North Pacific Fisheries Commission

NPFC-2026-TCC09-IP06 Rev.2

Submitted by the Secretariat

NPFC 2025 Vessel Monitoring System Overview

Abstract:

This report presents data from the Vessel Monitoring System (VMS) for 2025,

Secretariat Note:

Rev.1 provides updates to section 3 d) and Table 1 on page 8 and paragraph 15 of Annex 2.

Rev.2 Restored the summary section.

2nd Floor Hakuyo Hall,
Tokyo University of Marine Science and Technology,
4-5-7 Konan, Minato-ku, Tokyo
108-8477, JAPAN

TEL +81-3-5479-8717
FAX +81-3-5479-8718
Email secretariat@npfc.int
Web www.npfc.int

Table of Contents

1. Introduction

This report presents an overview of the NPFC VMS operations in its fourth full year of operation. The NPFC Vessel Monitoring System (VMS) CMM entered into force in September 2021, with the program becoming fully operational on 1 January 2022. Under this measure, all NPFC registered vessels are required to transmit their positions hourly when present within the Convention Area. In cases where automated reporting is interrupted, the measure requires vessels to submit manual reports after four hours of inactivity and mandates investigations when a vessel experiences two "failures to transmit" within a calendar year. In practice, most transmission failures seem to stem from systemic or technical issues rather than non compliance. The Secretariat continues to work closely with VMS Member contacts each year to resolve data interruptions and improve reporting consistency. As with any new program, several years have been required to identify and address operational challenges, but overall, the system functions as intended. Nonetheless, several enhancements would strengthen reliability and efficiency.

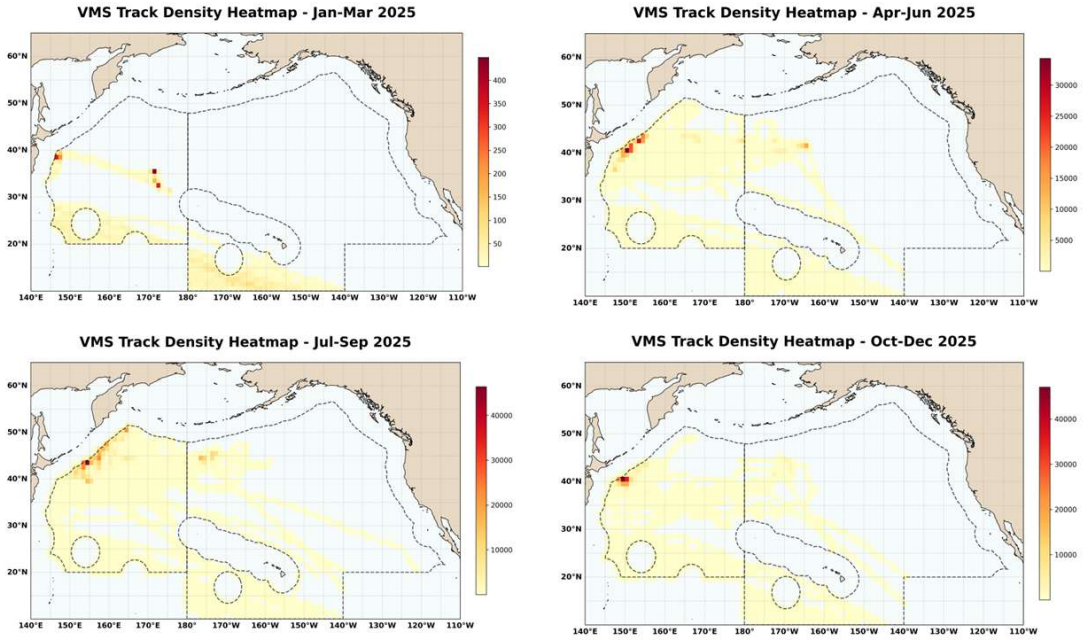
The VMS is an effective tool for monitoring vessel locations and assists MCS efforts in the Convention Area by allowing inspectors to locate vessels quickly and easily. It also supports a range of analytical projects such as tracking the concentrations of fishing and transshipment activities over seasons and facilitates a "cross check' of positional data against other reported sources, such HSBI/ air surveillance reports and transshipment records. No instances of non-reporting were identified in HSBI or aerial surveillance reports in 2025.

2. Overview in 2025

a) 2025 Quarterly Distribution

Monthly reporting statistics provide the Secretariat with a snapshot of vessel activity within the Convention Area throughout the year. Figure 1. represents a quarterly display of VMS signals. As indicated by the heat range bar on the right, while the absolute number of reports varies by quarters, it is possible to show the specific areas where registered vessels were active during a given period.

Figure 1. 2025 Distribution of VMS signals throughout the four quaters of the year



3. Data Interruptions

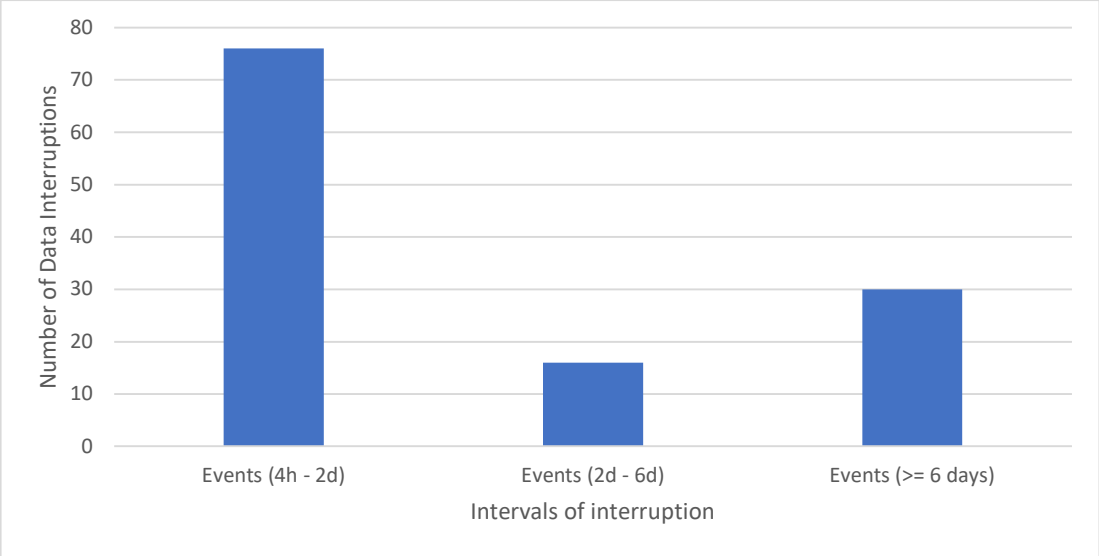
With more than 400 vessels reporting hourly in 2025, the system receives several million data points annually. Data gaps occur periodically due to satellite outages, equipment malfunctions, service provider issues, and other factors. These small data gaps typically occur without having a noticeable impact, and missing data points are quickly restored. However, when data interruptions exceed 4 hours, the vessel is required, by paragraph 18 of the measure, to report its position manually every 4 hours by another means:

> *18. 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.*

Figure 2. represents the number of interruptions exceeding 4 hours. Analysis indicates there were 122 such interruptions in 2025. While vessels experiencing these VMS interruptions should ideally transition to manual reporting, there are two primary challenges in determining whether these specific outages fall under the requirements of Paragraph 18. As will be discussed in Section 3 a), the first challenge involves the Entry/Exit issues at the

boundary of the Convention Area, and the second is the inadequate manual reporting (MAN) codes and discrepancies in vessel identification information (Section 3 b.). Therefore, a technical filtering process was applied to mitigate the impact of the two aforementioned issues and estimate the actual interruption cases. Given the high volume of data interruptions that naturally occur in a normally functioning system, it is simply not feasible to investigate every single instance. Moreover, because most outage assessments are conducted retrospectively—by which time any missing data has typically been restored, it is more productive to concentrate on areas where program performance can realistically be strengthened.

Figure 2. Number of Data Interruptions by Interruption Intervals(>=4h) in 2025



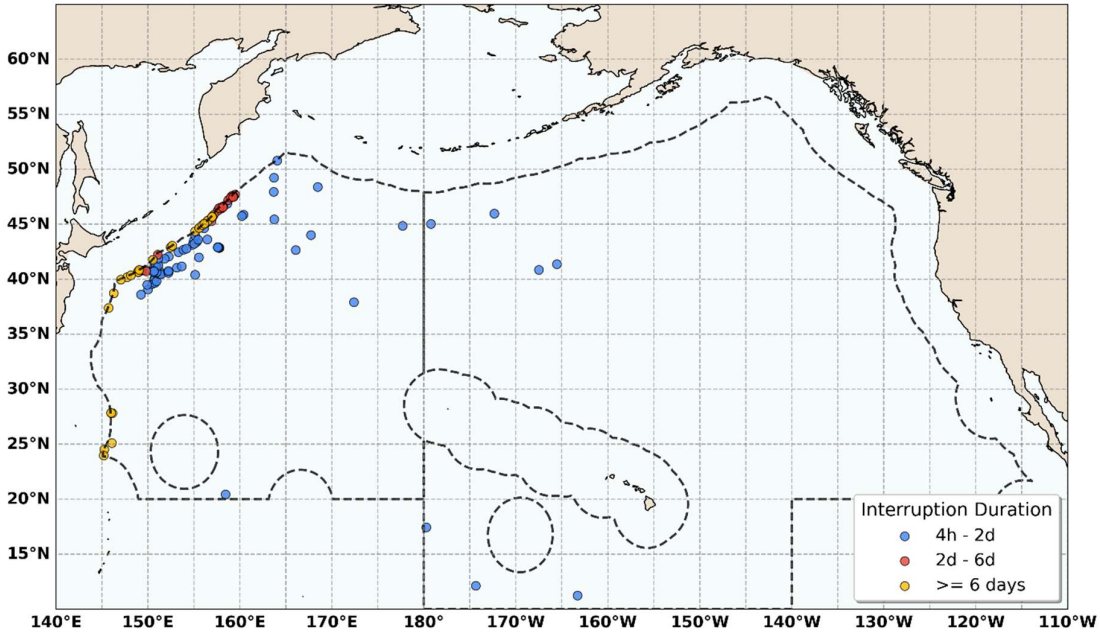
On the other hand, it is worth noting that across 66 high-seas inspections and 47 aerial surveillance patrols conducted in 2025, there was only one report of potential non-compliance related to VMS. This single instance concerned the absence of a tamperproof case for a Mobile Transmitting Unit (MTU), and importantly, no reports were received of any vessel operating without a functioning VMS. From the perspective of NPFC inspection activities, these facts suggest that position reports—which enable the monitoring of fisheries activities throughout the Convention Area—are likely being transmitted consistently and without significant issue.

a) Zone Entry / Exit Notification

As of 1 April 2026, all NPFC vessels will be required to submit entry and exit notifications in accordance with one of the options in Annex 2 of the CMM.

These notifications are expected to resolve many data gaps where vessels seem to "disappear" but are later confirmed to have exited the Convention Area. In one instance in 2025, the Secretariat's algorithm identified a 27-day data gap for a specific vessel. However, a detailed individual investigation revealed that the vessel had actually exited the Convention Area (CA) on the very first day the data transmission ceased. Figure 3. illustrates the spatial distribution of locations where data interruptions exceeding four hours were observed. As shown, a significant number of these cases occurred near the boundaries between the Convention Area and National Waters.

Figure 3. Geographic Distribution of Data Interruptions (> = 4h) in 2025



Although the NAF format supports automated entry/exit reporting, Members have opted to use other Annex 2 procedures, in part because many existing mobile transmitting units (MTUs) cannot generate automated messages.

Given that MTUs typically have a lifespan of 5-6 years, and it is understood that many NPFC units are more than 10 years old, future replacement cycles could require units with capacity for automated entry/exit reporting.

b) Manual Reporting / NAF Format

Although most vessels are submitting manual reports when transmission gaps exceed four hours, issues persist with the correct use of the NAF (North Atlantic Format) message structure—specifically, the omission of the "MAN" (manual) message type code. If this identifier is mislabeled or missing, the system fails to recognize the message as a manual report—even if the vessel is, in fact, submitting them. The NAF format, widely used across RFMOs, defines standardized codes for position (POS), entry (ENT), exit (EXI), and manual (MAN) messages. It is currently accessible through the THEMIS VMS user manual on the platform; however, it is proposed that the NAF format might be more accessible and better understood if annexed to the CMM and posted to the website.

Given the multitude of issues that have emerged within the VMS related to differentiating vessels, it is further proposed that the existing NAF format be updated to make the IMO number a mandatory field. This is suggested as the IMO is the most reliable unique vessel identifier available and its mandatory inclusion in VMS messages would eliminate the need to conduct manual searches when presented with conflicting vessel information. A draft revised format is provided in Annex 2.

c) SSL Certificate Renewal

A valid SSL certificate is essential for secure VMS data transmission. During the first two years of implementation (2022–2023), certificate expirations frequently disrupted data flows. A standardized renewal process was introduced in 2024. Members may use either their own certificates or those issued annually by the NPFC VMS service provider, but in both cases a specific renewal procedure must be followed to avoid transmission gaps. The renewal process is available at: https://www.npfc.int/manual-renewal-membercncps-vms-ssl-certificate.

Despite improvements, some Members continue to experience difficulties with the renewal process, occasionally resulting in significant data interruptions. The Secretariat now issues reminders one month prior to certificate expiry, which has reduced—but not eliminated—these disruptions. Neither the Secretariat nor the service provider receive details about the nature of the issues causing problems with renewing SSL certificates and therefore are unable to suggest potential solutions. Efforts to develop Standard Operating Procedures

(SoPs) with Member input have not yet received responses, but input will be essential to understanding the issue and developing solutions.

For outages caused by satellite malfunctions or service provider issues, there is little that can be done by either the Secretariat or Members to prevent such random occurrences, however, each such outage is a learning opportunity to better understand how to ensure a resilient system that can rebound quickly after such incidents to restore the data feed quickly and efficiently.

d) Anomalies in 2025

Table 1 shows the number of unique vessels that reported positions within the Convention area during a period without an active authorization in 2025 by month and by Member. Although the data could suggest potential instances of unauthorized fishing, further investigation is being conducted to confirm whether the vessels were simply transiting under another RFMO authorization or whether factors like vessel speed or trajectory indicate legitimate activity.

Table 1. Anomalies related to non- active vessels reporting VMS data in 2025

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
China	0	0	0	0	0	0	0	0	1	0	0	0
Japan	0	0	0	0	0	0	0	0	0	0	0	0
Korea	0	0	0	0	0	0	0	0	0	0	0	0
Panama	0	2	4	2	1	2	3	3	1	2	3	3
Russia	0	0	0	0	0	0	0	0	0	0	0	0
Chinese Taipei	0	1	0	0	0	0	0	0	0	0	0	0
Vanuatu	0	0	0	0	0	0	0	0	0	0	0	0
Total	0	3	4	2	1	2	3	3	2	2	3	3

Paragraph 8 of the VMS CMM requires that all NPFC registered vessels report their positions whenever they are present in the Convention Area (CA). Given the overlaps with the WCPFC CA and the SPRFMO Vessel Registry, it sometimes happens that a WCPFC carrier vessel operating inside their CA or a SPRFMO vessel in transit to that CA, may send

positions while in the NPFC CA. It can also happen that authorization periods for NPFC vessels are inadvertently allowed to expire, with the result that the vessel appears to be operating without authorization.

Since such cases may be detected as "unknown vessels" in the NPFC VMS platform, which could complicate assessment efforts, all cases of vessels transmitting under an apparently expired authorization are being followed up with Members.

4. Use of VMS Data to confirm Transshipment Information

VMS data is a valuable tool for MCS practitioners when planning patrols in the Convention Area, as it provides near real time information on the positions of active vessels. Beyond supporting patrol planning, it can also serve as an effective analytical resource for assessing compliance with VMS reporting requirements and other related obligations.

For example, VMS data can be used to identify the specific locations and times when offloading and receiving vessels converge for transshipment events. These data points can then be compared against information provided in transshipment notifications and declarations to verify accuracy and detect potential discrepancies.

With the introduction of API based data transfer in 2026 and mandatory electronic reporting in 2026, the intention is to conduct such analyses on a monthly basis and provide consolidated annual reports to Members going forward.

5. NPFC VMS Data Sharing and Data Security Protocol

Annex 2 of the VMS CMM (2024-12) contains the NPFC Data-Sharing and Data -Security Protocol for Vessel Monitoring (VMS) System. The protocol outlines provisions for data access, use and sharing while ensuring the safety and security of VMS data. The Members and the Secretariat have obligations to ensure that VMS data is securely stored and shared appropriately. Paragraph 8 outlines an obligation to report annually on compliance with the Protocol:

> *The Executive Secretary will report to the Commission annually on the compliance with this Protocol, including any breach thereof.*

Annex 2 presents the obligations from the Protocol and offers some explanation about how the protocol is being implemented in the NPFC.

6. SUMMARY

The NPFC VMS has become a robust and reliable platform for monitoring activities within the Convention Area and is on track to become an increasingly valuable analytical tool for assessing compliance with other CMMs as the full benefits of online reporting and automated data transfers are realized in 2026.

Although there were 122 data interruptions exceeding four hours in 2025, most were resolved through effective cooperation with Members. Looking ahead to 2026, the Secretariat is prioritizing improvements to manual reporting procedures, the implementation of mandatory entry/exit reporting, and enhancements to the certificate renewal process. These developments will help create an even stronger environment for monitoring, compliance assessment, and data-driven analysis.

Annex 1 – North Atlantic Format (NAF) for VMS messages

Data element	Field	Mandatory/	Type	Format	Remarks
Start Record	SR	M			Start of message
End Record	ER	M			End of message
Address Destination	AD	O	Char*3	ISO 3166-1 alpha 3 country code	Destination Country code Note: For NPFC, this value will always be "XNP".
From	FR	O	Char*3	ISO 3166-1 alpha 3 country code	Sender Country code
Type of Message	TM	M	Char*3		Type of message: • POS for standard position • ENT for entry to Convention Area • EXI for exit from Convention Area • MAN for manual position
Radio Call Sign	RC	O*	Char*20		Call sign of the vessel
Vessel Name	NA	O*	Char*20		Name of the vessel
Internal Registry	IR	O*	Char*20		Internal registration number
External registration	XR	O*	Char*20		External registration number
IMO number	IM	M	Char*20		IMO ship identification number
Flag State	FS	O	Char*3	ISO 3166-1 alpha 3 country code	Flag state of the vessel
Date	DA	M	Num*6/8	YYYYMMDD or YYMMDD	Year, Month, Day (UTC)
Hour	TI	M	Num*4/6	HHMM or HHMMSS	Hour Minute (in UTC) Or Hour Minute Second (in UTC)
Speed	SP	O	Num*3		Instantaneous speed (knot, to the nearest 0.1). Ex : SP/097 = 9.7 kt
Course	CO	O	Num*3	CCC	Instantaneous course (degrees) with a 1 degree resolution 0° = North, 180° = South. Ex : CO/047 = 47°
Latitude (decimal)	LT	M	Char*7/8	+/-DD.ddd(d) or hDDddd(d) h=N/S	Latitude (decimal degree to the nearest 0.01), between -90 and 90 degrees (negative sign for the positions of the south hemisphere). Ex : LT/-28.457 or LT/S28457 =
Longitude (decimal)	LG	M	Char*8/9	+/-DDD.ddd(d) or hDDDddd(d) h=E/W	Longitude (decimal degree to the nearest 0.01), between -180 and 180 degrees (negative sign for the positions of the west hemisphere). Ex : LG/+157.4572 or LG/E1574572 =

Annex 2- NPFC Data Sharing and Data Security Protocol for VMS

NPFC Data- Sharing and Data-Security Protocol		
Para #	**Text**	**Secretariat comment**
4	***All VMS data shall be considered confidential.***	**VMS data is classified as confidential. Access is granted exclusively to authorized Members upon formal request and through secure, verified login credentials.**
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.***	**The Secretariat employs robust security measures, including mutual (two-way) SSL certificate authentication between the Member's FMC and the NPFC VMS, alongside the provision of secure login credentials.**
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.***	**VMS data access is limited to authorized individuals and contractors who have signed the required Confidentiality Agreement (Appendix 1) to ensure data security and integrity.**
7	***Where VMS data is transmitted by the Secretariat, with the approval of the Commission, to a party not already***	**Access to the VMS platform is limited to authorized personnel who have completed and signed**

	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.	**the mandatory Confidentiality Agreement.**
8	***The Executive Secretary will report to the Commission annually on the compliance with this Protocol, including any breach thereof.***	**This report summarizes the current implementation status of the VMS Data-Sharing and Data-Security Protocol by the Secretariat, Members, and authorized third-party contractors.**
	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.	
9	***All authorized personnel having access to VMS data are prohibited from unauthorized use or disclosure of such data.***	**Access to VMS data is restricted to Members who have formally requested it for authorized MCS activities. All NPFC Secretariat personnel and third-party contractors are mandated to sign Confidentiality Agreements to ensure full compliance with this Protocol and to safeguard data against unauthorized use or disclosure.**
10	***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.***	**NPFC VMS data is stored in secure, physically inaccessible servers managed by authorized service providers, with comprehensive backup protocols in place. The system employs granular access controls: General Users (Members and contractors) are limited to "Read-Only" access for inspection and analysis, while only administrative users within the Secretariat and Service Providers possess the authority to modify or delete records.**

11	***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.***	
12	***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.***	**To ensure compliance with the Protocol, the Secretariat grants VMS data access solely for the purpose of authorized MCS activities.**
13	***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;***	**The Secretariat has established multiple contact points for all NPFC Members. A comprehensive and up-to-date list of VMS contacts is maintained on the official NPFC Website Contact List page (https://accounts.npfc.int/contact-lists)**
	(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 or surveillance operations at least 72 hours in advance, when practicable;	**In 2025, four Members submitted VMS data access requests, including required geographic areas and inspection plans, at least 72 hours in advance to ensure compliance with procedural requirements. Regarding the geographic specifications, two Members provided areas in multiples of 10 degrees latitude and longitude,**

		while the remaining two requested the entire Convention Area for their designated inspection operations
	(c) 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	**VMS data access is granted to Members with an established Inspection Presence. These Members assume responsibility for ensuring that data is accessed only by authorized authorities or inspectors, as defined under the CMM for High Seas Boarding and Inspection Procedures.**
14	***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.***	**For 2025, the Secretariat did not receive any formal requests from Members to retain VMS data beyond the completion of a designated inspection activity.**

15	***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.***	**In 2025, all 4 Members have provided written confirmation of data deletion following their MCS activities, however, one Member was delayed in submitting the notification.**
16	***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.***	**No requests for VMS data have been submitted to the Secretariat to support search and rescue operations during this reporting period.**
17	***All VMS data transmitted to the Secretariat in accordance with the Convention and CMMs shall be retained by the Secretariat.***	**The Secretariat retains all Member-transmitted VMS data within a secure server environment equipped with redundant backup systems. These facilities are physically inaccessible to unauthorized personnel, ensuring alignment with established NPFC data-retention and security protocols.**
18	***Each Commission Member shall retain VMS data for fishing vessels flying its flag for at least one year.***	**No issues Noted**

19	***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.***	**NPFC VMS employs two-way SSL authentication, requiring certificate exchanges between the Member's FMC and NPFC VMS to ensure secure data transmission. Furthermore, the NPFC VMS certificate is renewed each year, updating the security key to maintain system integrity.**
20	***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:***	**The NPFC VMS server is hosted in a secure, physically inaccessible facility. Logical access is controlled via granular permissions (Administrator, Operator, Reader) based on the user's operational necessity**
	i) physical access to the computer system which transmits, uses, and stores VMS data is controlled;	**Physical security protocols are in place; no direct or unauthorized physical access to the VMS server is permitted.**

	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;	**The NPFC VMS enforces individual authentication by assigning a unique identification (UID) and a secure password to each authorized user, ensuring all system entries are verified.**
	iii)user access shall be audited annually for analysis and detection of security breaches; and	**The system maintains comprehensive audit logs of all user activities. These logs are exportable and regularly monitored by the Secretariat to detect and analyze any potential security anomalies or breaches.**
	iv)each user shall be given access only to the data necessary for his or her task.	**Access is restricted through time-limited accounts or specific filters based on date, geographic zone, and fleet composition.**
	(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	**VMS data transmission between Members and the NPFC is tested semi-annually, coinciding with the renewal of SSL certificates. These tests ensure the continuous integrity and security of the communication channels between the respective VMS platforms.**
	(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.	**All data transmissions are encrypted via industry-standard HTTPS protocols, ensuring the confidentiality and authenticity of information exchanged between FMCs and the Secretariat.**

	(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.	**Service providers are tasked with the technical development and maintenance of the NPFC VMS, including access control protocols, system administration, and redundant backups. The Secretariat maintains active oversight, collaborating with providers to implement system enhancements and proactively resolve security vulnerabilities.**