



North Pacific Fisheries Commission

CMM 2023-12

(Entered into force 26 July 2023)

**CONSERVATION AND MANAGEMENT MEASURE
ON THE VESSEL MONITORING SYSTEM (VMS)**

The North Pacific Fisheries Commission (NPFC),

Recalling Article 2 of the Convention on the Conservation and Management of High Seas Fisheries resources in the North Pacific Ocean (Convention), the long-term conservation and sustainable use of the fisheries resources in the Convention Area while protecting the marine ecosystems of the North Pacific Ocean in which these resources occur.

Recognizing Article 7, paragraph 2 (e) of the Convention regarding the development of standards, specifications and procedures for Members of the Commission to report movements and activities using real-time satellite position-fixing transmitters for vessels engaged in fishing activities in the Convention Area and, in accordance with those procedures, coordinate timely dissemination of data collected from Members' satellite vessel monitoring systems,

Reaffirming that Article 13, paragraph 1 of the Convention that Members of the Commission or Cooperating Non-Contracting Parties (CNCPS) shall take necessary measures to ensure that fishing vessels entitled to fly their flag operating in the Convention Area comply with the provisions of the Convention and measures adopted pursuant to the Convention and such vessels do not engage in any activities that undermine the effectiveness of such measures and do not conduct unauthorized fishing activities within areas under national jurisdiction of another State adjacent to the Convention Area,

Determined to ensure effective monitoring, control and surveillance (MCS) and to address the challenge of illegal, unreported and unregulated (IUU) fishing in the Convention Area,

Adopts the following conservation and management measure (CMM) in accordance with Article 7 of the Convention:

Definitions

1. For the purpose of this CMM, the following definitions apply:

- (a) "Convention" means the Convention on the Conservation and Management of High Seas Fisheries resources in the North Pacific Ocean.

- (b) “Convention Area” means the area of the high seas areas of the North Pacific Ocean as specified in Article 4 of the Convention.
- (c) “Commission” means the North Pacific Fisheries Commission (NPFC) established under Article 5 of the Convention.
- (d) “Fishing activities” means the activities established under Article 1 (i) of the Convention.
- (e) “Fisheries monitoring center (FMC)” means the authorized authority or agency of a Member or CNCP responsible for managing VMS for its flagged fishing vessels.
- (f) “Fishing vessels” means any vessel described under Article 1 (j) of the Convention.
- (g) “Inspection Presence in the Convention Area” means the Member is authorized by the High Seas Boarding Inspection Procedure to conduct inspections and is planning for or actively engaged in surveillance in the Convention Area.
- (h) “Manually report” means the transmission via any alternative means of the date/time, current geographical position (latitude and longitude) when an MTU fails to transmit VMS data.
- (i) “Mobile transmitting unit (MTU)” means a satellite communication device capable of receiving and transmitting VMS data.
- (j) “VMS” means a satellite-based monitoring system that transmits VMS data from MTUs on fishing vessels to FMCs.
- (k) “VMS data” means data transmitted by an MTU including:
 - (i) MTU unique identifier;
 - (ii) the current geographical position (latitude and longitude) of the vessel (accurate to within 100m); and,
 - (iii) the date and time (expressed in Coordinated Universal Time (UTC)) of the fixing of the position of the vessel in paragraph 1(k)(ii).

Purpose

2. The VMS supports the Convention’s objective to ensure the long-term conservation and sustainable use of the fisheries resources in the Convention Area. The VMS forms an important part of the Commission’s MCS regime to ensure compliance with, and enforcement of, the provisions of the Convention and CMMs. The purpose of the VMS is to continuously monitor

the positions and movements of all fishing vessels in the Convention Area for compliance purposes. VMS data may also be used to support scientific processes as agreed by the Commission.

Application

3. The VMS applies to all authorized NPFC vessels in the Convention Area.
4. A Member or CNCP may request that waters under their jurisdiction be also covered by the VMS. This request shall be provided to the Commission for their consideration and approval.

Mobile Transmitting Units (MTUs)

5. Each Member or CNCP shall ensure that its vessels authorized pursuant to the relevant CMM for Vessel Registration under NPFC in the Convention Area are equipped with an MTU that complies with the guidance on minimum standards for MTUs contained in Annex 1.
6. Each Member or CNCP shall ensure that MTUs are installed on their flagged fishing vessels in the Convention Area in accordance with relevant domestic legal obligations, procedures and conditions.

VMS Data Transmission Requirements

7. Each Member or CNCP shall ensure its authorized NPFC vessels provide accurate VMS data to the Secretariat via its FMC, in accordance with this CMM.
8. All Members or CNCPs shall ensure that its flagged vessels that are authorized under NPFC and present in the Convention Area transmit VMS data every hour to their FMC.
9. A Member or CNCP may require its fishing vessels to transmit VMS data directly to the Secretariat.
10. Each Member or CNCP shall ensure that their FMC automatically transmits VMS data to the Secretariat, which shall be received no later than 60 minutes upon receipt of the data at their FMC.

Fisheries Monitoring Centers (FMCs)

11. Each Member or CNCP shall ensure that their FMC can automatically receive VMS data and transmit VMS data to the Secretariat.
12. Each Member or CNCP shall provide the Secretariat with VMS contact points in their FMCs including the name, position, email address and phone number of their VMS contact points. The Secretariat will make a list of VMS contact points available to all Members and Cooperating non-Contracting Parties.

Data Access and Use

13. All VMS data received by the Secretariat shall be treated as confidential information in accordance with NPFC's Data-Sharing and Data-Security Protocols for Vessel Monitoring System (VMS) Data (Annex 2).
14. In accordance with the NPFC's Data-Sharing and Data-Security Protocols for Vessel Monitoring System (VMS) (Annex 2), the Secretariat shall provide VMS data:
 - (a) By electronic means to a Member who has an inspection presence in the Convention Area;
or
 - (b) upon request from a Member to support search and rescue (SAR)

Data Sharing, Security and Integrity

15. In accordance with NPFC's Data-Sharing and Data-Security Protocols for Vessel Monitoring System (VMS) Data (Annex 2), VMS data shall only be accessed and used for the purposes included in this measure or for any other purposes as agreed by the Commission.
16. MTUs on fishing vessels shall be tamper-proof so as to preserve the security and integrity of VMS data.

VMS Data Transmission Failure

17. In the event that an MTU has failed to transmit VMS data for four hours, the flag Member or CNCP shall require the fishing vessel master to manually report every four hours to the FMC or the Secretariat by other means of communication.

18. A Member or CNCP may also require its fishing vessels to manually report directly to the Secretariat.
19. The flag Member or CNCP shall require an MTU that fails to transmit VMS data in accordance with this measure, be repaired or replaced as soon as possible and, in any event, within thirty (30) days of the VMS data transmission failure.
20. If the fishing vessel returns to port following an MTU VMS data transmission failure, the Member or CNCP shall not permit the vessel to undertake fishing in the Convention Area until the MTU has been replaced in accordance with the guidance in Annex 1 or is repaired and is able to transmit VMS data.
21. If a Member or CNCP finds that an MTU has failed to transmit VMS data for twelve hours, the Member or CNCP shall immediately notify the fishing vessel master, owner or authorized representative of this failure.
22. If a failure to transmit occurs more than two times within a period of one year, the flag Member or CNCP of the fishing vessel shall investigate the matter, including having an authorized official examine the MTU on board the vessel. The outcome of this investigation shall be forwarded to the Secretariat within fifteen (15) days of its completion.

Research Vessels

23. Notwithstanding the requirements in this CMM, research vessels operated by authority of a Member may use AIS for their position reporting. Such research vessels shall make their positions available via AIS at all times while engaging in research operations in the Convention Area. In the event of AIS data transmission failure, the research vessel is required to take steps as stipulated in paragraphs 16-21 mutatis mutandis. The flag Members of research vessels that make position reporting via AIS in accordance with this paragraph shall submit to the Secretariat relevant information (vessel name, MMSI number, abstract of research activities, etc.) 30 days prior to the initiation of their research activities. This paragraph will expire at the end of the 8th Commission meeting unless the Commission decides otherwise.

Review

24. The Secretariat shall report on the implementation of this measure annually to the Technical and Compliance Committee (TCC). The TCC shall review the implementation of the VMS after two years and make recommendations to the Commission as may be necessary.

Guidance on minimum standards for mobile transmitting units (MTUs)

1. The mobile transmitting unit (MTU) shall automatically and independently of any intervention by the fishing vessel, transmit VMS data as required by NPFC.
2. The VMS data shall be obtained from a satellite-based positioning system.
3. MTUs on fishing vessels must be capable of transmitting VMS data at least every fifteen minutes.
4. MTUs on fishing vessels must be tamper-proof so as to preserve the security and integrity of VMS data.
5. Storage of VMS data and other relevant information within the MTU must be safe, secure and integrated within a single unit under normal operating conditions.
6. It must not be reasonably possible for anyone, other than the Fisheries Monitoring Centre (FMC), to alter any of the VMS data stored in an MTU, including the frequency of position VMS data transmission to the FMC.
7. Any features built into the MTU or its software to assist with servicing shall not allow unauthorized access to the MTU that could potentially compromise the operation of the VMS.
8. MTUs shall be installed on fishing vessels by an authorized installer in accordance with the manufacturer's specifications and applicable standards and in accordance with a flag State's relevant domestic legal obligations, procedures and conditions.
9. Under normal satellite navigation operating conditions, VMS data must include the geographical location of a fishing vessel within an accuracy of 100 meters.
10. The MTU and/or the VMS service provider must be able send VMS data to multiple independent destinations.
11. The MTU and its component parts shall be fully integrated and housed in the same tamperproof physical enclosure.
12. The MTU must have:
 - (a) all components sealed by the manufacturer; or

(b) official seals¹, individually identified with unique serial numbers, applied.

13. Relevant domestic legal obligations, procedures and conditions for MTU installation on fishing vessels should be forwarded by members and cooperating non-Contracting Parties to the Secretariat or made available upon request.
14. The MTU must have an alternate power unit, to act as a backup in case of failure of the main power, to enable the MTU to continue to meet the VMS data transmission requirements of this CMM.
15. The MTU should include audible or visible alarms to indicate a unit malfunction.

¹ Official seals or other mechanisms must be of such a type to indicate whether the MTU has been accessed or tampered with.

NPFC Data-Sharing and Data-Security Protocol for Vessel Monitoring System (VMS) Data

Definitions

1. For the purpose of this Protocol, unless specifically defined herein, words and terms have the same meaning as in the Convention on the Conservation and Management of High Seas Fisheries Resources in the North Pacific Ocean (Convention) and any conservation and management measures (CMMs) adopted by the North Pacific Fisheries Commission (Commission or NPFC), including in particular the CMM on the Vessel Monitoring System (VMS).
 - (a) “Confidential” refers to non-public domain data and information held by Commission Members, the Secretariat, and by service providers contracted by the Commission, or contractors acting on their behalf, that is to be kept private, and shall not be accessed, released or disclosed unless such access, release or disclosure is for the purposes described in, and authorized by, this Protocol;
 - (b) “Scientific purposes” may include estimating distribution of fishing effort for use in the Commission’s research activities; planning for and implementing tagging programmes; modelling fishing effort for use in fisheries management activities, including management strategy evaluation (MSE); estimating abundance indices or undertaking stock assessments; validating logbook data; and, any other scientific purposes agreed to by the Commission.

Purpose

2. The purpose of this Protocol is to implement Article 16, paragraph 4 of the Convention, which states, “The Commission shall establish rules to ensure the security of, access to and dissemination of data, including data reported via real-time satellite position-fixing transmitters, while maintaining confidentiality where appropriate and taking due account of the domestic practices and domestic laws of members of the Commission.”

Scope of Application

3. This Protocol applies to VMS data transmitted to, received by, stored, and, used by the Secretariat, the Commission and its Members, and authorized contractors, from authorized NPFC vessels in the Convention Area.

General Provisions

Accountability and Control System

4. All VMS data shall be considered confidential.
5. It is the responsibility of each Commission Member, and the Secretariat, to take all necessary measures to comply with this Protocol when transmitting and receiving VMS data.
6. Prior to accessing VMS data, authorized contractors shall be informed that VMS data is confidential and shall sign the Confidentiality Agreement (attached as Appendix 1) stipulating that they have been informed that the VMS data is confidential and that they have reviewed, are familiar with, and agree to the procedures to protect confidential VMS data set forth in the Confidentiality Agreement.
7. Where VMS data is transmitted by the Secretariat, with the approval of the Commission, to a party not already authorized to receive VMS data in accordance with this protocol, the Secretariat shall remain responsible for such data. The third party must receive written authorization from Secretariat to receive VMS data and shall be required to sign the Confidentiality Agreement (attached as Appendix 1). Breach of the Confidentiality Agreement constitutes breach of this Protocol, and will result in access to confidential VMS data being revoked, until corrective actions deemed appropriate by the Commission and the Secretariat have been taken. The third party will maintain the data provided to it in a manner no less stringent than the security standards established by the Commission.
8. The Executive Secretary will report to the Commission annually on the compliance with this Protocol, including any breach thereof.

Data Purposes

9. All VMS data collection, access, storage, use, and dissemination shall only be undertaken for the purposes of monitoring, control, and surveillance in the Convention Area, supporting search and rescue operations, and fulfilling the functions of the Commission, as established in Article 7(1) and (2) of the Convention, including scientific purposes as defined above, and subject to any additional relevant regulations, protocols, CMMs or policies approved by the Commission.

Safeguards

10. All authorized personnel having access to VMS data are prohibited from unauthorized use or disclosure of such data.

11. All VMS data shall be protected against loss or theft, as well as unauthorized access, dissemination, copying, use, or modification, by security safeguards, in accordance with the Data Retention and Security Section of this Protocol.

Data Access and Use

12. VMS data should only be accessed and/or used by authorized personnel in the Secretariat, authorized MCS entities and personnel, and authorized contractors, for the identified purposes in this Protocol or for other purposes identified by the Commission.
13. The Secretariat shall not make VMS data available to a Member where the Commission has established that the Member has not complied with this Protocol, or the CMM for VMS.

Use for Inspection Presence in Convention Area

14. For a Member who has an Inspection Presence in the Convention Area, VMS data shall be made available electronically in accordance with the following provisions:
 - (a) Each Member shall identify a point of contact for VMS data;
 - (b) Each Member who has an Inspection Presence in the Convention Area shall provide the Secretariat with the geographic area (in multiples of 10 degrees latitude and longitude with a north and south latitude boundary and an east and west longitude boundary) of the planned boarding and inspection MCS activities at least 72 hours in advance, when practicable;
 - (c) Without prejudice and pursuant to CMM 2023-09, and following the notification process outlined above, the Secretariat shall make VMS data available electronically for the area defined in paragraph 14 b) as it is received, to each Member who has an Inspection Presence in the Convention Area. The provisions of this paragraph shall expire at the end of the next scheduled Commission meeting.
 - (d) Each Member who has an Inspection Presence in the Convention Area shall only make VMS data available to authorities or inspectors, as defined in the CMM for High Seas Boarding and Inspection Procedures for the North Pacific Fisheries Commission (NPFC) responsible for fisheries monitoring, control, and surveillance activities in the Convention Area unless the data is being used in an investigation, or a judicial, or administrative proceeding, and subject to any relevant domestic laws and policies, and has requested VMS data in support of HSBI/MCS activities.
15. Where the fishing vessel to which the VMS data pertains has been involved in an alleged violation of a CMM, the Convention, or domestic laws or regulations, the VMS data pertaining to the alleged violation may be retained, and the Secretariat will be notified, by Members who

have an inspection presence in the Convention Area until appropriate proceedings, including investigations, and judicial or administrative proceedings, have concluded.

16. Should no VMS data be retained pursuant to paragraph 15, each Member who has an Inspection Presence in the Convention Area shall delete all VMS data received from the Secretariat within seven days following the completion of monitoring, control, and surveillance activities in the Convention Area. The Member shall also submit a written confirmation to the Secretariat of the deletion of the VMS data within seven working days following the completion of monitoring, control, and surveillance activities.

Use for Search and Rescue Operations

17. For the purpose of supporting search and rescue operations by a Commission Member, the Secretariat shall make VMS data available upon request from a Member.

Data Retention and Security

Data Retention

18. All VMS data transmitted to the Secretariat in accordance with the Convention and CMMs shall be retained by the Secretariat.
19. Each Commission Member shall retain VMS data for fishing vessels flying its flag for at least one year.

Data Security

20. Each Commission Member and the Executive Secretary shall ensure the security of VMS data in their respective electronic data processing facilities, particularly where the use of VMS data involves transmission over a network.
21. Security measures must be appropriate to the level of risk posed by the transmission, processing, and storage of VMS data. At a minimum, the following security requirements must be implemented prior to transmitting or receiving VMS data:
 - (a) The Executive Secretary shall ensure that regional system access to VMS data under its control is protected such that all data that enters the system is securely stored and will not be accessed by or tampered with from unauthorized individuals by implementing, at minimum, the following measures:
 - (i) physical access to the computer system which transmits, uses, and stores VMS data is controlled;

- (ii) each user of the system is assigned a unique identification and associated password, and each time the user logs on to the system, he or she must provide the correct password;
 - (iii) user access shall be audited annually for analysis and detection of security breaches; and
 - (iv) each user shall be given access only to the data necessary for his or her task.
- (b) Data exchange protocols for electronic transmission of VMS data between Commission Members and the Secretariat shall be duly tested by the Secretariat and periodically reviewed by the Commission. Electronic transmission is subject to security procedures established in this Protocol.
- (c) Appropriate encryption protocols duly tested by the Secretariat and periodically reviewed by the Commission shall be applied by authorized contractors, including the use of cryptographic techniques to ensure confidentiality and authenticity.
- (d) Security procedures shall be designed by authorized contractors addressing access to the system hardware and software, system administration and maintenance, backup, and general usage of the system. Each Commission Member, and the Executive Secretary, shall ensure proper maintenance of system security and restrict access to the system accordingly. Each Commission Member shall liaise with the Secretariat in order to identify and resolve any security breaches or issues.

**Confidentiality Agreement For Accessing North Pacific Fisheries Commission (NPFC)
Confidential Vessel Monitoring System (VMS) Data**

Applicant Name, contact information, and signature:

Full Name	Agency/Organization, Address, Email, and Phone	Signature and Date

In return for the NPFC Secretariat granting me access to confidential NPFC VMS data, I hereby make the following declarations and promises:

1. I am (check the appropriate box):
 - a. a contractor employed by the NPFC, or one of its Members, whose official duties require access to confidential VMS data.
 - b. an employee of an organization, which the NPFC Secretariat has authorized in writing to receive confidential VMS data.

2. I am requesting access to confidential NPFC VMS data:
 - a. for the following purposes (provide a detailed explanation, attaching an additional sheet if necessary):
 - b. on behalf of the following organization: _____.

3. I have read and understood the NPFC Data-Sharing and Data-Security Protocols for Vessel Monitoring System (VMS) Data (“Protocols”). I understand that the VMS data I am requesting are confidential, as defined in the Protocols. I agree to abide by the provisions of the Protocols that address protecting and safeguarding confidential VMS data.
4. I agree to abide by any additional written conditions regarding the use of confidential VMS data the Secretariat attaches to this Confidentiality Agreement.
5. I agree to abide by the NPFC Data Sharing and Data Security Protocols.

6. I agree that the confidential VMS data shall be used only for the purposes for which I am requesting the data, be accessed only by me and other individuals who have signed a Confidentiality Agreement, and be destroyed upon completion of the usage for which the data are being requested. I further agree to report the destruction of the confidential VMS data to the Secretariat.
7. I agree to make no unauthorized copies of the requested confidential VMS data. If a copy of all, or part, of the data is made by me, all copies, and/or parts thereof, will be registered with the Secretariat and will be destroyed upon completion of the purpose for which I requested the data.
8. Prior to the publication of any report in which I intend to use requested confidential VMS data, I agree to provide the report to the Secretariat for clearance to ensure that no confidential VMS data will be published.
9. I agree to provide a copy of any published reports referenced in paragraph 8 to the Secretariat.
10. I agree not to disclose, divulge, or transfer, either directly or indirectly, the requested confidential VMS data to any third party without the prior written consent of the Secretariat.
11. I agree to promptly notify the Secretariat, in writing, of any unauthorized or inadvertent disclosure of confidential VMS data.
12. I assume all liability, if any, with respect to my breach of this Confidentiality Agreement after I receive the requested confidential VMS data.
13. In the event of my breach of this Confidentiality Agreement, I understand that the Secretariat will not grant me access to confidential VMS data until corrective actions deemed appropriate by the Secretariat have been taken by me, my employer, or by the Member under whose supervision I work.

This Agreement is effective on the date indicated below upon signature of an authorized representative of the Secretariat.

Authorized NPFC Secretariat Representative

Date