SPRFMO

5th Meeting of the Compliance and Technical Committee
Lima, Peru 26 to 28 January 2018

CTC 5 – Doc 13
# Process for providing access to the SPRFMO VMS (THEMIS) to authorised non-staff users
Secretariat

CMM 06-2017, ANNEX 2, specifies the security and confidentiality requirements relevant for the SPRFMO VMS and instructs the Secretariat to take appropriate measures.

## 1. Authorisation:

Access to the SPRFMO VMS will be provided to non-staff members that are authorised by the Commission in accordance with CMM 06-2017, Annex 2, paragraph 8. The access is provided to the requesting VMS point of contact in the following instances:

a. A member or CNCP wants to access their own data;

b. A member or CNCP wants to access the data of other member or CNCP after acquiring a written consent for the data to be shared;

c. While a member or CNCP is planning for inspection or active surveillance operation at sea; and

d. For the purposes of supporting search and rescue activities undertaken by a competent Maritime Rescue Coordination Centre (MRCC).

In all of these instances, the request for access will be made by the official VMS Point of Contact. The VMS Point of Contact will be responsible for the secure distribution of the access details to the user(s) in accordance with CMM 06-2017, Annex 2, paragraph 3.

## 2. Notification:

Members and CNCPs will request the Secretariat, through their VMS Point of Contact, in writing (via email), to provide access to the SPRFMO VMS using the following format:

a. Either full name of the authorised user and/or IP address of the computer used for access;

b. Purpose of the access;

c. Access period ('From' and 'To' dates);

d. Geographic area and

e. Flags or individual vessel(s) for which access is requested.

Such notification must be submitted at least five (5) working days in advance, except as otherwise defined in CMM 06.

## 3. Security considerations:

All communications with the VMS Points of Contact will be encrypted using an **encryption protocol** to be determined. The Secretariat will set up the encrypted communication ability with each VMS point of Contact in February and March 2018.

In addition, the Secretariat will implement the following security measures:

a. Each authorised user shall be assigned a unique user identification and associated password valid for a maximum of one year.

- The user ID must be person specific and not generic. This will allow for the identification of the person to whom the access to SPRFMO VMS has been provided
- The password will consist of at least eight alphanumeric characters (with at least one uppercase letter, with at least one lowercase letter and with at least one number) and be different from previous passwords and from the ID/User Name.
- Each user is responsible that their respective ID and password are secure. They have to ensure that the password is stored securely in a place to which nobody else has access to. If a user has reason to suspect that his/her password has been compromised, he/she must inform his/her VMS Point of Contact immediately. The Secretariat's System Security Administrator will be notified without delay and promptly disable the compromised password (during work hours).
- If an incorrect password is entered more than three times within 30 minutes, the system will not allow access to that user ID for at least one hour. If the user has forgotten his/her password, the VMS Point of Contact may request a new password from the Secretariat's System Security Administrator.

b. The Secretariat has nominated John Cheva as the Security System Administrator for the SPRFMO VMS. The Secretariat's System Security Administrator will maintain an electronic record of all issued user IDs and passwords.

c. A user will be given access to those and only those functions and data that he/she is authorised to have access to.

d. In the instance of a request for access for surveillance operation, the VMS Point of Contact will inform the Secretariat via email of the date and time at which the downloaded VMS data have been deleted after the conclusion of the surveillance operation in accordance with CMM 06.

1. **Access restrictions**: User access to the SPRFMO VMS can be limited by the Secretariat's Security System Administrator using several criteria (some combinations are possible):

- **Mobiles or fleet restriction**: The user can only view certain fleets defined by the flag.
- **Geographical restriction**: The user can only access VMS data in a defined geographic area**.**
- **Time restriction:** The user can only access VMS data for defined time periods.