COMMISSION
NINETEENTH REGULAR SESSION
Da Nang City, Vietnam
28 November to 3 December 2022

INFORMATION PAPER ON THE FFA FINAL DRAFT EM SSPs – ENDORSED AS INTERIM GUIDELINES

WCPFC19-2022-DP08
28 October 2022

FFA Member CCMs

Consultants' Summary Note on Final Draft FFA EM SSPs

1. Following the third FFA EM Workshop on April 28-29, 2022, the consultants made several substantive edits to finalise the draft EM SSPs 1-4. The consultants received further comments from FFA members in writing and via video consultation post-workshop, and those are also incorporated in this final version.

2. The final EM SSP deliverable consists of the draft SSPs 1-4 contained herein, and two Reference Reports that accompany SSPs 1 and 2, and SSPs 3 and 4, respectively. All background information on the development of the SSPs is contained in the accompanying Reference Reports.

3. The third FFA EM Workshop acknowledged several key outstanding issues that will require further discussion as the EM work develops in the region. Those issues are listed in this Summary Note.

4. A list of substantive edits to the Draft EM SSPs that were made post-Workshop to reflect both Workshop and post-Workshop feedback is as follows:

    a. Removal of specific references to the DCC Longline EM Minimum Data Field Standards to refer to "regionally agreed upon minimum EM LL data field standard". This change broadens the flexibility for development of minimum standards to suit individual and collective EM programme requirements.
    b. Reference to an "EM Certifier" in SSP1c (Certification) without specific reference to the FFA Secretariat as an example of such Certifier, to allow for maximum flexibility in selecting an appropriate process to support the region's EM certification requirements.
    c. Where there are placeholders or issues requiring further consideration by FFA members, a NOTE in blue text has been included in the far-left column of the relevant section to highlight the area requiring additional attention.

5. The third Workshop acknowledged the following 'Key Outstanding Issues' requiring further discussion by FFA members to support regional EM programme development including implementation of the FFA EM SSPs:

    a. **Interoperability** is the requirement for EM analysis software to be able to facilitate the generation of EM Data from all EM Records that will be reviewed in the DRC. The reference report to SSPs 1 and 2 contain additional background information on Interoperability. The main Options for consideration are:

        OPTION 1: Requiring the use of a single EM Service Provider for onboard hardware for all vessels that will deliver EM Records to the DRC for analysis and using EM analysis software from the same EM Service Provider.

OPTION 2: Using multiple EM analysis software packages; one from each onboard hardware provider delivering EM Records to the DRC.
OPTION 3: Using EM analysis software that can analyse EM Records from multiple EM Service Providers. This may be facilitated by:

a. Requiring EM Service Providers to share the file types, data structures, syntax, and semantics of their EM Records and reference datasets.
b. Specifying a common format for exchange of EM Records.

b. **Multi-zone EM Records partitioning** is the division of EM Records at the end of a trip that may have been collected in more than one EEZ and/or the high seas and are being reviewed by different DRCs.

c. **Allocation of Roles** such as those for the FFA Secretariat, SPC, and national fisheries authorities in EM programme administration and management.

d. **Auditing and oversight** of the regional EM Programme and who the appropriate body is to carry out that role.

e. **Standardised regional templates/formats** can support regional harmonisation and implementation of the regional EM Programme.

f. **Timeframe for retention, disposal** for EM Records and EM Data will vary according to national programme requirements and a regional minimum standard is dependent on decisions around the regional EM Programme structure and governance.

g. **Optional component in Annex 4.4 (SSP4)** contains highly specific SSPs on Evidential Integrity and Chain of Custody, which requires further consideration on the level of detail and specificity that will be required by national EM Programmes and the regional EM Programme.

6. The consultants wish to thank FFA members and key stakeholders for their input to the development of these EM SSPs over the last 11 months. We are also appreciative of the feedback received during the workshop series and through separate video consultations with individual FFA members. We approached this work with the intention of making a positive contribution to the region’s development of an EM programme to fit its collective and individual member needs, and we hope this body of work will help serve that purpose.

Standards, Specifications, and Procedures (SSPs)

The management of fisheries and enforcement of fisheries law in the western and central Pacific Ocean is dependent on the access to timely and accurate fishing activity information. Currently, there are several tools employed to collect data and support fisheries management and enforcement, including electronic monitoring (EM). EM is an integrated system of onboard cameras and sensors and associated hardware, software, and procedures for analysing EM Records to generate EM Data.

This document addresses the following Standards, Specifications, and Procedures (SSPs):

SSP1a: On-board EM systems
SSP1b: EM hardware and software in Data Review Centres (DRCs)
SSP1c: EM System Certification
SSP2a: EM Records Transmission
SSP2b: EM Records Analysis and Quality Assurance
SSP2c: EM Records and EM Data Storage
SSP3: EM Records and EM Data Ownership and Access
SSP4: EM Records and EM data security and confidentiality

The SSPs were developed by two separate consulting teams and are accompanied by two separate Reference Reports covering SSPs 1 and 2, and SSPs 3 and 4, respectively. The Reference Reports provide additional background information and detail on how the two consultant teams drafted SSPs 1 and 2 and SSPs 3 and 4. These reports highlight considerations around evolving EM technology, challenges, and best practices in EM programme components. All SSPs have been harmonised in the same format in this draft.

The draft SSPs 1 and 2 are performance-based and designed to maximise future flexibility as programmes and technologies evolve. Therefore, the SSPs are agnostic with respect to specific technology as well as the structure(s) and objectives that stakeholders may choose to define for their EM programme(s). These SSPs are intended to inform regional conversations about different implementation and operationalization options that stakeholders can choose from as they move forward with rolling out regional EM programme(s).

The draft SSPs 1 and 2 were developed by a team of specialist consultants[1] who worked together remotely between July 2021 and May 2022. The team comprised individuals working in private sector data management, including with existing electronic monitoring (EM) programs, as well as non-government organisation representatives working on electronic monitoring pilot programs in the Western and Central Pacific Ocean (WCPO). The team also included individuals with several decades of fisheries management experience working with Forum Fisheries Agency (FFA) members, including on development of national EM programs. The team carried out a series of video consultations with relevant stakeholders (see Appendix G of accompanying Reference Report) over a four-month period and that feedback is incorporated in this Report and the associated SSPs 1 and 2.

[1] Rhea Moss-Christian and Barbara Hanchard (Independent Consultants), James T Mudge (productOps, Inc), Dr. Melissa Garren (Working Oceans Strategies), Mark Michelin (CEA Consulting), and Mark Zimring and Craig Heberer (The Nature Conservancy)

SSPs 3 and 4 were developed by a team of two consultants, Kim Duckworth and Marianne Vignaux, each with about 30 years of experience in the related areas of IT, fisheries management, fisheries data and fisheries science, in both national and RFMO jurisdictions.

Terms and Definitions[2]

Note: In some cases, the original drafts of the SSPs used slightly different terms across the consultant groups. Where appropriate, this version addresses some of the inconsistencies without changing the meaning of the original drafts.

Ancillary Logs - Data records from the EM system that are supplemental to the EM Records, such as a record of changes in system configurations and settings and a summary of system health checks performed.

Artificial Intelligence (AI) - The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

Authorised Agent - A person designated by the appropriate authority to carry out a specific function.

Cold Data Storage - The storage of inactive data that is rarely used or accessed. Cold data storage takes longer to access but is generally much cheaper to store.

Control Centre - The EM control centre is a computer and software system that records and stores information from EM System components (e.g., video, sensor data, GPS data, system log data) and also controls the operation of onboard EM system components.

Custodian - A person or organisation designated by the EM records and EM data owner to manage authorization and storage of EM records and EM data. There may be a different custodian for records and data.

Data Lake - A storage repository that holds raw data in its native format until it is needed for analytics applications.

Data Records - Actual records or entries in a data file or database.

Data Review Centre - A facility with supporting software platform(s) used to analyse e-monitoring records and record e-monitoring data.

Designated Installer or Service Technician - A person or entity authorised by an EM Service Provider to install or service an EM System.

EM Analyst - A person qualified to analyse e-monitoring records and record e-monitoring data in accordance with the EM standard and analysis procedures.

EM Analysis - See EM Records Analysis/Interpretation.

EM Analysis Rate - The proportion of e-monitored records that are analysed.

EM Certifier - An individual or organisation which has been accredited by the appropriate authority to inspect and approve e-monitoring systems for use.

EM Data - Data produced through analysis of e-monitoring records that conforms with the data standards specified in the SSPs.

EM Data Quality Reviewer - A qualified EM Analyst who reviews EM Data to verify and validate information produced by the EM Analyst.

EM Programme - A process administered by a national fisheries regulator(s) that includes the use of EM systems on vessels to independently collect and verify fisheries data and information.

EM Records - Footage (still images and video) and sensor data recorded by an EM System that can be analysed to produce EM Data. Sensors may include any number of sensors (e.g., hydraulic sensors) that are part of the EM equipment and whose data is recorded on the vessel as part of the EM system.

[2] For consistency, when available, relevant terms and definitions have been sourced from FFA, 2020. “Regional Longline Fisheries Electronic Monitoring Policy.”

EM Records Analysis/Interpretation - The process of an EM Analyst reviewing EM records and converting them into EM Data.

EM Service Provider - A third-party provider of EM technical and logistical services. An EM Programme may have multiple EM Service Providers and they may provide different services within the programme (e.g., onboard hardware, DRC software, DRC review services).

EM System - All the vessel and shore-based components supporting the generation, storage, transmissions, analysis and reporting of EM Records.

Event - An occurrence in the EM Records that is enumerated into EM data.

FFA Observer - FFA member personnel who are trained under a common framework (PIRFO) to observe, collect, record and report on fishing activities both at sea and in port.

FFA VMS - systems employed by FFA members and coordinated by the FFA to monitor the position and activities of fishing vessels for the purpose of effective management of fisheries.

Fishing - (i) Searching for, catching, taking or harvesting fish; (ii) attempting to search for, catch, take or harvest fish; (iii) engaging in any other activity which can reasonably be expected to result in the locating, catching, taking or harvesting of fish for any purpose; (iv) placing, searching for or recovering electronic equipment such as radio beacons; (v) any operations at sea directly in support of, or in preparation for, any activity described above; or (vi) use of any other vessel, vehicle, aircraft or hovercraft, for any activity described in items (i) to (v) above, except for emergencies involving the health and safety of the crew or the safety of a vessel.[3]

Fishing Trip - The collection of activities from the time of a vessel's departure from port until the return to port.

Geolocation device - A device that is used to capture information on vessel position, speed, and heading.

Independent - with respect to audits - no financial or current employment interest with the DRC

IUU - Illegal, Unreported and Unregulated Fishing.[4]

Machine Learning (ML) - A subset of AI that refers to the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data.

Owner - The FFA Member that owns the EM Records and EM Data.

Privacy Impact Assessment - A systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme.[5]

Regional Agency - A regional or sub-regional organisation that supports FFA member national EM Programmes and EM Systems.

Review for Data Quality - The verification process of re-analysing/interpreting a portion of previously analysed EM records to determine completeness, adherence to protocols, and accuracy of the EM Data produced by the EM Analyst.

Sensors - EM systems may be equipped with a variety of integrated sensors that can provide additional information on fishing activity, trigger activation or adjustment of configurations of cameras, and identify points of interest to expedite EM video review. This may include "synthetic sensors" that process raw sensor information to identify objects or events.

Uninterruptible power supply (UPS) - Provides power to the system and enables controlled shutdown in the event of a power loss.

[3] Forum Fisheries Agency, 2019. "THE HARMONISED MINIMUM TERMS AND CONDITIONS FOR ACCESS BY FISHING VESSELS:As amended by FFC110 (May 2019)."

[4] See FAO for a complete definition of IUU.

[5] Clarke, Roger, 2009. "Privacy impact assessment: Its origins and development."

User interface - A display that communicates EM system status messages and provides views of onboard cameras.

Vessel Monitoring Plan (VMP) - A document describing how an electronic monitoring system is specifically positioned and configured on a vessel and how fishing operations on that vessel will be conducted to allow effective monitoring of fishing activity and accurate generation of EM Data specified by the EM Programmes.

Vessel Operator - any person who is in charge of, directs or controls a vessel, including the owner, charterer and master.

SSP1a: Onboard EM Systems

Onboard EM Systems comprise all vessel components supporting the acquisition of and reporting of EM Records as required by the Regional Longline Fisheries Electronic Monitoring Policy. Onboard EM Systems shall be configured such that they collect the information set out in a regionally agreed upon minimum data field standard [6]. The core EM System components covered in these SSPs are: control centre, user interface, cameras, geolocation device, uninterruptible power supply, sensors, and communication system. Together, these components ensure that required information is collected, including system health status, to support fisheries management and enforcement objectives.

On-board EM System component	SSP
1. Control centre ***NOTE: Item (k) relates to Interoperability*	The EM system control centre must: a. Control all onboard EM hardware components. b. Be powered on and remain on while the vessel is underway and during all fishing activity, including during any at sea vessel rendezvous activity. c. Store EM Records on a fishing trip necessary for a DRC to extract EM Data for all of the fields in the latest version of the agreed upon regional minimum data field standards. d. Store and transmit system health status information (See System Health Status). e. Have sufficient storage capacity for all EM Records generated during a fishing trip until EM Records are transmitted to a DRC for review. f. Have sufficient backup storage to prevent data loss. g. Have the ability to encrypt stored EM Records. (See SSPs on EM Records and EM Data Security and Confidentiality) h. Have unambiguous and unique identification of storage devices (e.g., barcode on hard drives). i. Allow for the recovery and secure transmission of EM Records at the end of each trip.

[6] For example, such as in the current draft of the Data Collection Committee (DCC) Longline EM Minimum Data Fields Standards (NOV-2020), which may be revised in the future.

	j. Store all EM Records on storage devices and in formats that are compatible or can be readily translated into formats that are compatible with DRC hardware and EM review software. k. Allow the export of EM Records (and related sensor and annotated data) into the regional standard EM Records transfer format (for subsequent use by EM review software of another EM Service Provider)[7].
2. User interface	The onboard user interface must: a. Include a display. b. Include software that shows EM system health status (System Health Status) and real time images from installed cameras on the display. c. Allow authorised users (e.g., EM Service Providers, EM service technicians) to adjust system configurations. The onboard user interface should: d. Include a keyboard, mouse, touchscreen, or other device to allow user inputs to the system.
3. Cameras ***NOTE: Item (d) requires further discussion about minimum levels to ensure they meet national evidentiary requirements and maximises performance and flexibility; see Reference Report for further details.*	a. An EM system must be outfitted with cameras to capture imagery of fishing activity. b. The number and position of cameras must be sufficient to capture necessary imagery to collect all data fields required by the EM Programme in a manner consistent with the latest version of the regional minimum data field standards, particularly those in the following sections ○ Setting and Hauling Information ○ Special Gear Attributes ○ Catch Event Information ○ Potential Compliance Events Cameras must: c. Capture imagery that meets image quality standards under all fishing conditions for an EM Analyst in a DRC to extract all required data fields of the most recent version of the regional minimum data field standards. See also (Vessel Monitoring Plan) d. Be capable of accommodating remote or onboard configuration of parameters to optimise camera functionality throughout a typical fishing trip, such as:

[7] See Interoperability discussion in the accompanying SSP Reference Report.

	i. Frame rate *(placeholder for minimum level TBD)* ii. Resolution *(placeholder for minimum level TBD)* iii. Bit rate *(placeholder for minimum level TBD)* iv. Aperture *(placeholder for minimum level TBD)* v. Shutter Speed *(placeholder for minimum level TBD)* *These configurations may vary throughout a trip based on fishing activity and camera location to minimise file sizes and storage needs* (*see accompanying reference report for more detail on Video File Sizes*.) Recorded imagery must: e. Be recorded in a widely used and accessible video or image file format, such as MP4 or JPEG, and compression standards that are able to be viewed. f. Include a timestamp, GPS location, and FFA Vessel Register ID watermark on the video.
4. Geolocation device	a. A geolocation device[8] must be present to record vessel location coordinates and the associated date and time in a format specified by the most recent version of the regional minimum data field standards. b. The geolocation receiver must be installed and remain in a location in accordance with the manufacturer's guidelines such that the device can reliably function. c. The EM system must transmit geolocation data and associated date and time, and vessel identification information to DRCs on a regular basis, as defined by the relevant programme requirements, throughout the duration of a fishing trip in a format compatible with DRC software. d. The EM system must be able to verify whether transmissions of geolocation data and associated date and time, and vessel identification information to DRCs are successful. e. If the EM system is unable to transmit geolocation data due to a communication error, it must store geolocation data and automatically send it as soon as practically possible after communication is restored. f. The vessel location and timestamp data from the geolocation system must be capable of integration with the EM video data.

[8] The EM system may use an existing geolocation device on type-approved hardware on the vessel (e.g., VMS) or have its own geolocation device.

5. Uninterruptible power supply	The EM system must be powered by an uninterruptible power supply capable of controlled shutdown in the event of power loss.
6. Sensors	a. EM systems may be outfitted with sensors, which may include the use of camera imagery as a synthetic sensor, to capture information about fishing activity. These may include, but are not limited to: i. Pressure sensors ii. Hydraulic or drum rotation sensors iii. Temperature sensors iv. Door open/closed sensors v. Proximity sensors vi. RFID readers b. The EM system must be capable of generating and recording a log file of readings from system sensors with all sensor readings linked to/integrated with the vessel identification, location and timestamp data from the geolocation system.
7. Communication system	a. The EM System must have or integrate with at least one network communication system that enables the reliable and regular transmission (e.g., daily or weekly, hourly) of near-real-time data on system health (including still images for EM system status verification when prescribed by the programme requirements), sensors (if applicable), and geolocation to DRCs during all fishing activity, and supports remote access to the EM system by the EM Service Provider or their designated service technicians. b. The network communication system(s) must be a widely used and globally recognized technology, such as i. 3G, 4G, or 5G cellular networks. ii. Wi-Fi iii. Satellite communications. c. The EM system must be able to verify whether transmissions of data on system health (including still images), sensors, and geolocation to DRCs are successful. d. In the event that the EM system is unable to transmit data due to a communication error, it must store that data and automatically send it as soon as practically possible after communication is restored. e. The EM System must have ethernet or any other communication system allowing data transfer and remote access to the system via the onboard Internet connection.

General Requirements for onboard EM Components	
1. Weather Resistance	On-board EM hardware components must be sufficiently dust and water resistant (e.g., IP66) and durable (e.g., corrosion, impact, and vibration resistant) to operate reliably under the range of conditions expected in their location on longline fishing vessels.
2. Tamper Resistant and Tamper Evident	a. The onboard hardware shall be robust and tamper evident to mitigate the risk of intentional sabotage or malfunctions. This shall include both physical and software features. b. The EM System should feature a login history tool which allows the tracking of information on when and by whom system configuration settings have been accessed offering insights into possible tampering attempts.
3. Compatibility with Other On Board Equipment	The EM System must be capable of functioning in close physical proximity to other onboard electrical and hydraulic equipment (i.e., EM System operations must not be materially impacted by the presence of other onboard electrical equipment and must not materially impact the proper functioning of other onboard electrical equipment).
4. Compatibility with DRC Review Software ***NOTE: Requires further discussion on Interoperability*	All EM Records (e.g., video files, system log files, sensor log files) generated by the EM system must be compatible with EM analysis software being used by the DRC(s) where EM Records from the EM System will be sent to generate EM Data per the EM programme definitions.
5. Capable of Spatial Calibration	An EM system must be capable of spatial calibration for accurate image and fish length measurements using EM analysis software as required by the EM programme.
6. System Health Status	a. The system must execute a system health test on power up and provide a visual signal that the system has passed or failed on the system display.

	b. The EM system must be able to generate a log file including, but not limited to, the following EM processes to capture the operational health status of the system: i. System power up ii. System shutdown planned iii. System shutdown unplanned (e.g., power cut) iv. Camera connectivity v. Camera recording start and stop times (planned) vi. Camera recording error[9] vii. Available hard drive space viii. Sensor connectivity ix. Sensor recording start and stop times (planned) x. Sensor recording error xi. Activation and deactivation of recording triggers (e.g., vessel speed, drum rotation sensors, geofencings, and time scheduled) c. System must undertake regular system health checks throughout the duration of the fishing trip at a frequency defined by the EM Programme and must show health status ALERTS (errors and warnings) on the display of the user interface (Onboard User Interface) of the control centre. d. The EM system must be able to capture and store single frame images from each onboard camera on a regular basis (e.g., timed intervals, such as hourly, or on event triggers such as geofences) to show that cameras are operational, not obstructed, obscured, or displaced.

[9] The appropriate time interval may require regular review and updating.

Installation, Operation, and Service of onboard EM Systems	
Requirement	SSP
1. EM system installation	The EM Service Provider or their designated installer must: a. Coordinate installation with the vessel owner or their designated representative. b. Install an onboard EM system that meets the performance standards described in onboard EM System Component and General Requirements. c. Ensure the onboard EM system meets the performance standards described in onboard EM System Component and General Requirements through system tests. d. Provide the necessary information for the vessel owner/operator or their designated representative to complete a Vessel Monitoring Plan (Vessel Monitoring Plans) or complete the Vessel Monitoring Plan on behalf of the owner/operator. e. Brief the vessel operator and crew member(s) and provide documentation on EM system operation, maintenance, and procedures to follow during regular operation and in the event of a system malfunction (Vessel Monitoring Plans). f. Submit notification to the relevant EM Programme of system installation in the agreed form that attests to the system functionality and its conformance with the performance standards described in onboard EM System Component and General Requirements. (See SSPs on EM Records and EM Data Security and Confidentiality)[10] The vessel owner or their designated representative must: a. Provide information[11] describing the vessel configuration and systems to facilitate EM system installation. b. Make the vessel and appropriate personnel (such as engineers, fishing master, multilingual staff, etc.) available and provide the EM Service Provider unfettered access, including to the ship's power supply, to complete EM system installation.

[10] Note: A standardised regional form could be useful for this purpose

[11] Note: A standardised regional form could be useful for this purpose

2. Vessel Monitoring Plan	a. Vessel owner or EM Service Provider must complete a Vessel Monitoring Plan , and submit it to the EM Programme for approval after installation of an EM hardware system on a longline vessel and prior to departure from port. (See section EI4 of SSPs 3&4)[12] b. Vessel Monitoring Plans shall be updated and submitted to the EM Programme at a frequency determined by the EM Programme and anytime changes are made to information or requirements outlined in the VMP (e.g., new vessel contact information, change in EM System configuration, change in catch handling guidelines). c. The Vessel Monitoring Plan must include: i. Contact information for the EM Service Provider, vessel owner(s), and vessel operator(s), and base manager(s) (if applicable). This should include information for a primary contact that can be used to communicate with the vessel while at sea, if available. ii. General vessel information as specified in the vessel identification section of the latest version of the regional minimum data field standards. iii. A diagram, description, and photo(s) of the vessel layout that identifies where key fishing activities will occur on the vessel (e.g., hauling, sorting, discarding) and measurements of all items, tools, or areas on the vessel that EM Analysts will use to estimate lengths of catch which require length measurement in the latest version of the regional minimum data field standards. iv. A description of the EM setup, including: ● The number and location of cameras including images of their installation location and an image from each camera's perspective, including at night to demonstrate sufficient lighting. ● A description and image of the location of all other components of the installed EM system (e.g., geolocations system, EM control system, sensors, power supply). ● A list of system configuration settings, including: ○ Camera configuration settings (e.g., frame rates, resolution, bitrate) ○ Sensor units and threshold values ○ Data recording frequencies and/or sensor triggers for recording ○ Software and Firmware versions ○ Spatial calibration settings

[12] Note: A standardised regional form could be useful for this purpose

	v. Required catch handling procedures to ensure that EM Records collected allow for an EM Analyst to generate EM Data for all the required fields of the latest version of the regional longline EM minimum data field standards (e.g., handling in view of cameras, allowable discard locations). vi. Vessel duty of care responsibilities to prevent system malfunctions, such as: ● Verifying system functionality at the beginning and throughout the duration of each trip ● Required frequency for checking camera lenses and cleaning obligations vii. Vessel responsibilities in the event of system malfunctions that describe the steps that must be taken. viii. There must be regionally standardised and enforceable requirements for adherence to the requirements of Vessel Monitoring Plans including, catch handling procedures, vessel duty of care responsibilities to prevent EM system malfunctions, and vessel responsibilities in the event of system malfunctions. (See SSP4 on EM Records and EM Data Security and Confidentiality)
3. Field and Technical Support Services	The EM Service Provider, in a timely manner, must: a. Communicate with vessel operators and the relevant EM Programme to coordinate service needs, resolve specific programme issues, and provide feedback on programme services. b. Provide maintenance and support services, including software and firmware updates, such that all installed EM systems perform according to the performance specifications described in onboard EM System Component and General Requirements and that field services are scheduled and completed with minimal delays to minimise disruption to fishing operations. c. Provide technical assistance to vessels upon request on EM system operations, diagnosing causes of system malfunctions, and providing assistance for resolving malfunctions. This assistance must be available 24 hours a day, seven days a week, year-round. This service must be provided in English or another language spoken by the vessel point of contact as defined in the programme specifications. d. Submit to the relevant EM Programme, and the EM Certifier, where appropriate, reports of all requests for technical assistance from vessels and service calls that include: i. The name and designation of the vessel point of contact ii. The date(s) and time a request for service was made. iii. The date(s) and time(s) when the EM Service Provider called or visited the vessel to provide technical assistance.

iv. A description of the issue.
v. A description of how the issue was resolved, including actions completed during all service calls or visits in response to the request for service.
vi. The date and time the issue was resolved.

The vessel owner/operator must:

a. Follow duty of care responsibilities described in the Vessel Monitoring Plan.
b. Immediately report EM system malfunctions to the EM service provider, including the date, time, and, if possible, the geolocation when the malfunction was first detected.
c. Follow vessel responsibilities outlined in the Vessel Monitoring Plan in the event of system malfunctions.

The EM Programme must:

a. Define vessel responsibilities in the event of system malfunctions that describe the steps that must be taken under different failure scenarios.
b. Respond to EM Service Providers or vessel owners/operators in a timely manner.

SSP1b: Data Review Centres

A data review centre (DRC) is an entity with access to supporting software platform(s) used to analyse EM Records and generate EM Data. DRCs may serve individual FFA members, subregional groupings, or the entire FFA membership. They may also be administered by individual FFA members, a sub-regional or regional body, or a third-party (commercial) provider. SSP1b is not specific to any DRC structure and covers the required infrastructure (hardware and software) to analyse EM Records. SSPs addressing storage infrastructure are contained in SSP2c. Security measures for DRCs are contained in SSP4.

A DRC must include the following components:

1. EM analysis software (which could be cloud-based)
2. EM analysis workstation(s)
3. Qualified EM Analysts

The EM programme must have:

4. A system to monitor EM system health on vessels, which may be part of or separate from the DRC

DRC Component	SSP
1. EM Analysis Software ***NOTE: This section requires further discussion on Interoperability.*	The DRC must use EM analysis software to facilitate the generation of EM Data from EM Records. The EM analysis software must: a. Be compatible with the file types, data structures, syntax, and semantics of EM Records that will be analysed with the software. b. Be the latest version of analysis software, including security patches c. Be able to decrypt EM Records. d. Be able to display EM analysed output: i. Display the vessel track on a map based on geolocation data integrated in the EM Records, with an option to display the geolocation data of each vessel. ii. Display synchronised imagery from all cameras simultaneously with zoom capability and other relevant imagery features.

	iii. Display a visual timeline with sensor readings or status. iv. Display synchronised sensor data (including vessel heading and speed) and video imagery simultaneously. e. Be able to spatially calibrate an image and measure the length of species brought onboard as required by the EM Programme (e.g. through a digital measuring tool which must be available in the EM analysis software). f. Allow EM Analyst notations. g. Be able to bookmark specific video segments or events that can be used to navigate quickly to those points in the video and data feed. h. Be able to extract and save segments of video and sensor data, including extraction and saving of still images and the ability to automatically extract short duration video clips of catch. i. Be compatible with relevant databases used in regional fisheries management organisations to store information on longline tuna fishing activity. j. Be able to import EM records (and related sensor and annotated data) from systems of other EM Service Providers that have been exported into the regional standard EM Records transfer format.
2. EM Analysis Workstations	The DRC must have EM analysis workstation(s) where EM Analysts will use EM analysis software to generate EM Data from EM Records. The EM analysis workstation must have: a. Hardware and software, or cloud-based platforms that enable effective EM analysis b. Reliable data transmission capabilities sufficient for efficient streaming or download/upload of data required for EM Records analysis, reporting of EM Data, and storage of EM Records. c. Have proper ergonomics that support analyst well-being, quality, and efficiency.
3. Qualified EM Analysts	The use of EM software to generate EM Data from EM Records must be conducted by qualified EM Analysts. The qualified EM Analysts must: a. Complete an FFA-recognized EM Analyst qualification and training programme. b. Meet a minimum standard on an examination(s) to demonstrate necessary knowledge and skills to complete EM Analysis (e.g., species ID, EM review processes, etc.). c. Have an absence of fisheries-related convictions. d. Be independent from fishing-related parties including, but not limited to, vessels, dealers, processors, canners, traders, shipping companies, fishers, fisheries managers, advocacy groups, or research institutions to prevent conflicts of interest, whether it be a direct or indirect interest that could substantially affect the performance or

	non-performance of the official duties of the EM Analyst. Any potential conflicts of interest must be declared to their employer and EM Certifier.
4. A system to monitor EM System health on vessels	a. The EM Programme must have a health monitoring system to receive and display near real-time information of onboard EM System health status (System Health Status), still images to verify functionality of onboard cameras (System Health Status), and geolocation data (Geolocation device). This system may be part of the DRC. b. The on-shore health monitoring system must receive any alerts (errors and warnings) that have been generated from the onboard health monitoring system. c. The health monitoring system must be able to display the latest geolocation of all covered EM Systems on a map.

SSP1c: EM Certification

There are at least three potential EM certification models, described in detail in the associated report, that the region could choose to adopt as the regional EM programme continues to take shape. This section is a detailed draft of SSPs for a Service Provider Approval model based on Member feedback from the January 2022 workshop.

Certification of EM Providers	SSP
1. General Requirements of EM Certification Mechanism	EM Service Providers must apply to a single oversight organisation (EM Certifier, such as an agreed upon regional body or independent 3rd party) that will review their qualifications and certify that they meet the standards required of EM Service Providers for the Regional Longline Fisheries Electronic Monitoring Policy. The EM Certifier must: a. Accept, review, and approve/reject applications for certification of new EM Service Providers on a regular basis. b. Renew certifications for or decertify EM Service Providers based on their compliance with EM Programme Requirements on a regular basis. c. Document all complaints or issues submitted by EM programme stakeholders concerning the performance of an EM Service Provider. EM Programmes must: a. Use only certified EM Service Providers. b. Document and communicate performance issues with EM Service providers to the EM Certifier to inform recertification/decertification processes.
2. Independent third-party	Any service provider intending to provide the electronic monitoring services described in the Regional Longline Fisheries Electronic Monitoring Policy must apply to and be approved/certified by the EM Certifier by

monitoring provider standards

***NOTE: Item 1(h) requires further consideration of how training equivalence will be assessed for commercial review providers*

Item 2(a)(v) requires further consideration pending development of regional and national EM frameworks, incl issues of time lag depending on trip lengths/types

Item 2(e) requires further consideration on appropriate conflict of interest text.

Item 2(f) requires further discussion pending designation of the EM Certifier and role of the FFA Secretariat.

Item 3 requires further

submitting a cover letter that specifies which services (e.g., on-vessel EM hardware, EM Records review) the provider is applying to provide, and a complete application that includes all of the information, documentation, and statements detailed in this section. The EM Certifier shall approve/certify service providers as eligible to provide the EM services or a subset of EM services, and can disapprove/decertify service providers through notice in writing to individual service providers if the following criteria are no longer being met:

1. **EM Service provider information.** As part of the application for service provider approval/certification, potential service providers must include at least the following information:
    a. Identification of corporate structure, including the names and duties of controlling interests in the company such as owners, board members, authorised agents, and staff; and articles of incorporation, or a partnership agreement, as appropriate;
    b. Contact information for official correspondence and communication; A statement from each owner, board member, and officer that they are free from a conflict of interest with fishing-related parties including, but not limited to, vessels, dealers, processors, canners, traders, shipping companies, , advocacy groups, or research institutions and will not accept, directly or indirectly, any gratuity, gift, favour, entertainment, loan, or anything of monetary value from such parties;
    c. A statement from each owner, board member, and officer describing any criminal convictions, contracts with the FFA or FFA Members that they have had along with any performance feedback they received on the contract, and previous disciplinary or decertification action while working as, or to fill the function of, an observer, or EM analyst or as an observer or electronic monitoring service provider;
    d. A description of any prior experience the applicant may have in placing individuals or monitoring equipment in remote field and/or marine work environments including, but not limited to, recruiting, hiring, deployment, equipment installation and maintenance, and personnel administration;
    e. A description of the applicant's ability to carry out the responsibilities and duties of an electronic monitoring service provider to meet the requirements of these SSPs and relevant EM Programmes

consideration of 3rd party review qualifications pending DCC advice on regional EM analyst qualifications.	and the arrangements to be used, including details on what specific elements of electronic monitoring services the service provider is able to offer; f. Evidence of adequate insurance (copies of which shall be provided to the vessel owner, operator, or vessel manager, when requested) to cover injury, liability, and accidental death to staff who provide electronic monitoring services to vessels; vessel owner; and service provider. g. Proof of benefits and personnel services provided in accordance with the terms of each electronic monitoring staff's contract or employment status; h. Proof that the service provider has EM Analysts that have successfully completed an FFA-recognized EM Analyst qualification and training programme; i. An Emergency Action Plan describing the provider's response to an emergency with any EM Service Provider staff and subcontractors providing EM Services in an EM Programme, including, but not limited to, personal injury, death, harassment, or intimidation; and j. Evidence that the company is in good financial standing. 2. **EM Service provider performance requirements.** Electronic monitoring service providers must be able to document compliance with the following criteria and requirements: a. A service provider must establish and carry out a comprehensive plan to deploy electronic monitoring equipment that is approved by EM Certifier in accordance with SSPs 1-4, including all of the necessary vessel reporting/notice requirements to facilitate such deployment, as follows: i. A service provider must be available to industry 24 hr per day, 7 days per week, with the telephone system monitored a minimum of four times daily to ensure rapid response to industry requests; ii. A service provider must be able to deploy approved electronic monitoring services to all ports in which service is required by the fishery, or a subset of ports as part of a contract with a particular party; iii. A service provider must report approved electronic monitoring system installations to the EM Certifier and the relevant EM Programme(s) in a timely manner;

iv. A service provider must assign approved electronic monitoring services without regard to any preference by the fisheries manager or representatives of vessels other than when the service is needed and the availability of approved EM services;

v. For service providers offering EM Records review services,

1. *The service provider must ensure that video reviewers remain available to the relevant EM Programme and compliance authorities, for debriefing for at least 2 weeks following any monitored trip or submission of EM data from a fishing trip. Electronic monitoring service providers that review EM Records and generate EM Data must ensure that the EM Records and EM Data are retained for a minimum of [6] months after EM Data is submitted to the relevant EM Programme for a fishing trip. The EM Service Provider must provide the relevant authorities access to EM Records and EM Data upon request;* [example text on availability of video reviewers and timeframe; timeframe should be determined by the relevant EM Programme and could be dependent on multi-EEZ trip scenarios]

b. The EM Service Provider must report possible electronic monitoring staff harassment; discrimination; concerns about vessel safety or marine casualty; injury; and any information, allegations, or reports regarding electronic monitoring staff conflict of interest or breach of the standards of behavior to the EM Programme and EM Certifier as specified by the EM Programme and the Regional Longline Fisheries Electronic Monitoring Policy;

c. The service provider must submit to the EM Certifier, if requested, a copy of each signed and valid contract (including all attachments, appendices, addendums, and exhibits incorporated into the contract) between the service provider and those entities requiring services and between the service provider and specific subcontractors, authorised installation and service technicians, or electronic monitoring staff;

d. The EM service provider must submit to EM Certifier or the EM Programme, if requested, copies of any information developed and used by the service providers distributed to vessels, such as informational pamphlets, payment notification, description of duties, etc.;

e. *Service provider's owner(s), must declare any direct or indirect interest in a fishery managed under a Members national laws or regulation, including, but not limited to, fishing vessel, dealers,* *shipping companies, sectors, sector managers, advocacy groups, or research institutions and may not solicit or accept, directly or indirectly, any gratuity, gift, favour, entertainment, loan, or anything of monetary value from anyone who conducts fishing or fishing related activities that are regulated by a Member, or who has interests that may substantially affect the performance or non-performance of the official duties of service providers.* [example text for consideration and discussion on appropriate approach to address potential conflicts of interest]

f. A system to record, retain, and distribute the following information to the EM Certifier, relevant EM Programmes, and where appropriate, the regionally agreed upon bodies (such as SPC), as requested, for a period specified by [FFA], including:
   i. Approved monitoring equipment deployment or video review levels, including the number of refusals and reasons for such refusals;
   ii. Incident/non-compliance reports; and
   iii. Electronic monitoring data and reports.
      - A means to protect the confidentiality and privacy of records submitted by vessels in accordance with SSPs 3 and 4.

3. **Standards for individual EM Analysts employed by EM Service Providers (i.e. non-FFA members or entities).** For an individual to be approved/certified as an EM Analyst, the service provider must demonstrate that each potential reviewer meets the following criteria:
   a. Complete an FFA-recognized EM Analyst qualification and training programme.
   b. Meet a minimum standard on an examination(s) to demonstrate necessary knowledge and skills to complete EM Analysis (e.g., species ID, EM review processes, etc.)
   c. Have an absence of fisheries-related convictions.
   d. Be independent from fishing-related parties including, but not limited to, vessels, dealers, processors, canners, traders, shipping companies, fishers, fisheries managers, advocacy groups, or research institutions to prevent conflicts of interest, whether it be a direct or indirect interest that could substantially affect the performance or non-performance of the official duties of the EM Analyst. Any potential conflicts of interest must be declared to their employer and EM Certifier.

	4. **Electronic monitoring operational standards.** In addition to the independent third-party monitoring provider standards specified above, any electronic monitoring program developed must meet the operational standards, specifications and procedures detailed in SSPs 1-4 to be approved by the EM Certifier.

SSP2a: EM Records Transmission

Transmission of EM Records occurs at the end of a vessel trip with the retrieval and delivery of a storage device from a vessel to a DRC. Technological advancements will impact how EM Records are moved from vessels to DRCs, i.e. via transfer of a physical storage device, internet, or satellite technology. All EM Records must be encrypted (see SSPs on *EM Records and EM Data Security and Confidentiality* on security of EM Records) and DRCs must keep a log of all EM Records that are received. The following SSPs apply to specific methods of transmission. Future technological advances may bring forward new methods of transmission that will require additional considerations.

Transmission Method	SSP
1. Storage Device Retrieval	Storage device retrieval (e.g., hard drives) requires the removal of physical storage devices from the vessel at port and transporting and/or shipping it to the DRC for review. This transport process may involve several steps including sending the storage device to an intermediary party (i.e,. a records custodian) or regional centre for records storage or record distribution to DRCs (i.e., records parsed and sent to DRCs based on EEZ). Specific SSPs related to the security logistics of records transmission and hard drives are included in *SSP4 on EM Records and EM Data Security and Confidentiality.* a. Vessel operators will transfer possession of the EM Records within the time frame specified by the relevant authority of arriving at a place/port of unloading to an authorised individual.

	b. Cleaned and formatted drives will be swapped for used drives at the time of transfer. Specifications on acceptable processes for removing (cleaning) data from drives are covered in the SSPs on EM Records and EM Data Security and Confidentiality. c. If the drives are being shipped outside of the port location, the authorised individual will be responsible for packaging the drives and shipping through a carrier or method approved by the relevant authority. d. Storage devices must be packed to ensure that they are not damaged or corrupted during transit. This is especially important for standard HDDs (hard disk drives) which are not as robust as SSDs (Solid State Drives), though care needs to be taken with any type of drive. e. Vessel owners or an authorised representative must sign for the removal of the hard drives. SSPs for vessel owners and couriers are outlined in the SSP4 on EM Records and EM Data Security and Confidentiality. f. EM Records must be brought from the vessel to the DRC, records processing centre, or processed for shipment by an authorised individual within the time frame specified by the relevant authority based on chain of custody rules in the programme specifications (see SSPs on EM Records and EM Data Security and Confidentiality). This may include delivery to an authorised centre in the place/port of unloading where the hard drive contents may be copied at the centre and sent digitally from the centre to a DRC in another location. g. Once the storage device (or an exact copy of the contents of the device) arrives at an authorised centre, its condition (e.g. damaged, corrupted, OK) must be logged and the drive secured in accordance with specifications outlined in SSPs on EM Records and EM Data Security and Confidentiality. h. Once the EM Records from the hard drive are cloned and stored, the hard drive should be cleaned, formatted, and prepared per the EM Service Provider specifications for use on future trips.
2. Bulk EM Records Transmission	Bulk EM Records transmissions are communications that transmit large amounts of data at one time, such as an entire trip's EM Records, and rely on various technologies to transmit information at high-speeds to shore-based data centres. Bulk EM Records transmissions may be approved as part of an EM programme if it meets the following performance-based criteria: a. Vessels can access shore-based communications with sufficient bandwidth to transmit all of the required EM Records.

	b. EM Records must be transmitted to the on-shore DRC (or authorised centre for records processing or storage per programme definition) or utilise shore-based infrastructure to transmit the records to a remote DRC. c. The vessel is in range of the port long enough that all the ships' EM Records can be transmitted while the vessel is within high-speed transmission range of shore.
3. Near Real Time Transmissions	Near real-time transmissions are similar to near-shore transmissions. The primary differences are the technology used (e.g., satellite), available speeds, and the duration of transmissions. Unlike bulk transmissions which require sending large amounts of EM Records at one time, near real-time transmissions can occur over the duration of the trip. a. The onboard EM system should verify that the EM Records were received by the intended recipient. If the EM Records were not verified as being received, the EM system should queue the records to be sent on a future attempt. If the EM system continues to have issues with EM Records transmissions, it must send an EM Systems alert with the status of the EM system to the EM Service Provider and Programme Director as well as the vessel operator. b. Vessel operators will contact EM system provider technical support if the EM notification system is not able to communicate with the EM Service Provider c. The vessel must retain a backup drive of all EM Records for instances when there are communication issues. See SSPs on EM Records and EM Data Security and Confidentiality. d. If the EM system is not able to transmit EM Records, the DRC or approved records custodian must have a process of retrieving/receiving the backup drive from the vessel for review when it comes into port from authorised parties per programme specifications. e. EM Records must be sent at a minimum of once a day. f. All organisations transferring records (i.e., DRCs and records custodians) must have a high-speed Internet connection capable of receiving transmitted EM Records. Organisations can utilise alternate locations such as cloud-based storage to receive transmitted records.

SSP2b: EM Records Analysis and Quality Assurance

EM Records analysis is conducted by an **EM Analyst** and is the process of analysing imagery (still images and video) and sensor data recorded by an EM System to produce EM Data. A quality assurance review is the process of verifying and validating a portion of previously analysed EM Records by an **EM Data Quality Reviewer** to determine completeness, adherence to protocols, and accuracy of the EM Data produced by the EM Analyst. These reviews will be conducted internally by the relevant DRC as a quality check.

Activity	SSP
1. EM Records Analysis and Development of EM Data ***NOTE: Item (i) has a placeholder for consideration of a regional template to assist with reporting*	a. EM Analysts will load EM Records from hard drives, local servers, or cloud-based accounts. b. EM Analysts will analyse EM Records in accordance with the regional Longline EM Minimum Data Field Standards, Instructions and Protocols. c. The EM Programme will ensure that the EM records are analysed in accordance with the Coverage and Analysis Rates as determined by the relevant national, sub-regional, or regional programme. d. EM Analysts will conduct analysis of the EM Records in accordance with the defined period as determined by the relevant authority e. EM Analysts will use EM analysis software to analyse EM Records f. EM Analysts will annotate EM Data required according to the latest version of the regional Longline EM Minimum Data Field Standards, Instructions and Protocols. g. EM Analysts shall follow Notes on EM Protocol in the latest version of the regional Longline EM Minimum Data Field Standards. h. EM Analysts will report any issues with EM Records, in accordance with recognized regional EM Analyst training standards. i. EM Analysts will produce a summary report [using the agreed regional format] for each trip and submit the data to the same EM Data platform as analysed data.

2. QA: Verification of EM Data for Accuracy	a. EM Data Quality Reviewer will conduct the systematic quality assurance review by re-analysing a stipulated proportion of the EM Data generated by the EM Analyst, including consideration of coverage and (field) completeness. b. Verification includes a review of a subset of the Minimum EM Data fields as determined by the EM program[13] such as, but not limited to: i. Vessel identification ii. Trip information (i.e., vessel plan) iii. Set and haul information iv. Gear information v. Timestamp accuracy vi. Geolocation accuracy (within 100 metres) vii. Species identification viii. Length frequency measurements ix. Fate determination x. IUU events xi. Compliance violations xii. DRC and reviewer information c. EM review output/report should indicate review protocol, including whether all fields or a specific subset of fields were reviewed, and whether a general compliance review has been conducted. d. EM reviews will be conducted according to agreed protocols.

[13] Programme specification of required information to be verified will be dependent on costs.

3. QA: Validation of EM Data with Other Sources	The purpose of validation is to ensure that EM Data is consistent with other trip data such as VMS, eLogs, and onboard observer reports. Validation should be performed on EM Data using the following analogous, independent sources: a. VMS will be used to validate time and position information. b. Where available, eLogs and observer reports will be used to validate EM Data such as catch and species information as well as violations or compliance issues. c. VMS (and eLogs, where available) will be used to compare vessel and trip information. d. Unloading, transhipment, boarding, and port inspection reports to verify total retained trip catch by species. e. Automated AI analysis, where applicable.

The following draft SSPs on EM Data Quality Reviews for Quality Assurance" and "Third Party Audits" are pending further guidelines to be developed and agreed by the region, and may include consideration of the following:	
4. EM Data Quality Reviews for Quality Assurance	*a. The DRC manager is responsible for the quality of reviews at the DRC.* *b. EM Data Quality Reviews will be conducted for data verification (see above).* *c. EM Data Quality Reviews will be conducted on a random subset of trips for quality assurance.* *d. The regional guideline will specify the share of trips that must go through EM Data Quality Reviews.* *e. EM Data Quality Reviews will be conducted by the same DRC or EM Service Provider that provided the initial analysis.* *f. EM Data Quality Reviews will be conducted by a person other than the one who created the initial analysis.* *g. EM Data Quality Reviews will be done prior to submitting the analysed data.* *h. EM Data Quality Reviews will be conducted at random per regional guidelines and programme specifications.* *i. EM Data Quality Reviews will be performed on an entire set, with the exception of a DRC manager review request and an ETP species interaction review (see below).* *j. A DRC manager may request a partial secondary review for part of a set (this does not count as part of the minimum amount of secondary reviews for a DRC).* *k. All ETP species interaction events must include a secondary review by the DRC manager for any potential compliance events.* *l. EM Data Quality Reviews will happen immediately after the initial review within the timeframe of programme specifications (recommended within one working day) in order to make sure that EM Records are still available for review.* *m. EM Data Quality Reviewers will have the same access to software and EM Records as the primary reviewer.* *n. EM Data Quality Reviewers will not have access to EM Records outside of the selected trip(s) for review.*

5. Third Party Audits	*a. The authorised third-party EM auditor is responsible for conducting periodic audits of DRCs, the EM Analysts, records/data custodians, and analysed data to verify that these specifications and standards are being complied with, and that there is reasonable quality control over all analysed data.* *b. The number of audits, to be planned on an annual basis, will be determined by the [TBD] and the corresponding members based on cost/benefit, logistical, and practical aspects.* *c. Audits will be an independent blind review.* *d. Audits will be performed by a qualified third-party and are the responsibility of the [TBD].* *e. Audit reports will include verification of:* *i. EM software* *ii. Qualified and trained EM Analysts* *iii. Quality control practises* *iv. Correctly formatted analysed data* *v. Data security* *vi. Data verification for accuracy (see above)* *vii. Data validation with other sources (see above)* *f. The DCC will determine the reporting requirements (template, frequency, etc.) for audit reports.*

SSP2c: EM Records and EM Data Storage

These SSPs describe the physical requirements for storage of EM Records and EM Data, including file structure and format. When possible, EM Records and EM Data should be stored in the region including cloud-based storage. EM Records and EM Data may be stored in a regional, sub-regional, or national data centre or cloud-based storage, in accordance with these SSPs. EM Records and EM Data storage capacity is dependent on national requirements for data storage to support legal processes and other national purposes.

Storage Item	SSP
1. EM Records	a. EM Records (still images and videos) must be stored at their original resolution. b. EM Records must be backed up for redundancy in accordance with the relevant IT, or other policy. c. For cloud-based storage, EM Records will be stored in a file structure hierarchy based on vessel, trip, and record type (e.g., camera, sensor). d. EM Records must be tagged accordingly with meta data in the storage system to allow for easy searching.
2. EM Data	a. EM Data must be transferred according to the regional minimum standards for storage in a machine-readable structured file format (i.e. JSON, XML, or CSV). b. EM Data must be stored in a machine readable structured file format such as JSON, XML, or CSV, or in a standard database. c. EM Data must be stored in a cloud-based data platform or a local database. d. EM Data storage must always have a backup available. e. EM Data must be tagged accordingly with meta data in the storage system to allow for easy searching.

SSP3: EM Records and EM Data Ownership and Access

Component	SSP
1. Ownership of EM Records & Data	Ownership is about who ultimately controls the EM Records collected or EM Data that are produced. The Policy specifies that EM Records and EM Data are owned by the licensing FFA member. In general, the same SSPs surrounding ownership are true for both EM Records and EM Data. FFA members will establish arrangements for the ownership of EM Records and EM Data. a. When EM Records (e.g., video) are captured from a vessel in the EEZ of an FFA member, that member is considered to be the Owner of the EM Records and EM Data that are generated from EM Records. b. When EM Records (e.g., video) are captured from a vessel in the High Seas the Flag State is considered to be the Owner of the EM Records and EM Data that are generated from EM Records. c. The Owner of the EM Records and EM Data is identified as [owning the Intellectual Property / copyright of the EM Records and Data and] having the authority to authorise the release and use of EM Records and Data, authorise the sharing of EM Records and EM Data and require that EM Records and externally shared EM Data be destroyed upon completion of the use for which its release was authorised. d. The Owner is responsible for the stewardship of the EM Records and EM Data. e. The Owner is responsible for ensuring that the management of the EM Records and EM Data meets these SSPs. f. The Owner will ensure that there is a record of the receipt of EM Records and Data. g. The Owner will be able to read the EM Records and Data that it owns.
2. Access and sharing arrangements ***NOTE: Item c(vi) requires further consideration of appropriate role and*	Access to data gives an organisation the right to receive and use information, but not to share it with another organisation (which only the Owner can do). Note: Granting access to EM Records does not necessarily grant that same access to the associated EM Data and vice-versa.

designation for "national administrator" and national database. *Item (d)(i) requires further consideration of appropriate approach to provision of software.*	a. The EM Records and EM Data Owner will ensure that when EM Records (e.g., video) are captured from a vessel, the following stakeholders will have Access [on request] to the EM Records and EM Data from that trip: i. Coastal State members within whose EEZs the vessel fished ii. Flag State of that vessel iii. Operator of that vessel b. The EM Records and Data Owner is responsible for providing appropriate access to EM Records. i. Appropriate information (e.g., documentation, advice, etc) describing the information (how it was gathered, processed, stored, strengths, weaknesses, known issues, etc) will be available to third parties who are granted access to the information. ii. The existence of the EM Records will be appropriately publicised, including that appropriate entries describing the information are present in all relevant metadata directories. iii. EM Records and EM Data will be stored/managed in such a way that facilitates their easy transfer from one custodian to a different custodian, including covering the scenario where the custodians are using significantly different technology. iv. The dataset will use standard codes, formats, and ontologies that allow it to be easily matched to, or compared with, other relevant datasets, in particular FFA VMS and FFA Observer Programme data. c. The Custodian must operate an appropriate infrastructure to allow authorised Users access to EM Records and EM Data. i. The Custodian may impose conditions on Users' access to and use of EM Records and EM Data, except that such conditions must not breach any other requirement specified within these SSPs. ii. The EM Records and EM Data Owner must unambiguously inform the Custodian regarding which Users are authorised to receive which EM Records, Ancillary Logs, and EM Data. iii. Users must appropriately authenticate before accessing EM Records / Ancillary Logs and Data.

iv. EM Data will be in the format defined by the DCC longline EM minimum data field standard unless the Custodian and User agree to use an alternative format.

v. The Custodian must log all provisions of EM Records and EM Data to Users. These logs must be stored securely and indefinitely.

vi. The National Administrator [requires discussion on appropriate role or designation] must ensure that a repository (i.e., a National Library (or National Libraries)) [requires discussion on appropriate national database] of original EM Records and Ancillary Logs exists and:

- Is highly secure.
- Allows authorised authenticated users-(e.g., Custodians) to easily control access to read and download EM Records and Ancillary Logs; at the level of the individual file and group of files (e.g., all of those files associated with one trip).
- Allows authorised authenticated users (e.g., Custodians) to easily create new users, including temporary / time-bounded users, and assign those users view / download access rights to EM Records and Ancillary Logs.
- Allows authorised authenticated users (e.g., Users, Data Review Centres) in possession of appropriate passwords to easily view / download the EM Records and Ancillary Logs that they have been assigned access rights to, including allowing the easy downloading in-bulk of all of the EM Records and Ancillary Logs for one trip.

vii. The Records Custodian must provide EM Records / Ancillary Logs to the User by granting the user access to those records / logs within the National Library of original EM Records and Ancillary Logs, unless the Custodian and User parties agree to use an alternative mechanism (e.g., the provision of a fragment of video in a commonly readable format).

d. The EM Service Provider must operate an appropriate infrastructure that allows authorised Users to easily view EM Records and Ancillary Logs stored in their proprietary format.

	i. The EM Service Provider, must offer authorised Users [free] [requires discussion on appropriate requirement] access to software allowing the User to easily view EM Records and Ancillary Logs stored in their proprietary format.
3. Retention and Disposal **NOTE: Item (a)(i) requires further discussion pending development of regional and national EM legal frameworks.	Any longline fisheries EM programme can be expected to collect vast quantities of video, and this video will be expensive to store. Video needs to be retained for long enough to ensure that members can obtain the value / use out of it that they require, but not so long that retaining the video becomes a significant cost burden. Please see the Retention and Disposal section of the SSP 3 and 4 Report for further information on how these draft SSPs address issues around Retention and Disposal of EM Records and EM Data. a. Regarding the EM Records: i. The Custodian will ensure that EM Records will be securely stored and held for a minimum of six months [once analysis has occurred/6 months/6 months from the date the EM Record was last reviewed/1 year/2 years/5 years]. [determined by national programme requirements on data retention and storage cost implications] ii. The Custodian will ensure that If the review of the EM Records identified a potential infringement or anything of concern, all footage related to that trip will be kept until the Records Owner has given explicit instruction for disposal (taking into account any requests from Users for continued use of the Records for investigation or prosecution purposes for any Records from that trip). iii. Media containing sensitive information such as hard drives will be stored and disposed of securely and safely. iv. Disposal of sensitive items such as hard drives will be logged in order to maintain an audit trail. v. After an exact copy of the EM Records on a data drive has been made, the data drive can be reformatted ready for use again. b. Regarding EM Data

	i. EM Data will be safeguarded against loss due to long-term technology change (e.g., changes in storage formats, changes in storage media, etc).

SSP 4: EM Records and EM Data – Security and Confidentiality

Component	SSP
1. Security	Information Security involves the preservation of three aspects of information: Confidentiality (ensuring that the information is accessible only to authorised individuals), Integrity (safeguarding the accuracy and completeness of information and processing methods) and Availability (ensuring that authorised users have access to relevant information when required). Because there are over 100 of these standards, the detailed standards are included in Annex 1. Please see the Security section of the SSP 3 and 4 Report for further information on how these draft SSPs address issues around Security of EM Records and EM Data. All of the entities involved with the EM Programme must work together to ensure that EM Data and EM Records are secured against the three information security risk management criteria of confidentiality, integrity and availability. Entities involved with the EM Programme must ensure: a. The physical security of EM Records and EM Data (e.g., by the use of perimeters to control access to areas where EM Records and EM Data are created or stored) as specified in SSPs 4.1.a of Annex 1 b. The operational security of EM Records and EM Data (i.e., protection from damage by fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster) as specified in SSPs 4.1.b of Annex 1. c. The communications security of EM Records and EM Data as specified in SSPs 4.1.c of Annex 1. i. The network security of EM Records and EM Data (i.e., networks will be adequately managed and controlled).

	ii. The security of physical media in transit (e.g., hard drives containing EM Records) as specified in SSPs 4.1.c.ii of Annex 1. iii. The security of EM Records and EM Data in transit by electronic means as specified in SSPs 4.1.c.iii of Annex 1. d. The procedural security of EM Records and EM Data (i.e., Procedures will be in place to control the allocation of access rights to information systems and services) as specified in SSPs 4.1.d of Annex 1. e. The computer system security of EM Records and EM Data (i.e., detection, prevention, and recovery controls to protect against malicious code) as specified in SSPs 4.1.e of Annex 1. f. The application security of EM Data and EM Records through correct installation and maintenance of applications and equipment as specified in SSPs 4.1.f of Annex 1. g. The integrity of the process by which EM Data is generated as specified in SSPs 4.1.g of Annex 1.
2. Confidentiality ***NOTE: Item (a)(iii) requires discussion on the utility of having a standard NDA template to support this requirement.* *Item (a)(vi) requires further discussion pending development of national and regional EM legal frameworks.*	Confidentiality is about ensuring that the information is accessible only to authorised individuals. Please see the Confidentiality section of the SSP 3 and 4 Reference Report for further information on how these draft SSPs address Confidentiality of EM Records and EM Data. a. The EM Programme must maintain confidentiality (the need to ensure that information is accessible only to those authorised to have access) of EM Records and EM Data i. The EM Service Provider will ensure that Records are encrypted to protect confidentiality of Records either stored or transmitted (see also standards in the SSP 4.4 Evidential Integrity and Chain of Custody section). ii. EM Records and EM Data may only be accessed if the Owner authorises their release. iii. Confidentiality provisions and a non-disclosure agreement will be used to protect EM Records and EM Data and the Custodian will inform signatories of their responsibility to protect, use, and disclose information in a responsible and authorised manner. iv. Users who are authorised to access a Owner's EM Records or EM Data must agree to be bound by the confidentiality agreement. v. Users will not disseminate information they are authorised to access to another party.

	vi. The Custodian will ensure that Media containing EM Records and EM Data will be stored and disposed of securely and safely for a minimum of XX years or in accordance with Member's national law (see also standards for Physical Security). vii. The Custodian will ensure that If no longer required, the contents of any re-usable media will be made unrecoverable (see also standards for SSP 3.3 Retention and Disposal). viii. The laws of countries in which EM Records and EM Data are stored / processed / transmitted could affect the privacy and confidentiality of the EM Records and EM Data they store. Any EM Records or EM Data stored / processed / transmitted may be subject to the privacy and data protection laws of those countries in which this occurs. The use of cloud computing services introduces particular data sovereignty risks.
3. Privacy ***NOTE: Item (a)(i) requires further discussion on appropriate approach to addressing privacy concerns.*	Privacy is about the restriction of access to, and appropriate use of, personal information of crew or observers seen in images. Please see the Privacy section of the SSP 3 and 4 Report for further information on how these draft SSPs address the issue of Privacy for EM Records and EM Data. a. The EM Programme must maintain the privacy (the restriction of access and appropriate use of personal information) of crew or observers seen in images. i. [The Programme Provider [or appropriate role] will ensure that a [vessel specific] Privacy Impact Assessment is done to identify the concerns of vessel operators.] [programmes could also have a Privacy Protocols Policy or similar] ii. The EM Service Provider will ensure that cameras focus on fish and fishing activities not at the crew or at observers and as far as possible should not intrude on individual privacy or private areas and be consistent with the recommendations of the Privacy Impact Assessment. iii. The EM Service Provider will ensure that wherever possible, while data collection requirements are met, sensor data will be used to determine when to record images during a day so that only fishing operations are recorded. iv. The Vessel Operator will ensure that all other privacy laws to which the vessel is subject (for example if a vessel is flagged to or fishing in a nation that requires affirmative consent to release of private information) will be complied with.

	v. Where possible, crew and observer faces should not be visible in still or video images that are released into the public domain, (e.g., through blanking out of parts of images to protect persons), unless the retention of these features are required to support the purpose for which the footage is released. vi. EM Data in the public domain shall not reveal the individual activities of any vessel, company or person and shall not contain private information.
4. Evidential Integrity and Chain of Custody _**NOTE: Item (a)(v-vi) requires further discussion on level of redundancy and cloning abilities, noting that EM systems do not currently store backups and are not set up for cloning records. There are also cost implications._	Evidential Integrity and Chain of Custody are about establishing that there has been no alteration, substitution, or change in the condition of EM Records from the time of their creation to the time they are admitted at a trial or proceeding. Because one FFA member may need to rely on EM Records collected by a different FFA member, it is important that Evidential Integrity and Chain of Custody procedures are regionally harmonised. Please see the Evidential Integrity and Chain of Custody section of the SSP 3 and 4 Summary Report for further information. The SSPs presented below are Low Specificity. Low Specificity SSPs are simpler and would require fewer changes to existing national EM programmes, but delay resolving issues of inter-programme coordination which will probably need to be addressed at a later stage. Examples of alternative High Specificity SSPs for evidential integrity / chain of custody can be found in Annex 2. Four of the draft Low Specificity SSPs are presented as optional. a. FFA members will use a harmonised approach to ensure that EM Records are of evidential quality, including in other member's courts. i. The onboard EM System (hardware, software, and settings) must be tamper-resistant and/or tamper-evident, such that the EM Records that it produces can reliably be used in all FFA member's judicial proceedings. ii. The Vessel Operator / Crew must not interfere with, and must actively facilitate, the correct operation of the onboard EM System. iii. FFA members will adopt a regionally harmonised infrastructure (e.g., an online register) which stores details of each onboard EM System operating in the region and allows FFA members to view these details.

iv. The onboard EM System must capture ancillary information that prove the origin and truthfulness of the EM Records that it produces including:

- A list of the EM Records that it creates; and
- A list of the EM Records that it packages for submission; and
- Information on the health of the onboard EM equipment (including power up/down events); and
- The makes, models and serial numbers of the sensors used to collect EM Records

v. [The onboard EM System must provide the capability for authorised enforcement officers who board the vessel to view and forensically clone the EM Records and ancillary information present.]

vi. [The onboard EM System must automatically store a complete backup copy of all EM Records submitted and allow the Vessel Operator / Crew to delete the backup copy after the successful receipt of the originals is confirmed.]

vii. Onboard EM System Providers must appropriately encrypt EM Records and ancillary information (e.g., logs), and operate a secure infrastructure to supply decryption keys to FFA members, such that only appropriately authorised people can view or alter EM Records.

viii. When submitting EM Records, Vessel Operators / Crew must use a reputable delivery mechanism which at all times documents the person in possession/control of those records.

ix. FFA members will adopt regionally harmonised procedures to ensure that, in those cases where EM Records come ashore in a country other than the FFA member which owns them, such records are efficiently and securely transported to the owner.

x. FFA members will adopt a regionally harmonised infrastructure (e.g., an online system) which allows Vessel Operators / Crew to log their submission of EM Records, Vessel Operators / Crew and FFA members to monitor the movement of such records, and FFA members to confirm their receipt of these.

xi. Upon receiving EM Records due to them, FFA members or their authorised representatives should promptly: verify that these are complete and readable, [and confirm their receipt,] and store an evidential quality copy of the originals.

Annex to SSP 4.1 Security - Additional details for SSPs (originally Annex 1)

Component	Highly Specific SSP
SSP 4.1 a *Entities involved with the EM Programme must ensure the physical security of EM Records and EM Data (e.g., by the use of perimeters to control access to areas where EM Records and EM Data are created or stored).*	i. Camera and control housings will be secure and suitably protected against unauthorised access. ii. If Storage Media are left unattended at any time, it must be in a location that is in a secure area, protected by defined security perimeters, with appropriate security barriers and entry controls. iii. Any site at which EM Records or EM Data are stored, analysed or viewed must be in a secure area protected by defined security perimeters with appropriate security barriers. iv. Any site at which EM Records or EM Data are stored, analysed or viewed must be in a secure area that is restricted to authorised personnel only. v. All storage media will be stored in a safe, secure environment, in accordance with manufacturers' specifications.
SSP 4.1 b *Entities involved with the EM Programme must ensure the operational security of EM Records and EM Data (i.e. protection from damage by fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster)*	i. Controls will be adopted to minimise the risk of potential physical threats, e.g., theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interference, communications interference, and vandalism. ii. Appropriate fire fighting equipment will be provided and suitably placed. iii. Equipment will be protected from power failures and other disruptions caused by failures in supporting utilities. All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning will be adequate for the systems they are supporting. iv. An uninterruptible power supply (UPS) to support orderly close down or continuous running will be used for equipment supporting critical business operations. v. Power contingency plans will cover the action to be taken on failure of the UPS. vi. At all times during a fishing trip, there will be a regular EM system health check confirming that the onboard system is functioning normally.

	vii. The System Health Monitor will ensure that if the EM system health check indicates abnormal function that appropriate remedial action is taken, including communicating with the vessel, the Programme Provider, the Onboard Systems Provider and the Regional Programme Office as required. viii. Any breakdowns or security issues will be reported immediately to the EM Programme Provider, and any follow up actions taken as instructed. ix. The extent (e.g., full or differential backup) and frequency of backups will reflect the criticality of the information to the continued operation of the EM programme. x. Back-up information will be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site will be extended to cover the backup site. xi. Back-up media will be sited at a safe distance to avoid damage from a disaster affecting the main site. xii. Back-up media will be regularly tested to ensure that they can be relied upon for emergency use when necessary. xiii. Restoration procedures will be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery. xiv. Backups will be owned by the owner of the information being backed up.
SSP 4.1 c *Entities involved with the EM Programme must ensure the network security of EM Records and EM Data (i.e. networks will be adequately managed and controlled)*	i. Controls will be implemented to ensure the security of information in networks, and the protection of connected services from unauthorised access. ii. Special controls will be established to safeguard the confidentiality and integrity of information passing over public networks or over wireless networks. iii. Appropriate logging and monitoring will be applied to enable recording of security relevant actions.
SSP 4.1 c.ii *Entities involved with the EM Programme must ensure*	a. If possible, possession of physical media will be transferred directly from one authorised person to the recipient or their agent and receipt will be registered.

the security of physical media in transit (e.g, hard drives containing EM Records).	b. If it is not possible to transfer possession directly to the recipient, reliable agents or couriers will be used, from a list agreed with the Programme Provider. c. The identification of agents/couriers will be confirmed before they take possession of physical media. d. Receipt of physical media will be logged and acknowledged. e. If no acknowledgement is received, the Programme Provider will be alerted to a possible security issue. f. Packaging will be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g., for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields. g. Tamper-evident packaging (which reveals any attempt to gain access) will be used while physical media are in transit. h. Equipment and media taken off the premises will not be left unattended in public places.
SSP 4.1 c.iii *Entities involved with the EM Programme must ensure the security of EM Records and EM Data in transit by electronic means*	a. If EM Data and EM Records are transmitted by electronic means, the information must be protected from unauthorised access, misuse or corruption during transmission, for example by appropriate cryptographic controls. b. If EM Data or EM Records are transmitted by electronic means, the recipient must log receipt. c. If no acknowledgement of secure receipt of EM Record or Data transmission is received, the Programme Provider will be alerted to a possible security issue. d. If EM Data or EM Records are transmitted by electronic means, the sender must retain a copy of all records until receipt has been acknowledged.
SSP 4.1 d *Entities involved with the EM Programme must ensure the procedural security of EM Records and EM Data (i.e. Procedures will be in place to control the*	i. Care will be taken that no single person can access, modify or use EM Data and EM Records without authorization or detection. ii. People on the vessel will not interfere with the proper functioning of the EM System in any way, including by moving cameras, altering the angle of cameras, obstructing cameras, altering timestamps, offsetting GPS readings, etc. iii. There will be formal user registration and deregistration procedures in place for granting and revoking access to EM Data and EM Records information systems and services.

allocation of access rights to information systems and services.)	iv.]Multi-user systems that require protection against unauthorised access will have the allocation of privileges controlled through a formal authorization process. v. Privileges will be allocated to users on a need-to-use basis in line with the access control policy i.e. the minimum requirement for their functional role only when needed. vi. An authorization process and a record of all privileges allocated will be maintained, and privileges will not be granted until the authorization process is complete. vii. Users will be required to sign a statement that they will keep personal passwords confidential. viii. Procedures will be established to verify the identity of a user prior to providing a new, replacement or temporary password. ix. Users will be required to follow good security practices in the selection and use of passwords. x. All users will have a unique identifier (user ID) for their personal use only, and a suitable authentication technique will be chosen to substantiate the claimed identity of a user. This control will be applied for all types of users. User IDs will be used to trace activities to the responsible individual. xi. Audit logs recording user activities, exceptions, and information security events will be produced and kept for an agreed period to assist in future investigations and access control monitoring. xii. User access to applications working with EM Data and EM Records functions will be controlled in accordance with a defined access control policy. xiii. Security responsibilities will be addressed prior to employment in adequate job descriptions and in terms and conditions of employment, addressing in particular any issues regarding conflict of interest. xiv. All employees, contractors and third party users understand their security responsibilities and be suitable for the roles they are employed in, in order to reduce the risk of theft, fraud or misuse of facilities. xv. Employees will sign an agreement on their security roles and responsibilities. xvi. All employees and, where relevant, other users will receive appropriate training and regular updates in policies and procedures, as relevant for their job function.
SSP 4.1 e *Entities involved with the EM Programme must ensure*	i. Appropriate controls exist to ensure that unauthorised software cannot be loaded onto computers.

the computer system security of EM Records and EM Data (i.e. detection, prevention, and recovery controls to protect against malicious code).	ii. A formal policy will be established to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures will be taken. iii. Regular reviews of the software and data content of systems supporting critical business processes will be conducted and the presence of any unapproved files or unauthorised amendments will be formally investigated. iv. Malicious code detection and repair software will be installed and regularly updated to scan computers and media as a precautionary control, or on a routine basis. v. Management procedures and responsibilities will be developed to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks. vi. Business continuity plans will be developed for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements. vii. Procedures will be implemented to regularly collect information about new malicious code, such as subscribing to relevant mailing lists and/or checking relevant websites. viii. Procedures will be implemented to verify information relating to malicious code, and ensure that warning bulletins are accurate and informative. Managers will ensure that qualified sources (e.g., reputable journals, reliable Internet sites or suppliers producing software protecting against malicious code) are used to differentiate between hoaxes and real malicious code. All users will be made aware of the problem of hoaxes and what to do on receipt of them. ix. If Information management services are outsourced, for example by using Cloud computing, suitable assessment must be done to ensure that information systems have been deployed with sufficient controls to protect the confidentiality, integrity and availability of the EM Data and EM Records they store, process and transmit before accrediting them for use.
SSP 4.1 f *Entities involved with the EM Programme must ensure the application security of EM Data and EM Records*	i. Only approved Onboard EM System equipment and software will be used, provided by the Onboard Systems Provider. ii. Noting that under IMO resolution MSC.428(98) an approved safety management system for vessels should take into account cyber risk management in accordance with the objectives and functional

through correct installation and maintenance of applications and equipment.	requirements of the International Safety Management (ISM) Code, cyber risks relating to EM systems on board the vessel must be appropriately addressed. iii. Installation/Maintenance Technicians will ensure that EM programme onboard equipment will be installed, configured and integrated into other systems in accordance with the supplier's recommended practices. iv. Only authorised Installation/Maintenance Technicians will install and configure onboard EM systems. v. EM onboard equipment will be maintained in accordance with the Onboard Systems Provider's recommended service intervals and specifications. vi. Only authorised Installation/Maintenance Technicians will carry out repairs to and service onboard EM systems. vii. Vessel operators will ensure that the Onboard EM Systems continue to function as required (for example wiping lenses) as instructed by the Onboard Systems Provider or by the Programme Provider. viii. Only approved DRC System equipment and software will be used, provided by the DRC Systems Provider. ix. Records will be kept of all suspected or actual faults, and all preventive and corrective maintenance. x. Appropriate controls will be implemented when equipment is scheduled for maintenance. xi. The correct setting of computer clocks is important to ensure the accuracy of audit logs. Therefore, where a computer or communications device has the capability to operate a real-time clock, this clock will be set to an agreed standard (including recording of time zone). xii. Software patches will be applied when they can help to remove or reduce security weaknesses. xiii. EM Data and EM Records processing and operating system software will only be implemented after extensive and successful testing; the tests will include tests on usability, security, effects on other systems and user-friendliness.
SSP 4.1 g *Entities involved with the EM Programme must ensure the integrity of the process*	i. The Data Review Centre will be selected by the Programme provider to analyse EM Records and generate EM Data for the Data Owner. ii. The Data Review Centre will analyse the EM Records, generate EM Data, and supply this using correct protocols to the Data Custodian for long term storage and dissemination.

by which EM Data is generated.	iii. The Data Review Centre will use approved software supplied by the DRC System Provider to generate EM Data. iv. Appropriate checks will be applied to ensure the integrity, authenticity, completeness or any other security feature of EM Records uploaded. v. Reconciliation control counts will ensure processing of all relevant EM Records. vi. EM Data will be generated according to EM Data Standards to ensure the integrity of the dataset of EM Data. vii. EM Data will be generated by qualified EM Analysts only in order to ensure the integrity of the dataset of EM Data. viii. EM Data will be validated (e.g., cross-referencing with recognized other sources) to ensure its integrity. ix. S7.9: Plausibility checks will test whether the EM Data generated is reasonable. x. There will be procedures for responding to validation errors on EM Data. xi. A log will be kept of the activities involved in the processing of EM Records and generation of EM Data. xii. Logs will provide sufficient information for a reader or subsequent processing system to identify who generated the EM Data and to determine the accuracy, completeness, precision, and classification of the EM Data generated. xiii. Any breakdowns or security issues will be reported immediately to the EM Programme Provider, and any follow up actions taken as instructed. xiv. Security logs and other evidence will be provided to the EM Programme Provider in the event that there is any need for an investigation. xv. Any errors in the EM Data reported by the Custodian or a User will be investigated and if necessary corrected by regenerating and transferring the revised EM Data. xvi. If the EM Data generation process is repeated (either as an independent check or to correct errors), it will be done following standard protocols and the different versions of the EM Data will be identified using version control.

Annex to SSP 4.4 - Example of Highly Specific Evidential Integrity and Chain of Custody SSP (originally Annex 2)

Component	Highly Specific SSP
SSP 4.4 a.i *The onboard EM System (hardware, software, and settings) must be tamper-resistant and/or tamper-evident, such that the EM Records that it produces can reliably be used in all FFA member's judicial proceedings.*	a. Onboard EM Systems must set their internal UTC date and UTC time, as used in EM Records and Ancillary Logs, from the GPS signals that they receive. b. Onboard EM Systems must be tamper-evident and designed such that attempts at unauthorised modification, whether to hardware or software or settings, are difficult to hide.
SSP 4.4 a.ii *The Vessel Operator / Crew must not interfere with, and must actively facilitate, the correct operation of the onboard EM System.* ***NOTE: Role of "National Administrator" requires further discussion and clarification.*	a. The National Administrator must ensure that an enforceable requirement for Vessel Operators / Crew to: a. not interfere with the correct operation of Onboard EM System exists and prohibits: ● Tampering with, or hindering the operation of, the Onboard EM System; including hardware, software, and settings. ● Tampering with, or hindering the operation of, the power supply for the Onboard EM System; ● Altering EM Records or Ancillary Logs in any way, including substituting, modifying, deleting, or renaming the files. b. Check the correct operation of Onboard EM System exists and requires the crew to: ● Regularly run an Onboard EM System health check. ● Regularly check the power supply to the Onboard EM System.

	● Regularly verify that EM Records are being correctly written to Storage Media, that the viewing angle of cameras has not been altered from the initial set-up, that cameras are unobstructed and have a clear view, that camera lenses are clear, and that the area cameras are viewing is appropriately lit. c. Report to the Programme Provider: ● Any possible attempts that they detect to interfere with the correct operation of the Onboard EM System. ● Any issues that they detect with the health of the Onboard EM System. ● Any issues that they detect with the power supply for the Onboard EM System. ● Any issues that they detect with EM Records not being correctly written to Storage Media. d. Check, before leaving port, that adequate recording space is available on Onboard EM System primary Storage Media and backup Storage Media.
SSP 4.4 a.iii *FFA members will adopt a regionally harmonised infrastructure (e.g., an online register) which stores details of each onboard EM System operating in the region and allows FFA members to view these details.* **NOTE: Item (a) is dependent on decisions on	a. The Regional Programme Office must ensure that a secure Regional EM Programme Installation Database exists, is appropriately accessible to the National Administrator of each FFA member country, and stores details of the Onboard EM System installed on each vessel participating in the regional EM programme, including: ● The Installation / Maintenance Technicians ID, Vessel ID, the date of completion of installation / modification, the place of installation / modification. ● The placement, makes, models and serial numbers of the central control centre hardware. ● The names and version numbers of software installed on the control centre. ● The placement, makes, models, serial numbers, system ID and MAC address of each camera / sensor. ● A photograph illustrating the viewing angle for each camera. ● The makes, models, and serial numbers of all Storage Media (e.g., disk drives) installed at the time.

the EM regional programme structure *Item (b) requires clarification on role of "Programme Provider"* *Item (c) has a placeholder for appropriate number of hours in which information is to be logged into the Regional EM Programme Installation Database.*	b. The Programme Provider must ensure that all installations of, or substantive modifications to, Onboard EM Systems are carried out by authenticated authorised Installation / maintenance technicians. c. The Programme Provider must ensure that all installations of, or substantial modifications to, Onboard EM Systems must be fully logged in the Regional EM Programme Installation Database within XX hours of being completed.
SSP 4.4 a.iv *The onboard EM System must capture ancillary information that prove the origin and truthfulness of the EM Records that it produces including:* ● *A list of the EM Records that it creates; and* ● *A list of the EM Records that it packages for submission; and* ● *Information on the health of the onboard EM equipment*	a. Onboard EM Systems must imprint Vessel ID, Camera ID, UTC date, and UTC time of recording onto all images recorded; while not obscuring those parts of the recorded image where activities of interest are most likely to occur. b. Onboard EM Systems must automatically generate Ancillary Logs sufficient to allow the reader of the log to easily identify the following events: ● The creation, by the Onboard EM System, of any EM Record. The log detail must include the name of the file that the EM Record was written into and the ID of the camera that the EM Record was recorded on. ● The packaging of EM Records for submission by the Onboard EM System to an FFA member country. ● Any power-up or power-down of the Control Centre. ● Any changes in Onboard EM System hardware (e.g., Control Centre, Camera, Storage Media) or software that occur. The log detail must include the following ■ the make of the hardware ■ model ■ serial number ■ system ID of

(including power up/down events); and ● *The makes, models and serial numbers of the sensors used to collect EM Records*	■ name and version of any new or updated software ● Any changes in Control Centre system settings that occur. The log detail must include the name of the setting, the old setting value, the new setting value, and the identity of the person that made the change. ● A summary of the results of any system health checks performed. The log detail must include the names of the files in the package and the serial number of the Storage Media that these were written to.
SSP 4.4 a.v *[The onboard EM System must provide the capability for authorised enforcement officers who board the vessel to view and forensically clone the EM Records and ancillary information present.]*	a. Onboard EM Systems must provide the capability for authorised enforcement officers, in possession of the appropriate decryption keys, who board the vessel to view EM Records and Ancillary Logs. b. Onboard EM Systems must provide the capability for authorised enforcement officers who board the vessel to forensically clone the full set of EM Records and Ancillary Logs present on Storage Media.
SSP 4.4 a.vi *[The onboard EM System must automatically store a complete backup copy of all EM Records submitted and allow the Vessel Operator / Crew to delete the backup copy after the successful*	a. Onboard EM Systems must allow vessel crew to easily retain a backup copy of all EM Records and associated Ancillary Logs submitted to a FFA member country. b. Onboard EM Systems must allow vessel crew to delete the backup copy of all EM Records and associated Ancillary Logs submitted to a FFA member country (once a Confirmation-of-Submission is received from that FFA member country). c. The National Administrator must ensure that an enforceable requirement exists for Vessel Operators / Crew to retain a copy of the submitted EM Records and Ancillary Logs until a Confirmation-of-Submission is received.

receipt of the originals is confirmed.]	
SSP 4.4 a.vii *Onboard EM System Providers must appropriately encrypt EM Records and ancillary information (e.g., logs), and operate a secure infrastructure to supply decryption keys to FFA members, such that only appropriately authorised people can view or alter EM Records.* _**NOTE: Item (d) has a placeholder for further consideration of encryption key format._ *Items (k) and (o) have placeholders for determining the appropriate number of hours for supplying the encryption key when a trip is ongoing or complete.*	a. Onboard EM Systems must automatically generate a Trip ID which identifies all of the events that occurred on the vessel between a known start datetime and a known end datetime. b. Onboard EM Systems must provide the capability for the vessel crew to easily view the Trip ID. c. Onboard EM Systems must encrypt all EM Records and Ancillary Logs using an encryption algorithm that: ● Is one of those specified in ISO/IEC 18033-3:2010; and ● Is a symmetric encipherment system (i.e., the same key is used for encryption and decryption); and ● Has the property that if a file is encrypted with key AAA, then the encrypted file is altered in any way, then decrypting the file with key AAA (or any other key) will fail in an obvious manner. d. Onboard EM Systems must encrypt all EM Records and Ancillary Logs using an encryption key that is at least XX characters long, complex, and changes with each trip. e. Onboard EM Systems must name EM Records and Ancillary Logs using the FFA Regional EM Programme standard for file names. f. Onboard System Providers must retain, indefinitely and in a highly secure manner, details of the EM Record decryption keys used by their Control Centres. g. Onboard System Providers must restrict access to EM Record decryption keys to a very small number (e.g., two) of their staff and no one else other than as described within these SSPs. h. Onboard System Providers must appropriately authenticate the staff of National Administrators to whom it is supplying EM Record decryption keys. i. Onboard System Providers must supply details of the method used by their Control Centres to encrypt EM Records to appropriately authorised staff of the National Administrator for a FFA member. These details must be adequate to allow a person in possession of the appropriate decryption key to decrypt the EM Records and Ancillary Logs for a trip. j. Prior to successfully loading the EM Records for a trip into their National Library of original EM Records, the National Administrator must restrict access to EM Record decryption keys to a very small number

	(e.g., two) appropriately authorised staff of their organisation, or staff of their Records Verification Agent(s), and to no one else other than as described within these SSPs. k. For a trip that is ongoing or complete, Onboard System Providers must supply (in a highly secure manner and within XX hours of being requested to do so by appropriately authorised staff of the National Administrator for a FFA member) the key that can be used to decrypt EM Records describing events that occurred outside of any FFA member country's EEZ. l. Onboard EM Systems must automatically change the files that EM Records and Ancillary Logs are written to if the EEZ that the vessel is in changes. m. Onboard EM Systems must encrypt EM Records and Ancillary Logs describing events which occurred inside of a FFA member country's EEZ using an encryption key that is unique to that FFA member country. n. Onboard EM Systems must encrypt EM Records and Ancillary Logs describing events which occurred outside of any FFA member country's EEZ using an encryption key that is unique. o. For a trip that is ongoing or complete, Onboard System Providers must supply (in a highly secure manner and within XX hours of being requested to do so by appropriately authorised staff of the National Administrator for a FFA member) the key that can be used to decrypt EM Records describing events that occurred within that countries EEZ.
SSP 4.4 a.ix *FFA members will adopt regionally harmonised procedures to ensure that, in those cases where EM Records come ashore in a country other than the FFA member which owns them, such records are efficiently and securely transported to the owner.*	a. The Regional Programme Office must ensure that a Regional EM Programme standard for naming EM Record and Integrity Log files exists and that the names of EM Records and Ancillary Logs include: the name of the Onboard System Providers, the vessel ID, and the Trip ID, and the ISO 3166-1 alpha-3 letter Country Code for the FFA member country within whose waters the events described in the file occurred (or "GEN" for events that occurred outside of any FFA member country's EEZ). b. EM Records / Ancillary Logs must be stored in a highly secure place immediately upon receipt. c. Anyone with access to EM Record decryption keys must not also have access to the EM Records / Ancillary Logs that it is storing.

**NOTE: Item (a) requires further consideration of appropriate designation. _Items (d-g) require further consideration of level of detail required._	d. EM Records and Ancillary Logs must, within XX hours of receiving EM Records / Ancillary Logs, be loaded into *** where *** - as an exact copy (e.g., as encrypted by the vessel's control centre, at their as-received size, in their native format, and retaining their as-received file names). *** Note – EI11.4 requires that each Coastal State keep an exact copy of its EM Records. The option shown above would be required if FFA member countries wanted to adopt a model whereby an additional copy of all of the EM Records from a single multi-EEZ trip were also stored together in one place. e. A Records Dissemination Agent must, within XX hours of receiving EM Records / Ancillary Logs and in a highly secure and reliable manner, transmit to the Records Verification Agent nominated by the owning FFA member country the EM Records and country specific Ancillary Logs due to that country, and all general Ancillary Logs, as identified by their file names. f. A Records Dissemination Agent must, within XX hours of receiving EM Records / Ancillary Logs and in a highly secure and reliable manner, transmit to the *** where *** the EM Records and Ancillary Logs not due to any single FFA member country (e.g., EM Records describing fishing on the high seas) as identified by their file names. *** Note – dependent on decision regarding where high seas EM Records will be stored. g. EI9.7: A Records Dissemination Agent must, when transmitting EM Records / Ancillary Logs, send either the original EM Records / Ancillary Logs received or an exact copy (as encrypted by the vessel's control centre, at their as-received size, in their native format, retaining their as-received file names) of the originals received.
SSP 4.4 a.x _[FFA members will adopt a regionally harmonised infrastructure (e.g., an online system) which allows Vessel Operators / Crew to log their submission of EM_	a. The Regional Programme Office must ensure that a Regional EM Programme Submission Logging System exists and: ● Takes the form of a website and web service, both connected to the same database of EM Record submission / receipt ● Is highly secure

Records, Vessel Operators / Crew and FFA members to monitor the movement of such records, and FFA members to confirm their receipt of these.] **NOTE: The last bullet point in Item (a) requires further consideration of the appropriate definition or description of how/where EM Records will be stored at the national level. *Items (f) and (h) has a placeholder for the number of hours for which receipts of EM Records/Ancillary Logs should be logged in the Regional system.*	● Allows Vessel Operators / Crew to log their submission of EM Records. This will include logging details of the submission mechanism, Vessel ID, and FFA members within whose EEZ's the trip occurred. ● Notifies the National Administrator for each FFA member within whose EEZ the trip occurred that a submission has been logged. ● Allows the National Administrator for each FFA member to specify where the EM Records (describing events in waters under that member's jurisdiction) for a given fishing trip should be sent to, noting that this could be an ongoing specification for all trips. ● Allows parties on behalf of FFA members to confirm their successful receipt of readable EM Records and Ancillary Logs. ● Allows the National Administrator for each FFA member country to specify which National Library should store the EM Records (describing events in waters under that member's jurisdiction) for a given fishing trip, noting that this could be an ongoing specification for all trips. b. The National Administrator must ensure that an enforceable requirement exists for Vessel Operators / Crew to log their submission of EM Records on the Regional EM Programme Submission Logging System. c. The National Administrator must ensure that EM Records and Ancillary Logs are not considered submitted until it lodges a Confirmation-of-Submission on the Regional EM Programme Submission Logging System. d. The National Administrator must ensure that an enforceable requirement exists for Vessel Operators / Crew to regularly monitor the Regional EM Programme Submission Logging System, to ensure that their submission of EM Records and Ancillary Logs is successful. e. A National Administrator must, within XX hours of a Vessel Operators / Crew logging their submission of EM Records / Ancillary Logs in the Regional EM Programme Submission Logging System, specify in the system: ● Where/Who the EM Records / Ancillary Logs should be sent; and ● The National Library in which the original EM Records and Ancillary Logs should be stored - noting that nothing prevents these from being an ongoing specification of a single destination. f. Within XX hours of receiving EM Records / Ancillary Logs, the receipt must be logged in the Regional EM Programme Submission Logging System.

	g. Immediately after checking EM Records / Ancillary Logs, the results of these checks must be recorded in the Regional EM Programme Submission Logging System and a Confirmation-of-Submission issued if no significant problems were identified. h. Within XX hours of receiving EM Records / Ancillary Logs, the receipt must be logged in the Regional EM Programme Submission Logging System. i. Immediately after transmitting EM Records / Ancillary Logs, the transmission must be recorded in the Regional EM Programme Submission Logging System.
SSP 4.4 a.xi *Upon receiving EM Records due to them, FFA members or their authorised representatives should promptly: verify that these are complete and readable, [and confirm their receipt,] and store an evidential quality copy of the originals.* ***NOTE: Items (d) and (e) have placeholders for determining appropriate hours, days, and percentages.*	a. The National Administrator must authorise a person(s) or organisation to assess, and accept / decline on its behalf, all EM Records and Ancillary Logs transmitted to it. b. The National Administrator must ensure that a National Library (or National Libraries) of original EM Records and Ancillary Logs exists and: ● Is highly secure. ● Automatically logs all actions involving EM Records and Ancillary Logs and does not allow any user to modify or delete these logs. ● Allows authorised authenticated users to write EM Records and Ancillary Logs into it. ● Does not allow any user to modify the EM Records and Ancillary Logs stored into it. ● Allows authorised authenticated users to delete EM Records and Ancillary Logs stored into it (e.g., in accordance with SSPs for EM Record Retention and Disposal). ● Can handle the storage of multiple versions of the same EM Records and Ancillary Logs. *** Note – these SSPs allow for the possibility that each FFA member country's National Library of original EM Records could be a ring-fenced area in a shared piece of regional infrastructure c. Immediately store EM Records / Ancillary Logs in a highly secure place upon receipt d. Within XX hours of receiving EM Records / Ancillary Logs, load an exact copy (e.g., as encrypted by the vessel's control centre, at their as-received size, in their native format, and retaining their as-received file names) of EM Records and Ancillary Logs received into the National Library of original EM Records and Ancillary Logs.

	e. Within X days of receiving EM Records / Ancillary Logs: ● Check that all of the EM Records / Ancillary Logs relevant to it (as identified by their file names) can be decrypted using the appropriate key; and ● Check that all of the EM Records which are expected to be present (as described in the Ancillary Logs) are present; and ● Check the EM Records and Ancillary Logs for viruses / malware; and ● Check XX% of the content of the decrypted EM Records to ensure that these are viewable.