activity in the Convention Area, and to validate fishing position information provided by those vessels.
5. Under normal satellite navigation operating conditions, positions derived from the data forwarded must be accurate to within 100 metres.
6. The ALC and/or forwarding service provider must be able to support the ability for data to be sent to multiple independent destinations.
7. Members and CNCPs shall ensure that VMS position reports are reported by each of their vessels:

    1. at least once every two hours if fishing using benthic or bentho-pelagic trawling[3] or if operating within 20 nm of an EEZ boundary;

    2. at least once every four hours in other circumstances[4];

[3] Bentho-pelagic trawling is interpreted here to mean trawling with a mid-water net where the net has a likelihood of coming into contact with the seabed at any time during the trawling operation.
[4] As at February 2013 China has advised that it is not able to report more frequently than twice daily according to domestic regulation.

Deleted: on

Deleted: :¶
<#>ALC static unique identifier;¶

Deleted: current geographical position (latitude and longitude) of the vessel; ¶
the date and time (expressed in Coordinated Universal Time [UTC]) corresponding to the position of the vessel

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Deleted: 1 b); ¶
The data referred to in paragraphs 1 b) and c) shall be

Deleted: from

Deleted: .

Formatted: Indent: Left: 1.27 cm, No bullets or numbering

Deleted: <#>The data referred to in paragraph 1 shall be received by the Commission within an interval determined by the Commission.¶
<#>ALCs fitted to fishing vessels must be protected so as to preserve the security and integrity of data referred to in paragraph 1.¶

Moved down [1]: <#>Storage of information within the ALC must be safe, secure and integrated under normal operating conditions.

Formatted: Font color: Black

Deleted: <#> ¶

Deleted: State

Deleted: <#>It shall be prohibited to destroy, damage, render inoperative or otherwise interfere with the ALC unless the competent authorities of the Flag State have authorised its repair or replacement.¶

Moved down [2]: <#>Any features built into the ALC or terminal software to assist with servicing shall not allow unauthorised access to any areas of the ALC that could potentially compromise the operation of the VMS.

Formatted: Font color: Black

Deleted: <#> ¶

Moved down [3]: <#>All ALCs shall be installed on vessels in accordance with their manufacturer's specifications and applicable standards.¶

Formatted: Font color: Black, English (United States)

Formatted: Font: 11 pt, Font color: Black, English (United States)

Deleted: square

Moved down [4]: <#>The satellite navigation decoder and transmitter shall be fully integrated and housed in the same tamper-proof physical enclosure.

Formatted: Font color: Black

Deleted: <#>¶

Annex 2

Security and Confidentiality Requirements

SECURITY PROVISIONS APPLICABLE TO ALL MEMBERS, CNCPS AND THE SECRETARIAT

1. The provisions of this Annex shall apply to all VMS data received pursuant to this CMM.
2. VMS data shall be treated as confidential information.
3. All Members, CNCPs, the Secretariat and the Commission's VMS provider shall ensure the secure treatment of VMS data in their respective electronic data processing facilities, in particular where the processing involves transmission over a network.
4. All Members, CNCPs and the Secretariat shall 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. The following features shall be mandatory:
    a) System access control: the system has to withstand a break-in attempt from unauthorised persons.
    b) Authenticity and data access control: the system has to be able to limit the access of authorised parties to only the data necessary for their task, via a flexible user identification and password mechanism.
    c) VMS data must be securely communicated: communication between Members, CNCPs and the Secretariat or the VMS provider for the purpose of CMM 06-2017 shall use secure Internet protocols SSL, DES or verified certificates obtained from the Secretariat.
    d) Data security: all VMS data that enter the system must be securely stored for the required time, and shall not be tampered with.
    e) The Secretariat shall design security procedures to address access to the system (both hardware and software), system administration and maintenance, backup and general usage of the system for consideration by the Commission.
5. Each Member, CNCP and the 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 Members or CNCPs, also act as a liaison with the Secretariat in order to solve security matters.
6. Members and CNCP as applicable shall submit a written confirmation of the deletion of the VMS data in accordance with this CMM. The Secretariat shall take all the necessary steps to ensure that the requirements pertaining to the deletion of VMS data handled by the Secretariat are complied with.
7. Each Member and CNCP shall designate a primary and secondary Point of Contact for the purposes of any communication regarding the VMS system ("VMS Point of Contact"). It shall transmit the name of the individual or office holder, email and any other contact information for its Points of Contact to the SPRFMO Executive Secretary no later than 180 days after the conclusion of the annual Commission meeting in 2017. Any subsequent changes to the contact information shall be notified to the SPRFMO Executive Secretary within 21 days after such changes take effect. The SPRFMO Executive Secretary shall promptly notify Members and CNCPs of any such changes.
8. The SPRFMO Executive Secretary shall establish and maintain a register of Points of Contact based on the information submitted by the Members and CNCPs. The register and any subsequent changes shall be published promptly on the 'Members only' area of the SPRFMO website.
9. The Secretariat shall inform all Members and CNCPs of the measures taken by the Secretariat to comply with these security and confidentiality requirement provisions at the annual meeting following the establishment of the Commission VMS. Such measures shall ensure a level of security appropriate to the risks represented by the processing of VMS data.

Deleted: ¶

Deleted: set out below

Deleted: CMM 06-2017 (Commission VMS).

Deleted: from vessels operating within the SPRFMO Convention Area

Deleted: Secretariat[1]

Deleted: (

Deleted:).

Deleted: only

ADDITIONAL SECRETARIAT SECURITY STANDARDS FOR THE USE OF THE COMMISSION VMS

10. The following features are the mandatory requirements for the Secretariat's staff use of the Commission VMS:

    a. Staff will be provided with only the keys, passwords and combinations required for them to undertake their direct work functions.
    b. A key register is maintained by the Executive Secretary as well as secure storage of spare keys.
    c. Staff are responsible for the integrity of their workplace security and common entry and exit doors. Office doors shall be locked after hours when staff are away from their workplaces as well as windows. Doors other than the main entry door should be locked when not in immediate use.
    d. Staff are to check their rooms and the premises as they leave the main office or any of the other buildings to ensure all windows and doors are properly secured. Special checks at the end of each work day will be undertaken by the Executive Secretary.
    e. Keys, passwords and combinations are to be kept secure.
    f. Visitors to the SPRFMO Secretariat are required to register upon access to the premises and be issued with a visitor's tag. Visitors, including family members are not to be permitted to move around the building unescorted.
    g. Each staff user shall be assigned an 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 staff user shall only have access to those functions and data that he/she is configured to have access to.
    h. System security issues/events must be auditable by a third party at any time at the request of the Commission.
    i. The Secretariat should develop an administrative procedure for the purposes of implementing these requirements.

11. The Secretariat, in consultation with the CTC Chair, shall develop internal electronic data and communication security procedures at the latest one month after the date established in paragraph 1 of this CMM based on the following key guidelines:

    a. Establishing adequate disaster recovery plan and procedures.
    b. Prevention of network compromise:
        i. Only authorized staff at the Secretariat have access to the corporate network with 'strong password' policy in place.
        ii. All corporate servers protected by proven firewall, antivirus and anti-spam solutions with real-time update policies activated. All network devices protected by anti-virus with live electronic updates.
        iii. Logs of key software updates, mail protection (anti-spam), anti-virus, Internet and network events, together with special event alert monitors allow administrators to address any problem issues before they happen.
        iv. Appropriate service level agreements (SLAs) are in place for outsourced support of critical systems and applications or otherwise foreseen in the contract with the Secretariat's IT service providers.
    c. Prevention of data compromise:
        i. Procedures to define 'acceptable mobile device for SPRFMO use' and restriction.
        ii. Automated procedures to keep all approved software 'up-to-date'.
        iii. Staff training on prevention of data compromise.
    d. Prevention of data loss:
        i. An enterprise backup and recovery solution is in place with full backups of business data run daily, Monday to Friday, and stored offsite.

Deleted: <#>All requests for VMS data must be made to the Secretariat by electronic means. Requests for VMS data must be made by a VMS Point of Contact, or an alternative contact nominated by the VMS Point of Contact. The Secretariat shall only provide VMS data to a requesting Member or CNCP where the VMS data relates to vessels flagged to other Members or CNCPs and all relevant Members and CNCPs have provided written consent through their VMS Point of Contacts for the data to be shared. The Secretariat shall only provide VMS data where it will be downloaded from a secure server by the relevant VMS Point of Contact.¶
<#>The Commission VMS shall have the following security features as a minimum: ¶
<#>The system shall be able to withstand a break-in attempt from unauthorised persons. ¶
<#>The system shall be capable of limiting the access of authorised persons to a predefined set of data only. ¶
<#>The system shall be capable of ensuring that VMS data are securely communicated and that all VMS data that enter the system are securely stored for the required time and that they will not be tampered with.¶
<#>Security procedures shall be designed addressing access to the system (both hardware and software).¶
Page Break
¶

Deleted: a

Deleted: has

Deleted: those and only

Deleted: Executive Secretary

Deleted: a process for authorising users who are not Secretariat

Deleted: , to be reviewed by the Commission at its 2018 meeting.

Formatted: Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Right + Aligned at: 3.17 cm + Indent at: 3.81 cm

ii. Staff training on storage of important business data in public folders or shared folders which get backed up.

12. Submission of VMS data for the purpose of this CMM shall use cryptographic protocols to ensure secure communications.

13. The Security System Administrator of the Secretariat shall review the log files generated by the software, properly maintain the system security, and restrict access to the system as deemed necessary. The Security System Administrator shall also act as a liaison between the VMS Point of Contact and the Secretariat in order to resolve security matters.

Deleted: CMM 06-2017 (Commission VMS)

Deleted: The Secretariat shall nominate a Security System Administrator.

Formatted: Font: Not Bold, Font color: Custom Color(RGB(0,51,204))

Formatted: Normal (Web), Space Before: 0.5 line, After: 0.5 line

Deleted: . ¶
¶
...

Annex 3

SPRFMO Rules on the manual reporting in the SPRFMO Convention Area.

1. In the event of non-reception of four consecutive, programmed VMS positions, and where the Secretariat has exhausted all reasonable steps[1] to re-establish normal automatic reception of VMS positions, the Secretariat shall notify the Member or CNCP whose flag the vessel is flying. That Member or CNCP shall immediately direct the vessel Master to begin manual reporting.
2. In accordance with the chosen means of reporting for VMS data of paragraph 10 of this CMM, the manual report shall be sent by the vessel to the Secretariat via their flag State's FMC, or simultaneously to both the Secretariat and its FMC as applicable.
3. Following the receipt of a direction from a Member or CNCP in accordance with paragraph 1 of this Annex, the vessel Master shall ensure the vessel manually reports its position every 4 hours. If automatic reporting to the SPRFMO VMS has not been re-established within 60 days of the commencement of manual reporting that Member or CNCP shall order the vessel to cease fishing, stow all fishing gear and return immediately to port in order to undertake repairs.
4. The vessel may recommence fishing in the SPRFMO Convention Area only when the ALC has been confirmed as operational by the Secretariat. Four consecutive, programmed VMS positions must have been received by the Secretariat to confirm that the ALC/MTU is fully operational.
5. The format for manual reports to be used is as below. Vessels are encouraged to use email as the primary means of communication and shall send these messages to vms@sprfmo.int.
6. The standard format for manual position reporting in the event of ALC malfunction or failure shall be as follows:

   a) IMO number (if applicable)
   b) International Radio Call Sign
   c) Vessel Name
   d) Vessel Master's name
   e) Position Date (UTC)
   f) Position Time (UTC)
   g) Latitude (with at least the level of accuracy specified at paragraph 7 of Annex 1)
   h) Longitude (with at least the level of accuracy specified at paragraph 7 of Annex 1))
   i) Activity (Fishing/Transit/Transhipping)

7. Members and CNCPs are encouraged to carry more than one ALC when operating in the SPRFMO Convention Area in order to avoid the need to manually report if the primary ALC fails.
8. The Secretariat shall publicise vessels that are reporting in accordance with this Annex 0n the SPRFMO Website.

Deleted: then

Deleted: The

Deleted: either

Deleted: Fisheries Monitoring Centre (

Deleted:)

Deleted: directly

Deleted: .

Deleted: decimal degrees, to

Deleted: nearest 0.01 degrees)

Deleted: decimal degrees, to

Formatted: English (United States)

Deleted: nearest 0.01 degrees

Deleted: also

Deleted:

Annex 4

Minimum Standards to prevent tampering with ALC Units Automatic Location Communicators (ALCs)

[1] The Member or CNCP, in coordination with the Secretariat and through communication with the vessel master as appropriate, will endeavour to re-establish normal automatic reception of VMS positions. If such efforts reveal that the vessel is successfully reporting to the Member or CNCP's VMS (indicating that the vessel's ALC hardware is functional), the Secretariat, in coordination with the Member or CNCP will take additional steps to re-establish automatic reporting to the Commission VMS.

1. ALCs fitted to fishing vessels must be protected so as to preserve the security and integrity of data referred to in paragraph 1 of Annex 1 in accordance to the provisions of this Annex.
2. ALCs must be of a type and configuration that prevent the input or output of false positions, are not capable of being over-ridden, whether manually, electronically or otherwise and are capable of detecting and transmitting satellite alerts in the case of a tampering event.
3. It must not be reasonably possible for anyone, other than the Fisheries Monitoring Centre (FMC), to alter any of the VMS data stored in the ALC, including the frequency of position reporting to the FMC.
4. Storage of information within the ALC must be safe, secure and integrated under normal operating conditions.
5. Any features built into the ALC or terminal software to assist with servicing shall not allow unauthorised access to any areas of the ALC that could potentially compromise the operation of the VMS.
6. The satellite navigation decoder and transmitter shall be fully integrated and housed in the same tamper-proof physical enclosure.
7. In the case that the antenna is mounted separately from the physical enclosure, a single common antenna shall be used for both satellite navigation decoder and transmitter, and the physical enclosure shall be connected using a single length of unbroken cable to the antenna.
8. All ALCs shall be installed on vessels in accordance with their manufacturer's specifications and applicable standards.

Moved (insertion) [1]
Formatted: Font color: Black
Moved (insertion) [2]
Formatted: Font color: Black
Moved (insertion) [4]
Formatted: Font color: Black
Moved (insertion) [3]
Formatted: Font color: Black
Formatted: Normal, Space Before: 0 pt, After: 5.8 pt, Line spacing: Exactly 12.25 pt, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.27 cm, No widow/orphan control, Tab stops: 1.29 cm, Left
Formatted: Font: 11 pt, Font color: Black

Annex 5

Process for the use and release of VMS DATA

1. A Member or CNCP seeking access to Commission VMS data for the purposes outlined in paragraphs 21 to 27 of this CMM shall forward a request to the Secretariat, through its VMS Point(s) of Contact, indicating the purpose(s) for which the data is sought and the time

period covered by the VMS data. The request shall indicate the commitment from the Member or CNCP to respect the Security and Confidentiality requirements of Annex 2 of this CMM as applicable. The request must be submitted at least 5 working days in advance of the intended use except for the purposes of paragraph 23 of this CMM.

Use and release of VMS data requiring the permission of the flag Member or CNCP

2. For the purposes of paragraphs 21 and 22 of this CMM, the Secretariat shall immediately forward the request to the relevant VMS Point(s) of Contact from whom access to VMS data is requested. The release of the VMS data to the requesting Member or CNCP shall only be permitted with approval from the Member or CNCP which owns the VMS data. A Member or CNCP who refuses the request for VMS shall send the reasons for the refusal in writing to the Executive Secretary within 15 days of the communication of the request by the Executive Secretary.
3. Members and CNPCs may permit full or restricted access to their VMS data in accordance with paragraph 8 of this Annex and within the capacity of the Secretariat (and their contracted VMS provider) to provide it, and without prejudice to any additional restrictions specified by Members or CNCPs in respect of their VMS data.
4. Members or CNCPs shall only use the VMS data for the purposes indicated in the request and which are agreed by the other Member or CNCP and shall not disclose the data in full or in part to any third party. Any additional restrictions for VMS data access established by Members or CNCPs in accordance with paragraph 3 of this Annex shall also be complied with.

Use and release of VMS data without the permission of the flag Member or CNCP

5. For the purposes of paragraph 23 to 27 of this CMM, upon receipt of a request for VMS data, the Secretariat shall immediately inform the VMS Points of Contact for which access to VMS data has been requested:
    a. the requesting Member or CNCP;
    b. The date the request was made to the Secretariat
    c. the proposed purpose(s) for the use of that VMS data
    d. the anticipated length of time that the VMS data will be required.

6. In accordance with paragraph 24 f), in the event of retention of the VMS data for longer periods than specified in the request, the Secretariat shall immediately inform the relevant VMS Points of Contact of the purposes of the retention and its expected timing.
7. The Secretariat shall immediately notify the relevant VMS Points of Contact when the requesting Member or CNCPs has ceased their use of that VMS data.

Restrictions

8. Member or CNCP access to the Commission VMS data can be provided without restrictions or subject to certain restrictions regarding, *inter alia*, data availability:

    a) Fleet restriction: data limited to certain fleets defined by flag;
    b) Geographical restriction: data limited to defined geographic area;
    c) Time restriction: data limited to defined time periods.

Formatted: English (New Zealand)