NATO Communications and Information Agency
Agence OTAN d’information et de communication

RFQ-CO- 115177-SEMARCIS

SECURE MARITIME CIS (SEMARCIS)

PART IV
STATEMENT OF WORK
(SoW)

TABLE OF CONTENTS

SECTION 1. INTRODUCTION

1.1. Purpose

1.1.1. The purpose of this Statement of Work (SoW) is to describe the requirements for the Secure Maritime Communications (SEMARCIS) capability and the related responsibilities, effort and services to be provided by the Contractor.

1.1.2. This SoW, while intended as an outline of the minimum requirement and the general concept shall be supplemented by the Contractor to ensure the finished system is complete meeting the listed requirements of the SoW and shall be capable of fulfilling the function in accordance with the requirements of this SoW.

1.2. Key Requirements

1.2.1. The SEMARCIS capability shall enable eight (8) ships and one (1) static location at land to provide:

1.2.1.1. PSTN calls to, from and between the ships.

1.2.1.2. File transfer, messaging and voice between the ships and the static location at land, all at SECRET level.

1.2.1.3. Print services for the ships.

1.2.2. The SEMARCIS capability shall consist of Commercial Off-The-Shelf (COTS) products, Purchaser Furnished Services (PFS) which includes subscriptions to commercial satellite services and network services, and Purchaser Furnished Equipment (PFE), which includes software and encryption equipment.

1.2.3. The SEMARCIS capability shall operate reliably regardless of ship positions and weather conditions.

1.2.4. The SEMARCIS capability for the ships shall be implemented as self-contained units, for two users per ship, which shall be easy to transport, install, operate and remove.

1.3. Scope

1.3.1. The subscriptions to commercial satellite services are not in the scope of the Contract but shall be integrated as Purchaser Furnished Services, part of an existing airtime contract held by the Purchaser.

1.3.2. Providing PSTN and network services for the static location at land is not in the scope of the Contract.

1.3.3. The installation of equipment on board of the ships is not in the scope of the Contract.

SECTION 2. PROJECT MANAGEMENT

2.1 Introduction

2.1.1 This section outlines the Project Management area of the SEMARCIS contract.

2.2 Project Organisation

2.2.1 Purchaser Project Team

2.2.1.1 The Contracting Officer will act as the Purchaser’s representative and will be the primary interface between the Contractor and Purchaser from the Effective Date of Contract (EDC).

2.2.1.2 The Purchaser PM will be supported by specialists in certain areas who may, from time to time, be delegated to act on the PM’s behalf in their area of expertise.

2.2.1.3 All changes to the Contract will be made through the Purchaser's Contracting Officer only.

2.2.2 Contractor Project Team

2.2.2.1 The Contractor shall provide all necessary suitably qualified manpower and resources to conduct and support the project and shall as a minimum include:

2.2.2.1.1 Project Manager: The Contractor shall designate a suitably qualified Project Manager (PM), who will direct and co-ordinate the activities of the Contractor's project team. The Contractor’s PM shall be the primary contact for the Purchaser’s PM and shall conduct all project meetings.

2.2.2.1.2 Technical Lead: The Contractor shall designate a suitably qualified Technical Lead for the project. The Technical Lead shall lead the analysis, design, development, integration, testing and follow-on enhancement efforts of the Contractor.

2.2.2.2 The Contractor Project Manager and Technical Lead shall liaise with the Project Manager and Technical Lead appointed by the Purchaser. The Contractor shall provide a Curriculum Vitae (CV) or résumé reflecting their experience that meets the following requirements:

Serial	Requirement
1	A University Degree in Information Technology, Computer Science or other relevant Scientific subject.
2	At least 4 years of experience as a Project Manager or Technical Lead for an effort of similar scope, duration, complexity and cost, including the application of a formal project management methodology such as PRINCE2 or PMI's PMP
3	Experience with implementation of secure infrastructures for defense, government or financial organizations.
4	Working experience in a multinational environment or working experience with a multinational company or military organization on similar projects
5	To be in possession of a valid Security Clearance Certificate at least up to NATO Restricted, recommended up to NATO Secret

2.3 Project Implementation Plan (PIP)

2.3.1 The Contractor shall provide a Project Implementation Plan (PIP), which shall describe how the Contractor will implement the Project.

2.3.2 The PIP shall be provided to the Purchaser for review and acceptance within four (4) weeks after Effective Date of Contract (EDC). The PIP will be reviewed by the Purchaser and comments submitted to the Contractor no later than five (5) working days after receipt. PIP final version will be provided to the Purchaser six (6) weeks after Effective Date of Contract (EDC).

2.3.3 The approval of the PIP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This approval in no way relieves the Contractor from its responsibilities to meet the requirements stated in this SoW.

2.3.4 The PIP shall be kept up to date throughout the project, and shall be subject of review at each Project Review Meeting (PRM), until and including Provisional System Acceptance (PSA). The PIP shall identify also security accreditation process.

2.3.5 The PIP shall include the sections listed and described here below:

2.3.5.1 **The Project Overview**, which shall provide an executive summary overview of the offered SEMARCIS capability.

2.3.5.2 **The Project Management Plan** which clearly describes the implementation of the project.

1) The Project Management Plan (PMP) shall describe how the Contractor will implement the totality of the project, including details of the project control that will be applied.

2) The PMP shall describe how the Contractor shall implement project/contract administration, including details of the controls that shall be applied to supervise Sub-Contractor performance.

3) After approval by the Purchaser, the final version of the PMP shall be the official document against which the Contractor is expected to conduct the performance of the Contract.

4) The Contractor shall ensure that the PMP remains current throughout the duration of the Project to reflect the actual state of the Contractor’s organization and efforts, and maintain a current copy on the Collaborative Environment.

5) The PMP shall cover at least the following areas: Project organization, project management processes, communication management, lessons learned management, security accreditation, and subcontracting plan.

2.3.5.3 **The Project Master Schedule (PMS)** that shall contain all contract events and milestones for the Project.

1) The PMS shall show all contractual deliverables, their delivery dates, and the tasks associated with them.

2) The PMS shall for each task identify the start and finish dates, duration, predecessors, constraints, and resources.

3) The PMS shall provide network, milestone, and Gantt views, and identify the critical path for the overall project.

4) The PMS shall be provided in Microsoft Project format.

2.3.5.4 **The Project Personnel**, which shall include the curriculum vitae and security clearance information for the personnel proposed for this project listed in SoW Section 2.

2.4 Project Meetings

2.4.1 General

2.4.1.1 Except where otherwise stated in the Contract, the following provisions shall apply to all meetings to be held under the Contract.

2.4.1.2 The Contractor shall take meeting minutes, submit them within three working days of the meeting in draft version to the Purchaser for approval.

2.4.1.3 The participants shall not regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract, or as a vehicle to alter the design or configuration of equipment or systems. Any such changes shall only be made by agreement, amendment or by authorised mechanisms as set forth in the Contract.

2.4.1.4 Any documentation, even in draft format, that may be useful to the Purchaser in preparing for meetings and ensuring efficient discussions during the meetings shall be provided to the Purchaser no later than 5 working days before the meeting.

2.4.2 Project Review Meetings

2.4.2.1 The Contractor shall coordinate and hold the following Project Review Meetings (PRM) with the Purchaser:

1) PRM 1 includes System Design Review Meeting
2) PRM 2 includes First Article System Test (FAST) Meeting
3) PRM 3 includes Provisional System Acceptance (PSA) Meeting
4) PRM 4 includes Final Systems Acceptance (FSA) Meeting

2.4.2.2 Two weeks before each PRM the Contractor shall provide a Project Status Report (PSR), with the status of all on-going tasks, the status of the Contract deliverables, and identifying any changes to the System Design Specification (SDS), Risk Log and Issue Log, as described in paragraph 2.5.

2.4.2.3 Problems shall be identified and discussed with the Purchaser Project Manager promptly, and shall not be held over until the next PRM. Problems should not remain undisclosed in between meetings.

2.4.2.4 The location of PRM 1, PRM 3 and PRM 4 shall be at the Purchasers premises in Brussels (BEL), Mons (BEL), CIS Sustainment Support Centre (CSSC) (NL) or Northwood (UK) and when possible, it shall be scheduled with other project meetings. When deemed necessary by the Purchaser the PRM shall be held in an alternate location.

2.4.2.5 The Contractor will provide minutes of the meeting as. The Minutes shall include:

1) Date, place, and time of the meeting:
2) Purpose of the meeting;
3) Name of participants;
4) Approval of previous meeting’s minutes and all resolutions;
5) Record of principle points discussed, action taken, and decisions made;

2.4.2.6 The normal PRM agenda shall include:

1) Review of the minutes recorded and agreed at the previous PRM;

2) The Contractor's presentation of the Project Progress Report;

3) Schedule Review;

4) Risk Log Review;

5) Issue Log Review;

6) Discussion/resolution of problems and areas of concern;

7) If necessary, a summary of items to be discussed; and

8) Any other business.

2.4.2.7 In addition to the mandatory meetings (2.4.2.1), the Contractor shall support ad-hoc meetings (up to five). These meetings will be held in the NCIA Agency The Hague, Mons, or CSSC premises, and will be devoted to discussing management issues, technical issues, or both. Technical issues will be discussed through Joint Technical Reviews.

2.4.3 System Design Review Meeting

2.4.3.1 The Purchaser shall host the PRM1/ System Design Review Meeting (paragraph 3.2.3) ten (10) weeks after EDC.

2.4.3.2 In addition to the scope and requirements for System Design Review as described at 3.2.3, the Contractor shall provide the following, if applicable, at all design reviews:

1) Changes to the PMS

2) Cost considerations

3) Risk assessment of proposed changes, and an update of the Risk Log and Issue Logs, steps to mitigate any risks identified in the Risk Log.

2.4.4 Other Meetings

2.4.4.1 The Purchaser shall host all other meetings unless there is a specifically agreed need to review material, witness technical demonstrations or testing, or perform any other activity outside of the Purchaser's premises, as part of the meeting.

2.4.4.2 Upon approval by the Purchaser's PM, the Contractor shall schedule, organise, and conduct such meetings.

2.5 Project Progress Reports

2.5.1 This PPR shall summarize the progress since the previous PRM or since the last PPR, any accomplishments, schedule of deliveries against progress, difficulties encountered and resolution of any issues raised in previous PRMs. The Highlight Reports shall include:

2.5.1.1 Overall project progress: the activities performed and works completed during the preceding period including major milestones achieved as applicable;

2.5.1.2 Description of issues/problems/risks that have occurred in the preceding period and the identified / proposed solution (Issue Log);

2.5.1.3 A list of Change Proposals with the current status;

2.5.1.4 Configuration Status Reports (CSR) for the system and all documentation (CDRL);

2.5.1.5 Answers to questions addressed by the Purchaser between two meetings;

2.5.1.6 The progress of work related to the schedule in the current PMP;

2.5.1.7 Status of the equipment (equipment order, in Contractor’s office, packing, transfer to site, deploy and test);

2.5.1.8 Any foreseen or possible changes to project performance or schedule. In case of changes, the Contractor shall give the updated performance or schedule;

2.5.1.9 Description of any identified problems and high risk areas and the proposed solutions and corrective actions;

2.5.1.10 Activities planned for the next period;

2.5.1.11 Supplies to be delivered by the Contractor and those to be provided by the Purchaser;

2.5.1.12 Update on the status of Action Items List (AIL).

2.5.2 Upon receipt of the PPR, and in absence of a Project Review Meeting, the Purchaser can call for an Ad-hoc meeting with the Contractor for the purpose of reviewing or discussing the PPR contents. The meeting may either involve physical presence, or take place over a video conference session.

2.5.3 The contractor shall maintain an archive of PPR

2.5.4 The Contractor must prepare and submit a Project Progress Report (PPR) to the Purchaser 2 weeks prior to the PRM throughout the performance period of the contract.

SECTION 3. SYSTEM DESIGN AND INTEGRATION

3.1 General

This section outlines the System Design and Integration tasks of the SEMARCIS Contract.

3.2 System Design

3.2.1 General

3.2.1.1 The Contractor shall design the SEMARCIS capability to meet the requirements set out in the System Requirements Specifications (SRS, Appendix A).

3.2.1.2 The SEMARCIS capability shall consist of Commercial Off-The-Shelf (COTS) products, Purchaser Furnished Equipment (PFE) and Purchaser Furnished Services (PFS).

3.2.2 System Design Specification (SDS)

3.2.2.1 The Contractor shall establish and maintain the SEMARCIS capability System Design Specification (SDS). The SDS shall be delivered at eight (8) weeks after EDC.

3.2.2.2 The System Design Specification (SDS) shall include the following information:

1) Physical breakdown of the SEMARCIS capability into Hardware, Software and Firmware Configuration Items (CI, refer to §5.4 for CI identification).
2) Integration of the SEMARCIS capability Hardware and Software components with the PFS and PFE, demonstrating meeting the Functional Requirements, including a brief motivation for the selection of the components, a description of the components with their settings, and a network diagram.
3) Physical design demonstrating meeting the requirements for Packaging, Size and Weight.
4) Manufacturer datasheets of all equipment, demonstrating compliance with the Environmental Requirements (A.6) and the Equipment Miscellaneous Requirements (A.7).

3.2.3 System Design Review Meeting

3.2.3.1 The Contractor shall conduct PRM 1/ System Design Review Meeting with the Purchaser, at ten (10) weeks after EDC.

3.2.3.2 During the System Design Review, the Contractor shall cover the following topics:

1) System Design, as presented in the System Design Specification (SDS), including any change request, or off-specification.
2) Draft Test and Acceptance Plan (TAP).
3) Project Management topics as identified in 2.4.3.2.

3.2.3.3 The duration of the review period of the SDS by the Purchaser will be two (2) weeks, i.e. will be finished by twelve (12) weeks after EDC.

3.2.3.4 A second System Design Review shall be conducted if the changes requested after the first meeting require the Contractor to re-engineer the solution in any way.

3.2.3.5 Purchaser review and acceptance of the SDS does not imply Purchaser acceptance of the SEMARCIS capability design. It remains the sole responsibility of the Contractor to prove the design through the regime of testing set forth in the Contract. It will be the sole responsibility of the Contractor in the event that the system proves deficient in meeting the Contractual requirements.

3.2.3.6 The Contractor shall update the SDS and TAP, in order to reflect changes, if any, and present it to the Purchaser two weeks in advance of each of the following major milestones:

1) The second System Design Review, if required.
2) FAST and PSA testing.
3) The Final System Acceptance (FSA).

3.3 System Integration

3.3.1 General

3.3.1.1 The Contractor shall be responsible for the integration of the SEMARCIS capability such that it meets the requirements of the SRS. This integration shall cover:

1) Contractor provided components as per § 3.3.2.
2) Purchaser Furnished Services (PFS) as per § 3.3.3.
3) Purchaser Furnished Equipment (PFE) as per § 3.3.4.

3.3.2 Contractor provided components

3.3.2.1 Contractor provided hardware and software components shall be integrated in accordance with the SRS.

3.3.2.2 The laptop Operating System is PFE and will not be provided to the Contractor. Therefore, apart from the design, the integration activities by the Contractor on the software applications will be limited to preparing the systems used during the First Article System Test (7.2). The Contractor shall use its own copy of the Operating System for the above activities.

3.3.2.3 For the software components installation media and licenses shall be provided to the Purchaser which shall enable the Purchaser to (re)install and operate all Contractor provided software on all SEMARCIS laptops. The Purchaser shall not have to undertake any action to migrate licenses.

3.3.3 Purchaser Furnished Services (PFS)

3.3.3.1 The PFS comprise:

1) Subscriptions to Inmarsat Satcom Services (BGAN, FBB) for PSTN access and IP network services.
2) Management of the NATO IP encryption device (PFE).
3) PSTN services for the static location at land.
4) Unclassified IP network services at ships and at land.

3.3.3.2 The PFS integration activities by the Contractor shall include:

1) Design of the SEMARCIS capability using the PFS to meet the SRS.
2) Configuration of the satellite terminals for subscription to the PFS.

3.3.3.3 The PFS will be available to the Contractor at PSA.

3.3.4 Purchaser Furnished Equipment (PFE)

3.3.4.1 The Purchaser Furnished Equipment comprises:

1) Microsoft Windows 10 Enterprise Operating System licenses for all laptops.
2) Office and Anti-virus applications for all laptops
3) Licence Palo Alto FW PAN-SVC-PREM-3220
4) NATO messaging software
5) NATO IP encryption devices (hereafter called ‘NATO IP crypto’) for each SEMARCIS unit, which is further specified in Appendix B.

3.3.4.2 The PFE integration activities by the Contractor shall include:

1) Design of the SEMARCIS capability incorporating the Microsoft Windows 10 Enterprise Operating System and the NATO IP crypto specified in Appendix B, to meet the SRS.

3.3.4.3 Physical integration, configuration and operation of the NATO IP crypto will be performed by the Purchaser.

3.4 System Documentation

3.4.1 The System Documentation shall consist of:

1) System Design Specification (SDS), refer to § 3.2.2;
2) Integrated Logistics documentation, refer to § 4;
3) System Configuration, refer to § 5.4.4;
4) Manuals, refer to § 4.8**Error! Reference source not found.**;
5) Test Plans and Test Reports (refer to § 7 of this SoW);
6) Security Accreditation Documentation (refer to § 8 of this SoW).

3.4.2 The Contractor shall document components settings that are required to operate as a SEMARCIS system and instructions for how these settings are applied. Components include:

1) The satellite terminal,
2) Handsets for PSTN and secure voice,
3) Operating System,
4) File transfer applications,
5) VPN device. Only the network settings (outside and inside IP address, static routes) have to be provided, instructions for applying the settings are not required.
6) NATO IP crypto. Only the network settings (red IP address, black IP address, static routes) have to be provided, instructions for applying the settings are not required.

3.4.3 All the documentation to be provided under this Contract shall be written in English (preferably United Kingdom Standard).

3.4.4 Any supporting COTS documentation shall be delivered in PDF format.

3.4.5 Any non-COTS documentation shall:

1) Have a clear title indicating the Contractual deliverable it pertains to, a reference and version number, and appropriate signature blocks demonstrating that the documentation has been subject to the Contractor's quality process.
2) Include a 'version history' block identifying at least for the last version the complete list of changes brought to the document since the previous version, and clearly indicating any superseded documents (including the previous version of the document).
3) Each change shall be identified at least by Section#, Page#, Nature of change. (A summary list is sufficient provided that the

changes are tracked within the document, e.g. using the ‘change tracking’ mechanism in Microsoft Word, or some equivalent for other applications).

4) Be delivered in both Microsoft Office editable format and in PDF format

5) Be classified and labelled according to their official NATO classification.

3.4.6 The documentation shall be made available in electronic format on electronic storage media (soft copy) and the manuals and training material shall also be made available in paper format (hard copy).

3.4.7 The manuals and training material shall be part of the packaging of each SEMARCIS unit, and three additional copies of the manuals and training material shall be made available to the Purchaser.

SECTION 4. INTEGRATED LOGISTICS SUPPORT (ILS)

4.1 General

4.1.1 This section addresses the ILS requirements of the project. The purpose of this section is to ensure that the Contractor uses sound, ILS best practice to plan and implement the ILS, as well as to ensure timely and correct delivery of equipment.

4.1.2 The Contractor’s internal Life Cycle Management (LCM) process and system shall comply with STANAG 4728 “System Life Cycle Management (SLCM)”.

4.1.3 The Contractor shall establish a Supportability Programme to manage the ILS activities within this Contract by:

1) Providing evidence that the designed system is for a service life of at least five (5) years based on the operational conditions required through the development of the activities described in the ILS Plan;

2) Appointing an ILS manager to conduct the ILS Programme that shall:

a. Be at a level commensurate with the systems engineering and the software engineering managers;

b. Have functional subordinates to reflect the programme ILS managerial structure;

c. Be point of contact to interface with the Purchaser on ILS matters.

3) Providing all relevant logistics data gathered as a result of all ILS processes in .xls file.

4.1.4 The following reference documentation is for ILS purposes.

Abbreviation	Full document Name and Reference
[STANAG 4728, Ed.2]	System Life Cycle Management. Ed.2, 2015.
[AAP-20, Ed.C, Ver.1]	NATO Programme Management Framework (NATO Life Cycle Model). Ed.C, Ver.1, 2015.
[AAP-48, Ed.B, Ver.1]	NATO System Life Cycle Processes. Ed.B, Ver.1, 2013.
[ALP-10, Ed.C, Ver.1]	NATO Guidance on Integrated Logistics Support for Multinational Armament Programmes. Ed.C, Ver.1, 2017.
[STANAG 6001, Ed.5]	Language Proficiency Levels. Ed.5, 2014.
[STANAG 4280]	NATO Levels of Packaging
[STANAG 4281, Ed.3]	NATO Standard Marking for Shipment and Storage. Ed.3, 2016.
[STANAG 4329, Ed.4]	NATO Standard Bar Code Symbologies – AAP-44(A). Ed.4, 2010.
[AAP-44]	NATO Standard Bar Code Handbook
[ISO/IEC 15288, 2015]	Systems and software engineering -- System life cycle processes
[ISO/IEC 12207, 2008]	Systems and software engineering -- Software life cycle processes
[ISO/IEC 25010, 2011]	Systems and software engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — System and software quality models

[IEC 60050]	International Electrotechnical Vocabulary (IEV). (www.electropedia.org)
[AIA/ASD SX000i, 2016]	International guide for the use of the S-Series Integrated Logistic Support (ILS) specifications. Issue 1.1, 2016.
[AIA/ASD S3000L, 2014]	International Specification for Logistics Support Analysis – LSA. Issue 1.1, 2014.
[AIA/ASD S1000D, 2019]	International Specification for Technical Publications. Issue 5, 2019
[SD-22]	Diminishing Manufacturing Sources and Material Shortages (DMSMS). 2016
MIL-HDBK-338B	Military Handbook - Electronic Reliability Design Handbook
MIL-STD-1629A	Military Standard – Procedures for performing a Failure Mode, Effects and Criticality Analysis

Table 4-1 Integrated Logistics Support Reference Documents

4.2 Integrated Logistics Support Plan (ILSP)

4.2.1 The Contractor shall provide an Integrated Logistics Support Plan (ILSP) that shall:

1) Describe the Contractor’s plans for the management control, interface, and integration of all elements of the Contractor’s Integrated Logistics Support with the system engineering and design processes;

2) Establish/describe the policies, procedures, constraints and methodologies to ensure the logistic requirements are achieved and to refine the support to the system;

3) Incorporate Purchaser-approved changes, additions and deletions.

4.2.2 The ILSP shall describe the Contractor’s approach and plans for each logistic element:

1) Reliability Availability Maintainability and Testability (RAMT),
2) Logistics Support Analysis (LSA) including Logistic Data and Supply Support,
3) Packaging Handling Storage and Transportation (PHST),
4) Parts Obsolescence Management,
5) Technical Manuals,
6) Training.

4.2.3 The ILSP shall document the Contractor’s plans, organizational structure, procedures and activities implemented, followed and performed to ensure that logistics and the logistics support elements influence and interface with system design and other functional areas, to satisfy supportability criteria.

4.2.4 The ILSP shall explain the interface of the Contractor’s ILS structure and the overall design process with his subcontractors, vendors and suppliers.

4.2.5 The ILSP shall include a schedule of the ILS Programme and a detailed description of the interaction of the ILS activities with the other activities performed.

4.2.6 The Contractor shall provide a preliminary ILSP that shall include the structure and foreseen content with initial details for this plan in the proposal phase so to show the concept of the activity.

4.3 Maintenance Task Analysis (MTA)

4.3.1 The Contractor shall provide a Maintenance Task Analysis (MTA) down to the hardware LRU and software CSCI level compliant with ASD S3000L iss.1.1.

4.3.2 The Contractor shall provide a Maintenance Task Analysis (MTA) covering hardware and software that summarizes the maintenance planning:

1) Analysing the results of the FMECA to identify candidate corrective maintenance tasks;

2) Identifying procedures, spares and materials, tools, support equipment, personnel skill levels, estimated and elapsed times as well as any facility issues that must be considered for a maintenance task;

3) Identifying scheduled maintenance tasks and develop a scheduled maintenance programme that is consistent with the maintenance concept described for the intended use of the system. The decision logic used for task selection shall implement the following priorities:

a. avoidance of safety and mission critical failures;

b. achievement of system availability requirements;

c. sustainability of deployed operations in accordance with the intended use and the logistics support environment of the system;

d. minimization of Life Cycle Cost;

4) Identifying the operation support tasks required to support operational readiness of the system;

5) Assessing for each maintenance task: skill levels, tools and test equipment required, facilities, spares and consumables, duration.

4.3.3 The Contractor shall provide a **Logistics Database** in .xls compliant with ASD S3000L iss.1.1 as annex to each issue of the MTA that shall match the Product Baseline (PBL), shall be coherent with the relevant information contained in the Technical Publications and Training Materials and shall include information fields required for each HW and SW item to be provided/updated:

1) Indenture level: Level of indenture starting from the system that is the first level and classified as End Item

2) Breakdown Element Identifier (BEI): String of characters used to uniquely identify a Breakdown Element and to differentiate it from other

Breakdown Elements that comprise a product. Note: used to establish a hierarchical structure of the technical system.

3) Reference Designator;

4) Subsystem;

5) Breakdown Element Name: Word or phrase by which the breakdown element is known and can be easily referenced.

6) Part Logistic Category[1];

7) Manufacturer item data: Cage Code, Part Number, Part Nomenclature;

8) Vendor/Contractor item data: Cage Code, Part Number, Part Nomenclature;

9) Item characteristics:

- LRU (Y/N), Serialized Item (Y/N); Mean Time Between Failure (MTBF) (in hours); Mean Time To Repair (MTTR) (in hours);
- LRU Maintenance Level (HL/SL 1 to 3 included); HW part repair ability (Y/N);
- NATO Stock Number (NSN); Unit Price and Currency;
- Provisioning Lead Time (PLT) (days); Turnaround Time (TAT) (days).
- Quantity: Qty per line item; Qty in Next Higher Assy; Qty in End item.

4.3.4 The Contractor shall provide a preliminary MTA that shall include the structure and foreseen content with initial details so to show the concept, understanding and commitment of the activity.

[1] The **Part Logistic Category** is a classification that defines an item (HW or SW) as designed in the context of product support. In particular these identifications can be used:

- **EI** - End Item and **SS** – System Subsystem
- Hardware (HW) Maintenance Significant Items (MSI): **LS** - Statistical Life LRUs (e.g.: Computers, Power PCs, Switches, Routers, IF modules, RF modules, Breakers, Power Supplies, Monitors, Modems, Power Amplifiers); **LL** – Limited Life LRUs (e.g.: Batteries, flexible waveguides, oscillators); **II** – Insurance Items [e.g.: docking stations, Keyboards, Mice, Cables, mechanical parts (e.g. Racks, drawers), simple E/M parts (e.g. patch panels)]; **C[T]** – Technical Consumables (e.g.: fuse, gas discharger, surge protection devices, lamps, bulbs, led); **C[NT]** – Non-Technical Consumables [e.g.: POL (Petrol, Oils, Lubricants), water, gas]; **C[G]** – Generic Consumables (e.g.: printer cartridges, toners, printers' paper); **AP** – Attaching Parts [e.g.: washers, gaskets (not EMI), nuts, bolts, screws].
- Software (SW): **SWA** – Application Software [e.g.: contractors' developed application SW, COTS application SW (e.g. MS Office, Adobe Acrobat)]; **SWO** – Software Operating Systems (e.g.: Linux, UNIX, MS Windows, LynxOS, Android, IOS); **FW** – Firmware; **DD** – Device drivers.
- Support equipment and tools: **CHT** (Common Hand Tool), **CSE** (Common Support Equipment), **PSE** (Peculiar Support Equipment);

4.4 Level of Repair Analysis (LORA)

4.4.1 The Contractor shall provide a Level of Repair Analysis (LORA) down to the hardware LRU and software CSCI level fully compliant with ASD S3000L iss.1.1.

4.4.2 The Contractor shall provide a Level Of Repair Analysis (LORA) to recommend the most cost efficient solution for the level at which each maintenance task should be performed and the decision to repair or discard unserviceable LRUs:

1) Generating a LORA candidate list containing those items whose maintenance task is not clearly allocated as NATO Maintenance Task (NMT) or Industry Maintenance Task (IMT) as a consequence of the MTA and for which a repair/discard decision is not immediately evident;

2) Determining the level (HL1-4 or SL1-4) and the location at which each maintenance task should be performed, including detail on any NMT for which specific limited support by industry personnel is recommended.

4.4.3 The Contractor shall provide **Repair Price List (RPL)** as annex to the final issue of the LORA.

4.4.4 The Contractor shall provide a preliminary LORA that shall include the structure and foreseen content with initial details so to show the concept, understanding and commitment of the activity.

4.5 Parts Obsolescence Management

4.5.1 The Contractor shall perform the Parts Obsolescence Management during the project execution up to the end of warranty period and inform the Purchaser about any:

1) Obsolescence related risk,
2) End of sale, production, support,
3) Mitigation options.

4.5.2 The Contractor shall provide a **Diminishing Manufacturing Sources (DMS) Report** to keep the Purchaser informed on the potential obsolescence problems or risks and the mitigation strategies.

4.5.3 The Contractor shall recommend, as part of the DMS Report:

1) A replacement (if available), when the designation of a replacement item becomes necessary due to discontinuance of support;

2) Either to implement an Off-The-Shelf (OTS) solution and modify the requirement accordingly or redesign a suitable alternative, when the recommended OTS item is not fully compliant with the Contract Requirements;

3) Items with form, fit and function features will be given first preference to avoid development costs.

Implementation of the above recommendations shall be in accordance with ECPs.

4.5.4 The Contractor shall provide a preliminary DMS Report to show the concept, understanding and commitment of the activity to be developed during the contract execution.

4.6 Supply Support and Provisioning

4.6.1 The Contractor shall provide the following fully detailed and priced lists including as a minimum the information of the table below for MDS:

1) **Recommended Spare Parts List (RSPL)** that shall detail all spares in a hierarchical breakdown;

2) **Recommended Consumable Items List (RCIL)** that shall detail all consumables used for maintenance tasks;

3) **Recommended Tools and Test Equipment List (RTTL)**, that shall detail all standard and special-to-type tools, test equipment and test fixtures, cables, connectors, support equipment (e.g.: cranes, lifting platforms, etc.).

4.6.2 The Contractor shall provide the full and complete inventory/Material Data Sheet (MDS) of all items and documents to be delivered under this contract at least ten (10) working days before shipment. It shall contain the following information:

Field	**Description**
CLIN	Contract Line Item Number (number-10 digits maximum). Sequence number assigned to a particular line item in a given contract. The combination CLIN-Contract No. shall always be unique.
Nomenclature	Short Item Description (text- 35 digits). Should always start with the main item name followed if possible by a technical specification, followed by the next higher assembly names in hierarchical order, separated by commas. E.g. for a coax connector of a television cable the nomenclature should read: CONNECTOR, COAX, CABLE, and TELEVISION.
EQRE (XB/ND)	Code (text-2 digits). Defines whether an item is repairable (ND) or not (XB) from a technical point of view.
True Manufacturer Part Number	True Manufacturer P/N (text-32 digits). Part Number given to this item by the original manufacturer.
True Manufacturer Code (or complete name and address)	True Manufacturer Code (text-5 digits). Code of the Company that has manufactured this item. This is an internationally recognized 5-digit code which is unique to that company. It corresponds to the "cage code" in the USA. Manufacturer Codes and Cage Codes are obtainable from the national governmental authorities or, if it already exists, from the "NATO Master Cross-Reference List" (NMCRL) obtainable from NSPA. In case the code cannot be obtained, it will be sufficient to enter the complete name and address information of the true manufacturer.

Field	Description
Vendor/Contractor Code (or complete name and address)	Vendor (Contractor) (text-5 digits). Company which sells the item or the complete system to which this item belongs. The vendor is the company with which the contract is placed but is not necessarily the true manufacturer of the item. If the vendor company has also designed and integrated the complete system it is also known as Original Equipment Manufacturer (OEM). The company code is an internationally recognized 5-digit code which is unique to that company. It corresponds to the "cage code" in the USA. Manufacturer Codes and Cage Codes are obtainable from the national governmental authorities or, if it already exists, from the "NATO Master Cross-Reference List" (NMCRL) obtainable from NSPA. In case the code cannot be obtained, it will be sufficient to enter the complete name and address information.
Vendor/Contractor Part Number	Vendor (Contractor) P/N (text-32 digits). Part Number given to this item by the company which sells the item or the complete system to which this item belongs. The vendor is the company with which the contract is placed but is not necessarily the true manufacturer of the item.
QTY ordered	Item Quantity (number-5 digits). Shows the quantity of this item ordered as individual item in this contract, i.e. if it is not delivered built-in in another unit. In case the item is not ordered as individual item or as spare unit but is built-in in another assembly, enter "0" (zero) in this field and complete fields: "Part Number of next higher assembly" and "qty in next higher assembly". Serialised items shall only have a quantity of 1.
Order Unit	Order Unit (text-2 digits). Unit under which the item is sold, e.g. each, set, meter, etc.
Serialized Item Tag	Serialized Items Tag (text-1 digit). Add a "Y" if the item carries a serial number independently whether serial numbers is already known or not. If known, complete column "Serial Number".
Serial Number	Serial Number. If Serialized Item Tag is "Y" (yes) then add serial number here. (1 serial number per line). If system is already installed, then the Contractor shall indicate here the serial numbers installed at user site. For items to be delivered to depots the Contractor may not know the serial number in advance, in that case it will be completed by the receiving site.
Serial Number Software Revision Level	Software Revision Level (text- 30 digits but can be expanded as necessary) If item carries a serial number and field "serial number" is completed, add SW revision level / version here if appropriate.
Serial Number Hardware Revision Level	Hardware Revision Level (text- 30 digits but can be expanded as necessary) If item carries a serial number and field "serial number" is completed, add HW revision level / version here if appropriate.
Other Serial Number attributes	Other Serial Number Attributes (text-to be defined). This field will be used and defined on a case by case basis to be decided by NCIA System Manager, NCIA and the Contractor for other attributes which might be required for a particular system.
Subject to Property Accounting	NDSS-MRCS (text-1 digit). NCIA will decide whether or not item is subject to property accounting and is to appear on the customer balance lists. This field will be completed Y or N by NCIA.
Currency	Currency (text-3 digits). International 3-digit code (ISO) representing the currency in which the item purchase price (or the estimated value) is expressed.
Price	Item Price (number-11 digits). Unit price with 2 decimals.
Warranty Expiration Date	Warranty Expiration Date (date: DD/MM/YY). Shows the date on which the warranty of this item expires, which is usually N days after delivery of the item. If delivery is scheduled for a certain date, warranty expiration date = delivery date + warranty period in days.

Field	Description
Receiving / Inspection Depot	Receiving / Inspection Depot (TXT-2 digits). Information will be provided to Contractor by the Purchaser's ILS Officer. This is the depot to where the vendor ships the material. Normally this depot will receive, inspect and put the material in stock against Dues-In to be created in accordance with Qty in column "Qty Ordered". In case of a deviation from this rule, the Purchaser will inform the Contractor of the correct final Depot and through which depot the items shall have to transit.
Issue to customer	Customer Code (text-4 digits - to be completed by NCIA). Code representing the customer to which the item(s) shall be shipped by the receiving/ inspecting depot.
Extended Line Item Description	Extended Line Item Description (text-no limit). Any additional information concerning this item shall be entered here, e.g. technical specifications, configuration, reference to technical drawings or manuals etc.…
Part Number of next higher assembly	Part-Number of Next Higher Assembly (text-32 digits) If item is built-in another assembly, indicate part number of that assembly here.
Qty in next higher assembly	Quantity in Next Higher Assembly (number-3 digits max). This field shows the built-in quantity of the item in the next higher assembly. This information shall be provided for configuration control purposes.
Qty installed at Operating Unit (Customer Site)	Quantity installed. This field is only applicable when the delivery is direct to an operating unit (customer site). However in that case it is mandatory. For non-serialized items it shows total quantity installed. For serialized items quantity shall only be one per serial number. Use a new line for each serial number.

Table 4-2 Inventory/Material Data Sheet information

4.7 Packaging, Handling, Storage and Transportation (PHST) Report

4.7.1 The Contractor shall provide a PHST Report that shall provide information critical to the PHST of equipment, spare parts and consumables. It shall include environmental and hazardous material information imperative for safe handling storage and transportation identifying also any special packing/removing requirements for equipment as required.

4.7.2 The Contractor shall identify all items which will be stored at the site or at the Contractor's repair facility and/or which may need transportation between the site and the Contractor's or vendor's repair facilities or depot, identifying the relevant PHST data.

4.7.3 The Contractor shall provide a single Packaging and Transportation Plan, which shall include details of the Contractor's proposed bar-coding system and shall give consideration to transportability, special handling/storage requirements and other hazards associated with the national/international transportation of items.

4.7.4 The Contractor shall provide a bar-coding system, for all hardware, software, training and technical documentation, which shall be compliant with STANAG

4329. The Contractor shall produce and affix bar-code labels to equipment items, packaging, containers and documentation.

4.7.5 The Contractor shall pack all spares and Contractor-provided Support Equipment in reusable containers suitable for the return of unserviceable similar items. These containers shall meet the requirements of NATO packaging level 3 of STANAG 4280 and shall protect the packed equipment from the environmental conditions.

4.7.6 The Contractor shall provide any special packing instructions and shall also be responsible to provide any special-to-type container(s) for the shipment of repairable items, at no cost to the Purchaser. Marking (including bar coding) of packages and reusable containers will be in accordance with STANAG 4281 and STANAG 4329.

4.7.7 The Contractor shall deliver all equipment under this contract to the NATO CIS Sustainment Support Centre (CSSC) at the following address:

NATO Communications and Information Agency
CIS Sustainment Support Centre
JFC Headquarters
Building 204
Rimburgerweg 30,
6445 PA Brunssum,
The Netherlands

4.7.8 The Purchaser will provide PoC for shipment instruction/request and for CSSC.

4.7.9 The Contractor shall provide ten (10) working days before the first delivery in electronic format a Material Data Sheet (MDS) that, as a minimum, shall include the data elements cited with an “M” mandatory below (if applicable). This listing, amended as necessary, shall be used for acceptance purposes and to create data element entries in the NATO Accounting system.

4.7.10 The Contractor shall provide the final System Inventory as a hard copy as well as on electronic media in Microsoft Excel or Access database format. Details on the exact format of the various data elements to be adopted will be communicated following contract award. An inventory template together with a full content description for each column (electronic format) shall be provided to the Contractor at the time of contract award. For information purposes, the minimum inventory/equipment data elements required are as follows (**M** is Mandatory):

- Contract Customer Line Item Number (CLIN);
- NATO Stock Number (NSN - if available);

- Nomenclature – **M**;
- Expendable/Repair code XB/ND – **M**;
- True Manufacturer Part Number – **M**;
- True Manufacturer Cage Code (or complete name and address) – **M**;
- Vendor/Contractor Cage Number (or complete name and address) – **M**;
- Vendor/Contractor Part Number – **M**;
- Quantity ordered- **M**;
- Order Unit – **M**;
- Serialized Item Tag – **M**;
- Serial number – **M**;
- Serial number software revision level;
- Serial number hardware revision level;
- Other serial number attributes;
- Currency – **M** ;
- Unit Price – **M** ;
- Warranty expiration date – **M** ;
- Receiving NATO Depot;
- Extended Line Item Description;
- Part Number of next higher assembly;
- Quantity in the next higher assembly.

4.7.11 The Contractor shall ensure that the various supplies will be transported, packaged, crated, or otherwise prepared in accordance with the best commercial practices for the types of supplies involved, giving due consideration to shipping and other hazards associated with the transportation of consignments to overseas.

4.7.12 The Contractor shall ensure that packing lists are provided in such a way as to permit easy identification of the items to be delivered to destinations. These packing lists shall accompany the shipment. Each individual box from a consignment shall have one packing list in weather proof envelope affixed to the outside of each box that indicates exactly what is contained inside. One copy shall also be put inside each box.

4.7.13 The Contractor shall provide a detailed description of packaging to be used and shall provide any special packaging materials required for the shipment of items.

4.7.14 The Contractor shall provide packages, palettes and/ or containers in which supplies are transported showing on a separate nameplate, in addition to normal mercantile marking: the project name, contract number and shipping address.

4.7.15 The Contractor shall provide all hardware packaging supplied marked as applicable with the true manufacturer's part number, serial number and revision level as identified in the relevant technical documentation.

4.7.16 The Contractor shall provide packing lists accompanying each shipment, which shall as a minimum include the following:

- The NCIA contract number;
- The NCIA Project Title;
- Item description;
- Item part number and serial number;
- CLIN number as per the SSS;
- Name and address of the Contractor/ Sender, the Purchaser and Consignor;
- Detailed weight and dimensions per box/pallet/container;
- Box number and number of boxes in the consignment.

Two copies of the packing lists shall be fastened in a sealed envelope on the outside of each box, palette and/ or container.

4.7.17 The Contractor shall ensure the timely request of Customs Forms 302 which are required for duty free import/export of supplies.

Following receipt of the request by the Purchaser, normally a maximum of three (3) working days is required for the issue of the form. This form is not required for movements within the European Union.

These forms shall be originals shall be originals and cannot therefore be faxed but shall be mailed or sent by mail/express courier. In case that an express courier has to be used to ensure that the form is available in time before shipment, all associated costs shall be the responsibility of the Contractor.

The written request for a 302 form shall contain the following information:

- Purchaser Contract Number.
- CLIN, Designation and Quantities.
- Destination.
- Number and Gross Weight.
- Consignors and Consignee’s Name and Address.
- Method of Shipment, i.e. road, rail, sea, air, etc.

In case a country refuses to accept the Form 302 and requires the payment of customs duties, the Contractor shall immediately inform the Purchaser by the fastest means available and obtain from the Customs Officer a written statement establishing that his country refuses to accept the Form 302. Only after having received Purchaser's approval the Contractor shall pay these customs duties and the Purchaser shall reimburse the Contractor at actual cost against presentation of pertaining documents.

4.7.18 The Contractor shall inform forwarding agents of the availability of Form 302 and how this form is utilised to avoid the payment of customs duties. This Form 302 shall be added to the shipping documents to be provided to the carrier.

4.7.19 The Contractor shall provide the Purchaser with a Notice of Shipment ten (10) working days before each shipment of supplies, comprising the following details:

- Shipment Date.
- Contract Line Item.
- Consignor and Consignee.
- Number of Packages/Containers.
- Final/Partial Shipment.

Mode of Shipment.

Number of 302 Forms used (if used).

4.8 Technical Publications (TP)

4.8.1 The Contractor shall detail approach and plans for Technical Publications in a relevant chapter into the ILSP. Updates shall be managed in a separate ad hoc document named **Technical Publication Development Plan (TPDP)** that shall include the **Writing Style Guide (WSG)** to be fully compliant with ASD S1000D iss.5.

4.8.2 The Contractor shall provide User Manuals and Maintenance Manuals for all (non PFE) Hardware and Software installed in the SEMARCIS units, including COTS and Contractor customized items, modified items and fully developed items.

4.8.3 The Contractor shall provide User Manuals and Maintenance Manuals as per requirements of personnel operating and maintaining the equipment in accordance with the Maintenance Concept:

4.8.3.1 User Manuals: is for the operation of the equipment and describes operation, settings and fine tuning of the equipment to achieve maximum performance including administration instructions (e.g.: guidance on how to show, edit and save the System Configuration Files on the respective devices, together with default user or administrator passwords, as required).

4.8.3.2 Maintenance Manuals: is for the maintenance of the equipment and includes:

4.8.3.3 Scheduled and Unscheduled Maintenance detailed instructions, Troubleshooting and fault finding techniques (including descriptions of all indicators, switches, switch positions, displays, menu's, settings etc), Installation and dismantling of the equipment (including as applicable physical, electrical, software, safety, RF aspects etc.), repair and test procedures up to HL3/SL3 activities included;

4.8.3.4 Drawings of the mechanical, electrical and electronic assemblies and sub-assemblies that comprise the equipment in sufficient detail to allow technical staff to maintain the system at site level in accordance with the Maintenance Concept;

4.8.3.5 As-built drawings (ABDs) for full details of how all of the major assemblies of the supplied equipment have been physically installed and mechanically/electrically integrated (e.g.: drawings of intra-rack and inter-rack cabling);

4.8.3.6 Detailed and lower level repair and maintenance of sub-assemblies and components shall be addressed by the Original Equipment Manufacturer' s (OEM) manuals unless it has been agreed that specific activities are NMT.

4.8.3.7 Physical, functional, performance, environmental data and descriptions (including support equipment/tools and interfaces to external systems)

4.8.4 The Contractor shall provide Original Equipment Manufacturer (OEM) Technical Manuals for all the items from other manufacturers/vendors used into the system, equipment and test equipment assuring that they:

4.8.4.1 Provide detailed information necessary to disassemble and assemble the units down to the lowest Line Replaceable Unit (LRU) level of maintenance;

4.8.4.2 Provide the necessary drawings/schematics, specifications, wiring diagrams, etc., to allow the operators to troubleshoot, and fully understand, the design and operation of the particular equipment;

4.8.4.3 Supplement but do not substitute User Manuals and/or Maintenance Manuals and thus be expected to be referenced in the latter as a way of providing specific details on a particular piece of equipment;

4.8.4.4 Are amended by preparation of supplemental data to make them fully acceptable for Purchaser use.

4.8.5 The Contractor shall provide the OEM TMs together with each associated equipment:

- On electronic format (e.g.: CD, DVD),
- In hardcopy.

4.8.6 The Purchaser will review and approve (in 8 weeks) the Technical Publications delivered under this Contract. Upon acceptance of the draft version, the Contractor shall deliver the final version of the technical publications.

4.9 Training

4.9.1 The Contractor shall detail approach and plans for Training Publications in a relevant chapter into the ILSP. Updates shall be managed in a separate ad hoc document named **Training Plan (TP)** that shall include the **Training Needs Analysis (TNA)** (the last shall also enumerate the duties that a worker must perform, provide a detailed job description and detail the desirable entrance criteria to the training so to help the Purchaser to select the best training candidate).

4.9.2 The Contractor shall assume that trainees and audience will have proficiency in the English language, knowledge of the Microsoft Windows Operating System and the audience will tailored for a maximum twelve (12) students plus maximum four (4) auditors.

4.9.3 The Contractor shall provide evidence of the trainer, or a Subject Matter Expert (SME) supporting the trainer, qualifications and in particular to have at least two years practical experience with the installation and operation of the items under training.

4.9.4 The Contractor shall provide training and training materials for test personnel, operators, maintainers and instructors:

1) Based on the maintenance and support concept (Logistics database):
2) Based on technical publications,
3) Containing slides used during the training, and provide a hardcopy to each student.

4.9.5 The Contactor shall provide training for the SEMARCIS capability at the Purchaser premises in Northwood UK prior to the Provisional System Acceptance.

4.9.6 The training shall cover:

- Overview of the SEMARCIS capability (functions, components).
- Satellite services:
  - Introduction of the Commercial Satellite Service (capabilities, coverage, cost).
  - Overview of the satellite terminal (interfaces, indicators, functions, supported services, performance etc.).
  - Installation at land (using the materials delivered as part of the SEMARCIS) for testing and training.
- Operation of the terminal (making PSTN calls, using data).

Installation of the terminal in a maritime environment (how to, where to install, hazards, materials, interference, protection against intrusion of water, etc.).

- Applications:
  - Overview of the file transfer applications (relevant features).
  - How to install/ configure the applications.
  - How to use the applications (operation, relevant menu's).
- Handset for SECRET level calls:
- Overview of phone (relevant features & properties).
  - How to configure.
  - How to make calls.

4.9.7 The Purchaser will review and approve (in 10 weeks) the Training Material delivered under this Contract. Upon acceptance of the draft version, the Contractor shall deliver the final version of the training material.

4.10 Warranty

4.10.1 The Contractor shall be responsible for the maintenance of the system (except for PFE) during the implementation phase until FSA and shall therefore provide its own spare parts, tools and test equipment to maintain the system (except for PFE) to the required performance level.

4.10.2 The Purchaser will operate the system After FSA.

4.10.3 The Contractor shall provide a standard warranty for a period of one (1) year starting with the successful completion of FSA.

4.10.4 The contractor shall provide the following services during the Warranty to maintain the system (except for PFE) to the required performance level:

a. Hardware corrective/unscheduled and preventive/scheduled maintenance: repair and/or re-placement of all defective technical installations/equipment;

b. Software corrective/unscheduled and preventive/scheduled maintenance: remediation/resolution of all bugs, flaws, etc. of all software installations, provided as part of this contract.

4.10.5 The Purchaser will responsible (at its own expenses) for returning of failed items to the Contractor.

4.10.6 The Contractor shall repair repairable items received at the Contractor's plant in maximum Turnaround Time (TAT) thirty (30) days. This shall include in-processing, trouble shooting, repair and check-out and release to the Site or Depot.

4.10.7 The Contractor shall be responsible for returning of repaired items to the Purchaser (i.e.; to NATO CIS Sustainment Support Centre, at Brunssum).

4.10.8 The Contractor shall be responsible for the provision of any alternative or superseding items, should the original part be no longer available ensuring SRS and PBL compliance.

4.10.9 The Contractor shall submit at the end of the Warranty period a **Warranty Report** that documents all identified Warranty cases, affected CI's, corrective actions, cost and schedule.

4.10.10 The Contractor shall provide a preliminary Warranty Report to show the concept, understanding and commitment of the activity to be developed during the contract execution.

SECTION 5. CONFIGURATION MANAGEMENT (CM)

5.1 General

5.1.1 This section addresses the CM requirements of the project. The purpose of these requirements is to ensure that the Contractor establishes and executes NATO-compliant and effective configuration management during the execution of the project until FSA.

5.1.2 The Contractor's internal Configuration Management process and system shall comply with STANAG 4427 "Configuration Management in System Life Cycle Management" and the requirements of [ACMP-1] through [ACMP-7].

5.1.3 The Contractor shall establish a Supportability Programme to manage the CM activities within this Contract, maintaining an effective CM organization to implement the CM program and manage the CM functions (configuration identification and documentation, configuration control, configuration status accounting, configuration audits).

5.1.4 The Contractor shall be responsible for the application of all necessary CM procedures throughout the duration of the Contract.

5.1.5 The Contractor shall maintain a version control system as part of its CM program.

5.1.6 The Contractor shall ensure that there is full traceability through all baselines back to the functional baseline.

5.1.7 The Contractor shall populate and maintain the Baselines and their CI's in the Configuration Management Data Base (CMDB).

5.1.8 The Contractor shall deliver a fully populated CMDB to the Purchaser before FSA.

5.1.9 The following reference documentation is for CM purposes.

Abbreviation	Full document Name and Reference
[STANAG 4427, Ed.3]	Configuration Management in System Life Cycle Management. Ed.3, 2014.
[ACMP-2000, Ed.A, Ver.2]	Policy on Configuration Management. Ed.A, Ver.2, 2017.
[ACMP-2009, Ed.A, Ver.2]	Guidance on Configuration Management. Ed.A, Ver.2, 2017.
[ACMP-2100, Ed.A, Ver.2]	The Core Set of Configuration Management Contractual Requirements. Ed.A, Ver.2, 2017.
[ISO 10007:2003]	Quality Management System – Guidelines for Configuration Management. Second edition, 2003.

Table 5-1 Configuration Management Reference Documents

5.2 Configuration Management Plan

5.2.1 The Contractor shall establish, provide, execute, and maintain an effective Configuration Management Plan (CMP) throughout the period of performance of this Work Package. The Contractor shall organize review meetings for CM progress starting from the first draft of CMP.

5.2.2 The CMP shall be a Product Lifecycle document that will outlast the project post-FSA. As such, this document is not to be submitted as part of the PIP, but shall be part of the Technical Proposal.

5.2.3 The CMP shall assure the establishment and maintenance of configuration item records, configuration item life cycle records, and baselines throughout the duration of the contract and provide assurance that all changes to the baselines are performed through a formal change control process once a baseline has been established and agreed.

5.2.4 The CMP shall be structured as a living document compliant with ACMP-1 and subject to revisions and updates, as required. The Contractor shall place the plan under configuration control prior to its implementation and for the life of the Contract.

5.2.5 The CMP shall identify, document and justify the organizational structure, roles and responsibilities, tasks, milestones and procedures to be used by the Contractor to implement the CMP and fulfil the requirements of this Contract.

5.2.6 All Contractor and Purchaser activities and milestones related to CM shall be identified and included in the Project Master Schedule (PMS) of the PMP in the PIP.

5.2.7 The CMP shall at a minimum include the following Sections:

1) Introduction;
2) Organization;
3) Configuration Identification and Documentation;
4) Baselines;
5) Configuration Control;
6) Interface Management;
7) Change Request Process;
8) Configuration Status accounting;
9) Configuration Audits and Reviews;
10) Management Tools.

5.2.8 The Contractor shall provide in the CMP the rationale and criteria for the CI identification and CI numbering for the Purchaser approval, based on the criteria for selection of CIs detailed in [NATO ACMP 2009, 2017].

5.3 Configuration Management Baselines

5.3.1 The Contractor shall provide and maintain Configuration Baselines throughout the performance period of the project. The following baselines shall be created and maintained:

1) Functional Baseline (FBL);
2) Allocated Baseline (ABL);
3) Product Baseline (PBL);
4) Operational Baseline (OBL).

5.3.2 The Contractor shall be responsible for the consistency between the baselines throughout the project. Any update or change shall be introduced formally and revision controlled.

5.3.3 The **Functional Baseline (FBL)** is a set of documents that specifies the functional and non-functional requirements of a service or product and that is used as the approved basis for comparison. In particular the Contractor shall develop and provide the FBL that:

1) Shall be derived from the SRS and shall be established at the successful completion of the SRR with the approved updated SRS.

2) Shall be provided for Purchaser approval following the approval of Final SRR Report. Any changes on the approved FBL shall be requested through ECP.

5.3.4 The **Allocated Baseline (ABL)** is a set of documents that specifies the design of a service or product and is used as the approved basis for comparison. In particular the Contractor shall develop and provide the ABL that:

1) Shall meet the functional and non-functional requirements allocated in the FBL.

2) Shall contain (but is not limited to) the following documents:
   a) System Design Specification;
   b) Test Plan;
   c) Requirement Traceability Matrix (RTM).

3) Shall be established at the successful completion of the FDR.

5.3.5 The **Product Baseline (PBL)** is a set of products and/or services, including supporting documents, which is used as the approved basis for comparison. In particular the Contractor shall develop and provide the PBL that:

1) Shall meet the functional and non-functional requirements allocated in the FBL and the design of the ABL.

2) Shall be established after successful completion of the IV&V Assessment. It reflects the “as-built” configuration of the system.

5.3.6 The Contractor shall provide the CMDB to reflect the PBL upon completion of the CDR with:

1) All related documentation, software, hardware, configuration files, services and any other related information or deliverable necessary to establish the PBL completely

2) A full CI-tree structure prior to CDR that shall be reviewed by the Purchaser for acceptance. The CI-tree shall identify all CI’s and structure them in a functional tree hierarchy from system down to sub-system to assembly down to replaceable item level (i.e. LRUs; SRUs down to replaceable card/port level; software modules).

5.3.7 The **Operational Baseline (OBL)** is a set of products and/or services, including supporting documents that reflect the “as-deployed” (“as-delivered”) configuration of the system. In particular the Contractor shall develop and provide the Operational Baseline (OBL) that:

1) Shall be initially established after successful completion of the PSA,

2) Shall then be finally established after successful completion of FSA.

5.3.8 The Contractor shall provide the CMDB to reflect the OBL upon completion of FSA.

5.4 Configuration Item Identification

5.4.1 The Contractor shall identify and describe hardware, software and documentation Configuration Items (CI’s) as defined in ACMP-2.

5.4.2 The Purchaser reserves the right to modify the CI structure prior to its baselining.

5.4.3 The Contractor shall also identify any PFEs provided for implementation as Configuration Items (CI’s) and integrate them within their CM and related part of the CI structure. The revision or change information for CI control will be provided by the Purchaser.

5.4.4 The Contractor shall chose the Cis to assure visibility throughout the development effort and easy support to the operational system after acceptance. In particular:

1) Every CI and its associated documentation shall have a unique identifier and name.

2) All COTS, adapted, and developed software shall be designated as Computer Software CIs (CSCIs).

3) All subsystem configuration files shall be designated as CSCIs.

4) All stand-alone, bespoke documentation that is not a specification of a CI, but required to operate and maintain the system shall be designated as Documentation Cis (e.g. non-COTS training material and manuals).

5.4.5 The Contractor shall create a Configuration Item (CI) – tree:

1) The Draft CI-tree shall be delivered 4 weeks before System Design Specification (SDS),

2) The Final CI-tree shall be delivered 4 weeks before First Article system Test (FAST).

5.5 Configuration Control

5.5.1 The Contractor shall be fully responsible for the Configuration Control of all CI's and baselines until FSA, and in accordance with ACMP-3.

5.5.2 The Contractor shall be responsible for issuing in a timely manner, as required by this SOW, all approved changes and revisions to all baseline documents included in the Contract. This includes changes originated both by the Contractor and the Purchaser.

5.5.3 Where a change affects more than one document, or affects documents previously approved and delivered, the Contractor shall ensure that the change is properly reflected in all baseline documents affected by that change.

5.5.4 The Contractor shall define the Configuration Baseline Change procedures and shall submit Notice of Revision or Request for Deviations and Waivers when required and approved by the Purchaser. All proposed changes to the baselines (FBL, ABL, PBL, and OBL) shall be submitted to the contractor's Configuration Control Board (CCB) prior to the submission to the Purchaser for approval. The Contractor's internal CCB process shall be defined in the CM Plan. Additionally, the Contractor shall propose an external CCB process to communicate and discuss the changes with Purchaser before officially presenting the changes for approval.

5.6 Engineering Change Proposals (ECP)

5.6.1 The Contractor shall submit change requests in the form of Engineering Change Proposals (ECP) or Requests for Deviation (RfD) or Requests for Waiver (RfW), when required. All requests shall be captured and logged in a change request register to be identified in the CMP. Forms based on ACMP requirements designed by the Contractor for this purpose shall be submitted for approval by the Purchaser prior to use.

5.6.2 Changes to the Contractor's baselined CIs shall be processed as either Class I or Class II ECPs.

1) Class I ECPs shall have to be mutually agreed upon by the Contractor and Purchaser. Extensions to the target times for processing Class I ECPs shall be mutually agreed upon by the Contractor and Purchaser.

2) Class II ECPs shall be submitted by the Contractor to the Purchaser for review and classification concurrence prior to implementation.

3) If the Purchaser's representative does not concur in the classification, Class I ECP procedures shall be applied by the Contractor and then formally submitted to the Purchaser for approval or rejection.

5.6.3 When submitting ECPs, the Contractor shall assign a priority rating of Emergency, Urgent or Routine Extensions to the target times for processing.

5.6.4 The Contractor shall use the configuration control procedures specified in the CMP for the preparation, submission for approval implementation and handling of ECPs to baselined CIs.

5.6.5 Any Engineering Change Proposal shall include, as a minimum, the following information:

1) Reference Number;
2) Requirement affected;
3) Nature of change;
4) Rationale for the change;
5) Impact of change / CIs affected;
6) Description of how the change will be reflected in the delivered system's cost, schedule, and/or performance. This description shall include any trade-offs that shall be considered;
7) Status;
8) Priority.

5.6.6 All design changes shall be included in the technical documentation by the re-issuance. Changes/revisions shall be provided for consideration and approval to the Purchaser by the Contractor in accordance with ECP procedures.

5.6.7 Any ECP affecting FBL shall be submitted by the Contractor to the Purchaser for review, classification concurrence and approval. No Class I ECP affecting the FBL, including a change to a baseline document shall be implemented until it has been approved by the Purchaser.

5.7 Requests for Deviation (RfD) and Requests for Waiver (RfW)

5.7.1 The Contractor shall (if required) prepare, handle, and submit for Purchaser's approval, RfD and RfW as defined in ACMP.

5.7.2 The Contractor shall propose in the CMP an RfD /RfW format based on the requirements in ACMP.

5.7.3 The Contractor shall be aware that permanent departures from a baseline shall be accomplished by ECP action rather than by RfD.

5.8 Deficiency Reports (DRs)

5.8.1 The Contractor shall establish and maintain a process for reporting, tracking, and resolving deficiencies in the Developmental and Product Baselines. Deficiency Reports (DRs) shall document problems during the design, configuration, implementation, or operation of the system.

5.8.2 DRs shall be closed when the identified problem is resolved through procedure or other action that does not affect the system baselines, or when a corresponding Change Request is opened to correct the deficiency through a change to a baseline.

5.8.3 The Deficiency Log shall be maintained by the Contractor and contain the following information:

1) Serial number for each deficiency;

2) Description of the deficiency;

3) Test and test case or event under which the deficiency was first observed (e.g.: FAT, SIT);

4) Date of the observation of the deficiency and expected date of its correction;

5) The personnel raising and endorsing the observation;

6) Any clearance action taken such as repair and testing, notification, receipt of a written reply from the Contractor;

7) The authorized personnel endorsing the correction, and the date of correction;

8) The Contractor’s proposed way forward, in case the deficiency remains, with target dates and description of the intended resolution strategy.

5.8.4 The Deficiency Log shall be first created at the time of First Articles Acceptance Testing, and shall remain updated at PSA and then until FSA.

5.8.5 During testing or other inspection procedures, the Purchaser may observe perceived deficiencies. These Purchaser observations shall be included in the Contractor’s Deficiency Log, and appropriately documented.

5.9 Configuration Status Accounting

5.9.1 The Contractor shall be fully responsible for the Configuration Status Accounting (CSA) for all baselines and CIs in accordance with ACMP-4.

5.9.2 The Contractor shall propose the format of CSA report in the CMP for Purchaser's approval.

5.9.3 The Contractor shall deliver CSA reports to the Purchaser both as part of management and specialist products in this contract and also as standalone documents at the Purchaser's request.

5.9.4 At the end of the Contract, the Contractor shall deliver a set of final CSA reports for each CI in both hard copy and in electronic media.

5.9.5 The Contractor shall provide its Configuration Status Accounting (CSA) database and maintain the database throughout the period of performance of this Work Package.

5.10 Configuration Auditing

5.10.1 The Contractor shall organize and support Purchaser witnessed configuration audits to demonstrate that the actual status of all CIs matches the authorized state of CIs as registered in the CSA Reports compliant with STANAG 4427 and ACMP-5.

5.10.2 The Contractor shall provide (before each configuration audit) the Purchaser with all baseline documentation required to perform the configuration audit. At each audit, the Contractor shall make available the technical personnel capable of answering questions from the Purchaser's auditor.

5.10.3 The Contractor shall organize and execute **Physical Configuration Audits (PCA)** on site at each location not later than two weeks after successful FAST and before PSA. The PCA shall be witnessed by the Purchaser and shall include:

1) A full inventory check of all equipment ,software and documentation delivered on site, including auditing of equipment and cable labelling and marking, safety marking and warnings, part numbers and serial numbers;

2) Verification of manuals and training material to assess consistency between documentation and equipment and software found on site;

3) Verification of design configuration specification against equipment and software found on site;

4) Verification of all change requests against equipment and software found on site.

5.10.4 The Contractor shall solve any deficiencies found during a PCA within the agreed timeframe and update the baseline accordingly.

5.10.5 The Contractor shall deliver not later than four (4) weeks after successful FAST and not later than two (2) weeks after the each PCA the outcome of the PCA in the PCA Report for the Purchaser's approval summarizing the results of the audit.

5.10.6 The Contractor shall organize, support and execute at least one **Functional Configuration Audit (FCA)**, to occur between FAST and the PSA (not later than 2 weeks after successful SAT) that is the Purchaser's formal audit of the equipment performance with regard to the contract's specifications and shall be conducted by the Contractor upon the delivery of the first of each configuration type.

5.10.7 The Contractor shall demonstrate:

1) By means of the system design and test documentation that each of the technical requirements have been satisfied (during the FCA).

2) The configuration documented is the same with the configuration installed in the physical system (before each testing activity and after the changes based on the tests). This shall entail the demonstration of HW and SW configuration.

5.10.8 The Contractor shall deliver not later than 4 weeks after successful FSA, the outcome of the FCA in the FCA report for the Purchaser's approval summarizing the results of the audit.

5.11 Configuration Management Data Base (CMDB)

5.11.1 In the execution of his Configuration Management responsibilities, the Contractor shall employ a Configuration Management System (CMS) incorporating the Configuration Management Database (CMDB).

5.11.2 The Contractor shall deliver a fully populated CMDB to the Purchaser before PSA. The CMDB shall be in a non-proprietary format and free of any use restrictions to the Purchaser.

5.11.3 The Contractor shall provide its entire CMDB file set for Purchaser to be able to import to his CMDB tools and databases products if requested by the Contractor.

5.11.4 The Contractor shall allow the Purchaser access to his CMDB and to the status of all baselines, Configuration Items, Configuration Item Records and Change Records at all times during the execution of the contract.

SECTION 6. QUALITY ASSURANCE (QA)

6.1 General

6.1.1 This section addresses the QA requirements of the project. The purpose of these requirements is to ensure that the Contractor provides all deliverables on time and at the required level of quality by utilising a professional, best practice quality assurance framework and through internal quality control independent from the Contractor's project organisation. A second objective is to minimise the duration of the review cycles and decrease the review workload by ensuring that the Contractor provides mature deliverables only.

6.1.2 Quality Assurance (QA) is as a procedure or set of procedures intended to ensure that a product or service under development meets specified requirements.

6.1.3 Quality Control (QC) is a procedure or set of procedures intended to ensure that a manufactured product or performed service adheres to a defined set of quality criteria or meets the requirements of the Purchaser.

6.1.4 Under this contract the Quality Assurance process is intended as Quality Assurance and Control Process. The term Quality Assurance will include also the Quality Control definition. The Contractor shall establish a Supportability Programme to manage the QA activities within this Contract.

6.1.5 The Contractor's internal Quality Assurance process and system will be required to comply with STANAG 4107 "Mutual acceptance of Government Quality Assurance and usage of the Allied Quality Assurance Publications (AQAP)".

6.1.6 The Contractor shall recognize and accept the application of STANAG 4107 for this Contract and sub-contracts thereof. The Contractor shall use AQAP 2070 as guidance to the delegation of QA.

6.1.7 The Contractor shall provide all necessary assistance to the Purchaser QA Representative (QAR), or his delegated National Quality Assurance Representative (NQAR), if and when Quality Assurance (QA) activities are delegated in accordance with STANAG 4107.

6.1.8 If sub-contracted quality resources are used, the Contractor's Quality Assurance Process shall describe the controls and processes in place for monitoring the sub-Contractor's work against agreed timelines and levels of quality.

6.1.9 The following reference documentation is for QA purposes.

Abbreviation	Full document Name and Reference
[STANAG 4107, Ed.11]	Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications. Ed.11, 2019.
[AQAP-4107, Ed.A, Ver.2]	Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications (AQAP). Ed. A, Ver.2, 2018.
[AQAP-2000, Ed.3]	NATO Policy on an Integrated System Approach to Quality Through the Life Cycle. Ed.3, 2009.
[AQAP-2070, Ed.B, Ver.3]	NATO Mutual Government Quality Assurance (GQA). Ed.B, Ver.3, 2015.
[AQAP-2105, Ed.C, Ver.1]	NATO Requirements for Quality Plans. Ed.C, Ver.1, 2019.
[AQAP-2110, Ed.D, Ver.1]	NATO Quality Assurance Requirements for Design, Development and Production. Ed.D, Ver.1, 2016.
[AQAP-2131, Ed.C, Ver.1]	NATO Quality Assurance Requirements for Final Inspection and Test. Ed.C, Ver.1, 2017.

Table 6-1 Quality Assurance Reference Documents

6.2 Quality Assurance Plan (QAP)

6.2.2 The Contractor shall establish, execute, and maintain an effective Quality Assurance Plan (QAP) throughout the period of performance of this Contract. The Contractor’s QA Process shall be described in the QA Plan. The process is subject to approval by the Purchaser, or its delegated representative(s), whenever it does not meet the Quality Assurance requirements that are stated in this contract. The Contractor shall organize QA Review meetings starting from the first draft of QA Plan. The location of the first meeting shall be Contractor’s facilities and ad-hoc meetings shall be arranged upon agreement.

6.2.3 The Contractor shall establish and maintain an effective QA organization to implement the QAP and manage the QA functions. It shall be managed independently of the management of the project.

6.2.4 The QAP shall describe the Contractor’s QA organization, QA programme, roles and responsibilities and procedures to ensure that all activities are performed in accordance with the requirements of this Contract.

6.2.5 The Contractor’s designated Quality Assurance Manager shall ensure that all required roles, responsibilities, processes and control mechanisms are identified and implemented to make sure that all the functional, non-functional requirements within the scope of the contract are analysed, planned and satisfied.

6.2.6 The Contractor’s QAP shall be structured as a living document subject to revision/update, as required.

6.2.7 The Contractor’s QAP shall reference or document and explain the Contractor’s QA procedures for analysis, software support, development, design, production, installation, configuration management, control of Purchaser furnished property, documentation, records, programming standards and coding conventions, library controls, reviews and audits, testing, corrective action and certification as specifically related to this project.

6.2.8 The QAP shall apply to all hardware, software, documentation, activities, services and supplies that are designed, developed, acquired, maintained or used, including deliverable and non-deliverable items.

6.2.9 The QAP shall also ensure that the exchange of deliverables from the Contractor to the Purchaser shall be adequately controlled, and that no deliverables shall be presented by the Contractor without adequate quality control and sign-off by the Contractor’s QA Manager.

6.2.10 The Contractor’s QAP shall be compatible and consistent with all other plans, specifications, standards, documents and schedules, which are utilized under this Contract.

6.2.11 All Contractor procedures referenced in the QA Plan shall either be submitted with the plan, or described in the plan and made available for review by the Purchaser upon demand.

6.2.12 All Contractor and Purchaser activities and milestones related to QA shall be identified and included in the Project Master Schedule (PMS) of the PMP in the PIP.

6.2.13 The QA Plan and all related QA procedures shall be subject to Purchaser approval.

6.2.14 The Contractor shall maintain a QA log during the lifetime of the project in which records are kept accounting for all QA-activities, most notably all QA reviews. All accounting shall be done through dating and sign off by the responsible QA person. The QA log shall enable the Purchaser to verify if and when a deliverable has been QA reviewed and by whom and with what result.

6.3 Quality Assurance Process

6.3.2 The Quality Assurance (QA) implemented by the Contractor shall apply to all hardware, software (including firmware) and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract. This includes non-deliverable test and support hardware and software.

6.3.3 The Contractor's QA Process shall ensure that procedures are developed, implemented and maintained to adequately control the development, design, production, testing and configuration of all deliverables.

6.3.4 Personnel performing QA functions shall have specific documented definitions of their assigned duties. In no case shall the QA personnel managing or performing QA functions be the same personnel responsible for performing other tasks that are reviewed by QA.

6.3.5 The Contractor shall demonstrate, with the Quality Assurance process, that the processes set up for design, develop, produce and maintain the product will assure the product will meet all the requirements.

6.3.6 If sub-contracted quality resources are used, the Contractor's Quality Management Process shall describe the controls and processes in place for monitoring the sub-Contractor's work against agreed timelines and levels of quality.

6.3.7 The Contractor shall assure that all the test and procedure used to demonstrate the requirements will be monitored and controlled under the QA process.

6.3.8 The Contractor shall periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser POC.

6.3.9 The Contractor shall on request provide the Purchaser with a copy of any subcontracts or orders for products related to the contract.

6.3.10 The Contractor shall notify Purchaser if a subcontract or order has been identified as constituting or involving risk.

6.3.11 The Contractor shall flow down the applicable contractual requirements to Sub-suppliers by referencing the stated contractual requirement, including relevant AQAP(s).

6.3.12 The Contractor shall be responsible of ensure that the procedures and processes required to fulfil contract requirements are fully implemented at the Sub-supplier's facilities.

6.4 Auditing of Contractor Performance

6.4.2 The Purchaser reserves the right to perform Reviews and Quality audits at any of the Contractor (or Sub-Contractor(s)) facilities.

6.4.3 Audit activities at Sub-supplier's facilities do not relieve the Contractor and Subcontractors from any contractual quality responsibilities.

6.4.4 The Purchaser may engage auditors to evaluate the performance of the Contractor (or Sub-Contractor(s)) and verify, validate Contractor (or Sub-

Contractor(s)) deliverables. The auditors can also monitor, assess, and report any perceived problem areas.

6.4.5 The auditors may be requested by the Purchaser to monitor Contractor activities at Contractors' facilities or other sites related to the development, testing and implementation of the contract. The Contractor shall fully support such activities and in particular:

6.4.5.1 Host inspection visits by Purchaser's auditors;

6.4.5.2 Make himself available for answering questions and furnishing all the information related to the project;

6.4.5.3 Allow the Purchaser's auditors to inspect and monitor testing activities;

6.4.5.4 Allow the Purchaser's auditors to inspect and monitor the Contractor's processes and tools applicable to this project.

6.4.6 The Contractor shall transfer to the Purchaser's auditors all information deemed necessary to perform the activities, on his own initiative or on request by Purchaser's auditors.

6.4.7 A non-exhaustive list of information that the Contractor shall transfer to the Purchaser's auditors includes minutes of meetings, planning documents, source code, requirements documents, and database, design, test and other technical documentation.

6.4.8 Based on the Audit results if there are any disconformities or irregularities with the contract requirements, the Contractor shall immediately make necessary corrections and take necessary precautions to ensure the satisfaction of the requirements.

6.5 Certificate of Conformity

6.5.2 The Contractor shall be solely responsible for the conformance to requirements, of products provided to the Purchaser.

6.5.3 The Contractor shall deliver all the Certificate of Conformity (CoC) for products, COTS SW (including firmware) and hardware released by the COTS Vendors unless otherwise instructed.

6.5.4 The CoC is a document, signed by the Supplier, which states that the product conforms with contractual requirements and regulations

6.5.5 The CoC verifies the process quality-enabled items produced or shipped comply with test procedures and quality specifications prescribed by the customer. It presents data derived from quality management information.

6.5.6 Any CoC delivered by the Contractor shall be part of the acceptance data package of the product and shall be provided before the start of any Site Acceptance Tests.

SECTION 7. TESTING AND ACCEPTANCE

7.1 Testing Approach

7.1.1 The Purchaser requires a set of testing activities to verify the SEMARCIS's capability's compliance with the requirements of the SoW.

7.1.2 The Contractor shall have the overall responsibility for meeting the SEMARCIS's capability testing requirements and conducting all related activities. This includes the development of all test documentation, personnel, tools and test equipment required under this Contract, the conduct of all testing and the evaluation and documentation of the tests results.

7.1.3 All testing activities such as FAST and PSA shall be detailed in the Test and acceptance Plans (TP or TAP).

7.1.4 Test Plan shall be coordinated with the purchaser and approved by the purchaser prior to FAST.

7.1.5 Testing shall be performed according to TAP.

7.1.6 Airtime expenditures associated to development, FAST, PSA testing and training preparation will be borne by the Contractor using Contractor owned SIM cards.

7.1.7 The testing comprises:

7.1.7.1 The First Article System Test (FAST).

7.1.7.2 Provisional System Acceptance (PSA) testing.

7.1.7.3 Final System Acceptance (FSA) testing.

7.1.8 During the testing the Contractor shall prove compliance through any combination of the following demonstrations as directed by the Purchaser:

7.1.8.1 Testing Ship to Shore communication for voice and data services, secure or non-secure,

7.8.1.2 Testing Ship to Ship communication for voice and data services, secure or non-secure,

7.1.9 Showing Certificates of Compliance and/ or equipment specifications.

7.1.10 The Purchaser has the right to observe the FAST and PSA testing

7.1.11 The Purchaser has the right to requires Contractor to perform additional selected testing tasks, to confirm compliance.

7.1.12 As the supporting documentation for each test session the Contractor shall develop Test Plans (refer to § 7.6.1).

7.2 First Article System Test

7.2.1 During the FAST the Contractor shall prove that the design and integration of the SEMARCIS capability meets the following requirements of the SRS in the following areas:

7.2.1.1 Functional Requirements

7.2.1.2 Performance Requirements

7.2.1.3 Physical Requirements

7.2.1.4 Environmental Requirements

7.2.1.5 Equipment Miscellaneous Requirements.

7.2.2 The Contractor shall conduct FAST at their premises.

7.2.3 Demonstration of compliance of Functional Requirements shall be performed as testing between two SEMARCIS units.

7.2.4 The Contractor shall document the FAST results in a FAST Test Report.

7.2.5 The Purchaser has the right to include deficiencies in the FAST Test Report, also if outside the scope of the areas as defined in 7.2.1 or not part of the FAST Test Plan.

7.2.6 PFS and PFE will not be provided to the Contractor, therefore:

7.2.6.1 The Contractor shall emulate the functional specifications of the NATO IP crypto by using a router based IP SEC VPN.

7.2.6.2 The Contractor shall use its own subscription to the Commercial Satellite Services.

7.2.6.3 The Contractor shall be responsible for the installation and configuration of the Windows 10 Operating System on the laptops used for FAST.

7.3 Provisional System Acceptance (PSA) testing

7.3.2 For PSA testing the Contractor shall, at the Contractor Premises, verify the correct operation of all components of each SEMARCIS unit, including keys and buttons, data interfaces, fans, displays, disks, cables, power supplies, batteries, transmission functions etc. as detailed in the Test Plan.

7.3.3 The Contractor shall document the PSA testing test results in a PSA Test Report.

7.3.4 The Purchaser has the right to include deficiencies in the PSA Test Report, also if outside the scope of the areas as defined in 7.2.1 or not part of the PSA Test Plan.

7.4 Provisional System Acceptance

7.4.1 In order to request Provisional System Acceptance (PSA) of the SEMARCIS units the Contractor shall have completed the following actions:

7.4.1.1 Successful completion of FAST and PSA testing, including approval by the Purchaser of the associated Test Reports.

7.4.1.2 Delivery of all the System Documentation, as per § 3.4 and 4.8.

7.4.1.3 Delivery of all the SEMARCIS units as per SSS.

7.4.2 The Purchaser will evaluate whether to accept delivery of the SEMARCIS units depending on the type and nature of any identified deficiencies during FAST and PSA testing.

7.5 Final System Acceptance (FSA)

7.5.1 The conditions for Final Systems Acceptance (FSA) are that all equipment and services as detailed in the Schedule of Supplies and Services have been delivered and all deficiencies noted at the Provisional Systems Acceptance (PSA) tests have been cleared by the Contractor to the satisfaction of the Purchaser.

7.5.2 PRM 4 is designated as the FSA meeting and will take place at the Purchaser’s premises in Brussels.

7.6 Test Plans

7.6.1 The Test Plan shall document how Contractor plans to verify that SEMARCIS capability meets the SRS requirements.

7.6.2 For each SRS requirement to be tested the Contractor shall provide a Test Plan containing the following information:

7.6.2.1 Its objective, by clearly identifying the SRS requirement intended to be demonstrated by the test procedure.

7.6.2.2 The SEMARCIS CIs and facilities and test equipment involved.

7.6.2.3 Any conditions which shall be satisfied prior to application of the test.

7.6.2.4 The test setup.

7.6.2.5 The data to be collected.

7.6.2.6 The sequence of testing steps in the procedure, to a level of detail that enables full understanding by the Purchaser of the purpose and effect of each test step.

7.6.2.7 The expected outcome.

7.6.2.8 The means of measurement or assessment for the test.

7.6.2.9 The results of each test called for in the Test Plan shall be recorded in test results sheets incorporated in the relevant test procedure.

7.6.3 Each test will only be declared 'passed' if the entirety of the expected results were obtained when running the test.

7.6.4 The Purchaser will review all the Contractor's Test Plans for correctness, completeness, and acceptance.

7.7 Test Failures

7.7.1 Should a failure occur during testing, a failure report shall be raised by the Contractor and a preliminary investigation shall be immediately carried out in order to classify the failure as one of the following:

7.7.1.1 Class "A": there is evidence that the cause was an external or transient condition;

7.7.1.2 Class "B": there is mutual agreement that the cause was an inherent design or manufacturing deficiency in the unit under test; or

7.7.1.3 Class "C": When the specific nature of the cause cannot be immediately determined and a more detailed investigation is required before a conclusion can be drawn.

7.7.2 The Contractor shall be responsible for all costs related to the rectification of deficiencies or failures and subsequent re-testing caused by the design or production of the deliverables identified during the verification and/or testing cycles. The Contractor shall be responsible for any travel, subsistence and other incidental expenses incurred by the Purchaser as a result of the requirement for the re-performance of tests necessitated by test failures.

7.7.3 After remedial action has been taken by the Contractor, the test may be resumed at the step during which the deficiency or failure was identified, however, the Purchaser shall have the right to require that re-testing includes all of the tests related to the verification of that particular specification requirement.

7.7.4 The Contractor shall seek the Purchaser's agreement of a mutually suitable time when testing shall be resumed, subsequent to the Purchaser having accepted the contents of a formal submission by the Contractor providing full details describing the cause of the failure and the recommended remedial actions to be taken.

7.8 Test Reports

7.8.1 The Contractor shall document the FAST, PSA and FSA Test results in a Test Report. The Test Report cover sheet shall clearly show whether the testing passed, failed, or was not run, and for what reasons.

7.8.2 The Test Report shall include:

7.8.2.1 Test procedures

7.8.2.2 Test result for each test procedure (Pass, Fail, Not run)

7.8.2.3 Test summary, indicating which test procedures resulted in Fail or Not Run.

7.8.2.4 Any annotations by the Purchaser's representative

7.8.2.5 Comments

7.8.2.6 Contractor representative signature

7.8.2.7 Purchaser representative signature.

7.8.3 On completion of the FAST and PSA Tests, the Contractor shall forward the Test Reports to the Purchaser for review and approval. Purchaser approval of both Test Reports is a condition for PSA as defined in 7.4.1.

SECTION 8. SECURITY ACCREDITATION

8.1 Introduction

8.1.1 The SEMARCIS Deployable CIS (DCIS) needs to achieve security accreditation in order to be granted the authorisation for operational use. Therefore, the security accreditation process established by the appropriate Security Accreditation Authority (SAA) is to be followed.

8.1.2 The primary objective of security accreditation is to ensure that an adequate level of protection is achieved and maintained throughout the life cycle of the SEMARCIS. This includes ensuring that the SEMARCIS conforms to NATO Security Policies and Directives identified in the paragraph 8.2 below, and in the SEMARCIS-specific security-related documentation (SRD) (see paragraph 8.4).

8.1.3 The security accreditation of the SEMARCIS DCIS is to follow a structured process based on the high level requirements established in the Management Directive on CIS Security (ref. 8.2.2.8), as detailed in this document. Deviations from this structured process are to always be documented and can only be authorised by the appropriate SAA.

8.1.4 The Security accreditation is to be granted by the SAA for the SEMARCIS to store, process and/or transmit NATO information in its desired environment.

8.2 Applicable Documents

8.2.1 SECAN Doctrine and Information Publication

8.2.1.1 Selection and Installation of Equipment for the processing of Classified Information (SDIP-29/2), NATO RESTRICTED, dated March 2015

8.2.2 NATO Security Documents

8.2.2.1 The following NATO Security documents are applicable:

8.2.2.2 Security within the North Atlantic Treaty Organisation (C-M (2002)49), COR 12, dated 14 September 2015

8.2.2.3 Directive on Personnel Security (AC/35–D/2000–REV7), dated 07 January 2013

8.2.2.4 Directive on Physical Security (AC/35–D/2001–REV2), dated 07 January 2008

8.2.2.5 Directive on Security of Information (AC/35–D/2002–REV4), dated 17 January 2012

8.2.2.6 Directive on Classified Project and Industrial Security (AC/35–D/2003–REV5), dated 13 May 2015

8.2.2.7 Primary Directive on CIS Security (AC/35-D/2004-REV3), dated 15 November 2013

8.2.2.8 Management Directive on CIS Security (AC/35-D/2005-REV3), dated 12 October 2015

8.2.2.9 INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms (AC/322-D/0047-REV2 (INV), NATO RESTRICTED, dated 11 March 2009

8.2.2.10 Technical and Implementation Directive on CIS Security (AC/322-D/0048 – REV3), NATO RESTRICTED, dated 18 November 2019

8.2.2.11 INFOSEC Technical & Implementation Directive on Emission Security (AC/322-D (2019)0021), NATO RESTRICTED, dated 25 Apr 2019

8.2.2.12 Guidelines for the Security Accreditation of CIS (AC/35-D/1021-REV3), dated 31 January 2003

8.2.2.13 Guidelines for Security Risk Assessment and Risk Management of CIS (AC/35-D/1017–REV2), dated 26 June 2017.

8.2.2.14 Guidelines for the Development of Security Requirement Statements (SRSs) (AC/35-D1015–REV3), NATO RESTRICTED, 31 January 2012

8.2.2.15 Guidelines for the Structure and Content of Security Operating Procedures (Sec OPs) for CIS (AC/35-D/1014-REV3), dated 31 January 2012

8.2.2.16 INFOSEC Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS) (AC/322-D/0030-REV5), NATO RESTRICTED, dated 23 February 2011

8.2.2.17 INFOSEC Technical & Implementation Guidance for the Interconnection of Communication and Information Systems (CIS) (AC/322-D (2005)0040), dated 17 October 2015

8.2.2.18 INFOSEC Technical and Implementation Directive on the requirement for, and the Selection, Approval and Implementation of Security Tools (AC/322-D (2004)0030, NATO RESTRICTED, dated 17 May 2004

8.2.2.19 Guidance on the Marking of NATO Information (AC/322-N(2011)0130 dated 16 June 2011

8.2.2.20 INFOSEC Technical and Implementation Guidance for the Protection of CIS from Malicious Software (AC/322-D (2004)0019(INV), dated 09 March 2004

8.2.2.21 INFOSEC Technical and Implementation guidance on Identification and Authentication (AC/322-D (2005)0044), NATO RESTRICTED, dated 26 October 2005

8.2.2.22 INFOSEC Technical & Implementation Directive for Transmission Security (AC/322-D/0049), NATO RESTRICTED, dated 29 April 2002

8.2.2.23 Security Configuration Catalogue, NCI Agency Cyber Security Service Line, v.1.9, December 2017

8.2.2.24 NATO Secret CIS Security Reference Baseline, Security Mechanisms (SMs) Requirements for Core and Site Services, version 2.0, dated 05 July 2017.

8.2.4 NATO Templates

8.2.4.1 The following NATO Templates are applicable:

8.2.4.2 Security Accreditation Plan Template, version 4.0, dated 08 July 2016

8.2.4.3 CIS Description Template, version 2.0, dated 02 May 2017

8.2.4.4 Security Risk Assessment (SRA) Report (NATO PILAR) Template, version 1.0, dated January 2013

8.2.4.5 System Security Requirements Statement (SSRS) Template, version 3.0, dated 12 January 2018

8.2.4.6 Abbreviated System Interconnection Security Requirements Statement (A-SISRS) Template, version 1.0, dated 19 September 2017

8.2.4.7 Secure AIS Generic Sec OPs, version 1.0 dated 20.05.2014

8.2.4.8 Generic Security Test & Verification Plan, version 1.0, dated 17 February 2014

8.2.4.9 Electronic Security Environment Conformance Statement (ESECS) Template, dated 05.02.2018.

8.2.4.10 Approval for Test Request Template, dated 23.01.2017

8.3 Security Accreditation Requirements

8.3.1 The Security Accreditation Process for SEMARCIS, as described in the NATO Security Policies and Directives SHALL be strictly followed by the Contractor and SHALL encompass overall development, production and implementation of the SEMARCIS DCIS.

8.3.2 A verification that security measures (personnel security, physical security, security of information, CIS security controls), including security baselines identified in the respective System-specific Security Requirement Statements (SSRS) and Sec OPs have been properly implemented in accordance with the requirements of the Security Accreditation Authority is one of the primary bases for the security accreditation for the SEMARCIS.

8.3.3 This verification is carried out by the SAA and typically supported by appropriate results of security testing conducted based upon agreed Security Test and Verification Plan (STVP) which is to cover all security requirements identified and approved in form of System-specific Security Requirement Statement (SSRS).

8.3.4 Due to the SEMARCIS architecture and its operational purpose (DCIS), Electronic Security Environment (ESE) assessment process is to be decoupled from the assessment provided for the Global Security Environment (GSE) and Local Security Environment (LSE). This is because for the SEMARCIS, being deployable CIS, both target GSE and LSE are unknown and cannot be addressed in advance. As the opposite, appropriate evaluation of ESE for the SEMARCIS will be done before any deployment.

8.3.5 The achievement of security accreditation for SEMARCIS is related with development and Security Accreditation Authority (SAA) approval of necessary Security-related Documentation (SRD). The Contractor should expect a number of review rounds per document before it will be approved.

8.3.6 Coordination with the SAA will be conducted by the Purchaser.

8.3.7 In support of producing the deliverables the Contractor SHALL closely engage directly with representatives of the Purchaser and/or Security Accreditation Authority (through the Purchaser) in order to discuss particular security-related requirements but also to clarify and/or enhance the documentation to be provided as part of the Security-related Documentation.

8.3.8 This process SHALL be organised in the form of one or more workshops that SHALL be attended by the Contractor and by representatives of the Purchaser. Location of the meetings and workshops will be defined by the Purchaser and will typically take place at a facility located on the Purchasers site. The Contractor may be invited to provide briefings and/or technical expertise for meeting(s) with the SAA.

8.3.9 The SAA may provide advice and instructions to the Contractor on any security implication or any proposed change based on the findings and results of the assessments and/or security tests.

The advice, instructions and guidance from the SAA SHALL be considered by the Contractor. The Contractor SHALL take action(s) to follow, carry out the necessary work and to implement the advice, instructions and guidance given by the SAA.

8.3.10 The Contractor SHALL recognize the NATO Security Policies and supporting Directives, in order to take into account all related requirements in the resulting SEMARCIS system design and installation thereof.

8.3.11 The Contractor SHALL take into account the NATO CIS security requirements for the implementation and support of NATO SECRET (NS) security domain in the deployed environment, respectively.

8.3.12 The Contractor SHALL be responsible to develop and implement the SEMARCIS system in accordance with the NATO CIS security requirements and provide all required security-related documentation for SEMARCIS system (in English language) in order to achieve security accreditation of the SEMARCIS DCIS.

8.3.13 Security accreditation for SEMARCIS needs to be achieved before the system is to be put into the operation(s).

8.3.14 When there will be a requirement to test the specific SEMARCIS deployable kit(s) or its element(s) before this is used in its final operational environment, the SAA may grant an Approval for Testing by identifying specific conditions for the AfT including, for example, the scope of tests, the classification of information involved in the testing, the test plan and the timeframe for the AfT. The Contractor SHALL coordinate with the Purchaser all AfT requirements and provide filled AfT Request (based on the Purchaser provided template to the Purchaser as required. The Purchaser is to coordinate this request with SAA.

8.3.15 Approval for Testing is typically required (but not limited) to conduct necessary security testing in accordance with Security Test and Verification Plan (STVP).

8.3.16 Depending on the infrastructure involved, functional testing of SEMARCIS may also require AfT to be issued by the SAA.

8.3.17 All of the equipment shall be compliant with TEMPEST (emission security) requirements of SDIP-29/2 for Radiated and Conducted Emissions.

8.3.18 The software not included on AFPL shall follow Configuration Change Process (CCP) run by NCI Agency, and granted approval by the Change Advisory Board (CAB) before applications are implemented into the NATO systems.

8.4 Security-related Documentation

8.4.1 The Security-related Documentation (SRD) in support of the accreditation process, comprised of the following deliverables in English language, SHALL be provided by the Contractor except the Security Accreditation Plan that will be developed by the Purchaser:

8.4.1.1 Security Accreditation Plan

8.4.1.2 CIS Description

8.4.1.3 Security Risk Assessment (SRA) including SRA Report

8.4.1.4 System Specific Security Requirement Statement (SSRS)

8.4.1.5 Security Operating Procedures (Sec OPs)

8.4.1.6 Security Test and Verification Plan (STVP)

8.4.1.7 Security Test and Verification Report (STVR) and

8.4.1.8 Electronic Security Environment (ESE) Conformance statement (ESECS)

8.4.2 The Contractor SHALL produce key security-related documentation or inputs to documents in support of the SEMARCIS security accreditation, as detailed below.

8.4.3 The Contractor shall produce required documentation or inputs to documents using templates (as listed in Table 1 - Security Accreditation Documentation and Contractor Responsibility) provided by the Purchaser. **These will be provided after contract award.**

8.4.4 Security Accreditation Plan (SAP)

8.4.4.1 The Security Accreditation Plan describes the steps to be taken to achieve security accreditation for SEMARCIS DCIS.

8.4.4.2 The Security Accreditation Plan for the SEMARCIS is to be developed by the Purchaser and presented for the approval to the SAA. This document will be made available to the Contractor **after contract award**.

8.4.4.3 The Contractor SHALL strictly adhere to the security accreditation activities described in the SAP as approved by the SAA. All activities related with the security accreditation process SHALL be identified in the respective Project Implementation Plan (PIP) and in the Project Management Plan (PMP).

8.4.4.4 The SAP SHALL be maintained by the Purchaser during the project.

8.4.4.5 Any changes required by the Customer to be incorporated into the SAP SHALL be provided to the Purchaser who will (if accept the changes from the overall contractual obligation) coordinate this with SAA.

8.4.5 CIS Description

8.4.5.1 The CIS Description for SEMARCIS is the first document in support to security accreditation

8.4.5.2 To be developed **after contract award**.

8.4.5.3 The CIS Description for SEMARCIS DCIS SHALL be developed by the Contractor based on Purchaser's provided template and shall be approved by the SAA (through the Purchaser).

8.4.5.4 The CIS Description SHALL be formulated at the earliest stage of the project (SEMARCIS planning stage) and SHALL be further enhanced as the project develops.

8.4.5.5 The CIS Description document SHALL at a minimum include but not limited to the following information:

1) Detailed technical description showing the main components and the high level as well as detailed information flows,

2) Description of all internal and external connections of the system,

3) List of hardware and software components used,

4) Overview of the security mechanism which are going to be implemented in the SEMARCIS DCIS.

8.4.5.6 The Contractor developed CIS Description SHALL be submitted to the Purchaser for review before they will be provided to the SAA for approval.

8.4.5.7 The Contractor SHALL take into account any comments from the reviewers and SAA and SHALL update the CIS Description document as many times as necessary in order to obtain SAA approval.

8.4.5.8 The Contractor SHALL maintain and keep the CIS Description document up to date throughout the project.

8.4.6 Security Risk Assessment (SRA)

8.4.6.1 The Security risk assessment is the process of identifying security risks, i.e. the threats and vulnerabilities of a CIS, determining their magnitude and identifying areas needing countermeasures. Security risk assessment serves to identify the risks that exist, identify the current security posture of the CIS in respect to handling information, and then assemble the information necessary for the selection of effective security countermeasures, based upon NATO Security Policy and supporting Directives and Guidance.

8.4.6.2 The Security risk assessment contributes to the decision on which security measures are be required, and how the apportionment between technical and alternative security measures can be achieved, and gives an unbiased assessment of the residual risk.

8.4.6.3 The Security Risk Assessment (SRA) for the SEMARCIS SHALL be conducted by the Contractor with the support of the Purchaser (as required) and based on the information provided in the CIS Description document. SRA is to be approved by the SAA.

8.4.6.4 SRA SHALL be conducted in accordance with AC/35-D/1017 (ref. 8.2.2.13).

8.4.6.5 The Contractor SHALL use the SRA application “PILAR” with NATO profile for producing the Security Risk Assessment for the SEMARCIS.

8.4.6.6 The Contractor SHALL use the NATO template “SRA Report (PILAR) to document the results of the SRAs.

8.4.6.7 Objective of the SRA is to define the security objectives of confidentiality, availability and integrity/authenticity of the designed SEMARCIS systems according to the particular services to be provided by the resulting SEMARCIS system, the values of the traffic and information stored and transported over the SEMARCIS system, and the nature and levels of the particular threats being identified.

8.4.6.8 The Contractor SHALL organise SRA workshop(s) at Purchaser or Contractor facility. Respective Purchaser’s Subject Matter Experts (SMEs) shall be invited to support proper assessment. It has been anticipated that at least 2 (two) up to 5 (five) days SRA workshops will be required.

8.4.6.9 The Security Risk Assessment process for the SEMARCIS shall include the following stages:

1) Identification of the scope and objective of the security risk assessment (which shall be agreed with the Purchaser and SAA);
2) Determination of the physical, personnel and information assets which contribute to the fulfilment of the mission of the SEMARCIS;
3) Determination of the value of the physical and personnel assets;

4) Determination of the value of the information assets against the following impacts: disclosure, modification, unavailability and destruction;

5) Identification of the threats and vulnerabilities to the risk environment and their level;

6) Identification of existing countermeasures;

7) Determination of the necessary countermeasures and a comparison with existing measures; identifying those countermeasures which are already installed and identifying those countermeasures which are recommended.

8.4.6.11 Based on the results of the Security Risk Assessment SRA, the Contractor shall identify areas of SEMARCIS DCIS requiring safeguards and countermeasures to comply with NATO Security Policy and supporting Directives. The decision on specific security mechanisms shall be based on evidence(s) and results produced by the Security Risk Assessment.

8.4.6.12 Where the implementation of security measures results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components, the Contractor shall consider these changes to be within the technical and financial scope of this Contract; no Engineering Change Proposal (ECP) shall be generated.

8.4.6.13 Here the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand, an ECP shall be raised by the Contractor.

8.4.6.14 The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conducts update of SRA document as many times as necessary in order to obtain SAA approval.

8.4.6.15 The SRA for the SEMARCIS shall be composed as a standalone document.

8.4.7 Systems-specific Security Requirement Statement (SSRS)

8.4.7.1 The System-specific Security Requirement Statement (SSRS) is a complete and explicit statement of the security principles to be observed and of the detailed security requirements to be met.

8.4.7.2 SSRS specifies how security is be achieved, managed and checked.

8.4.7.3 The SSRS for SEMARCIS DCIS shall be developed by the Contractor based on Purchaser’s provided template and shall be approved by the SAA (through the Purchaser).

8.4.7.4 The SSRS shall be formulated at the earliest stage of the project (SEMARCIS planning stage) and shall be further developed and enhanced as the project develops.

8.4.7.5 The Contractor’s developed SSRS shall:

1) Describe the minimum levels of security deemed necessary to countermeasure the risk(s) identified in a risk assessment;

2) have a unique identifier for each security requirement;

3) Indicate mandatory and recommended Security Mechanisms (SMs).

8.4.7.6 SSRS shall be based on NATO Security Policy and supporting Directives and the Security Risk Assessment. The SSRS for SEMARCIS shall also take into consideration parameters covering the operational environment such as the lowest level of personnel security clearance, the highest classification of information handled, the security mode of operation and other Purchaser's specific requirements.

8.4.7.7 The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of SSRS document as many times as necessary in order to obtain SAA approval.

8.4.7 Security Operating Procedures (Sec OPs)

8.4.7.1 Security Operating Procedures (Sec OPs) are a description of the implementation of the security measures to be adopted, the operating procedures to be followed and the responsibilities of the personnel.

8.4.7.2 Sec OPs for SEMARCIS DCIS shall be developed by the Contractor based on Purchaser's provided template and shall be approved by the SAA (through the Purchaser).

8.4.7.3 Sec OPs for the SEMARCIS shall contain separate chapters for personnel performing security management as well as administrative functions (e.g. Core Administrators, Local Administrators, and CIS Security Officer) and SEMARCIS users.

8.4.7.4 Sec OPs for the SEMARCIS, as a minimum, shall include following sections:

1) Administration and organisation of security, including points of contact;
2) Personnel security, physical security, security of information;
3) CIS Security;
4) Incident and emergency procedures;
5) Configuration management;
6) Acceptable use policy.

8.4.7.5 Sec OPs shall also cover all security requirements identified in the SRA and SSRS which are not fully fulfilled by technical countermeasures. For example, following security procedures should be addressed (not exhaustive list):

1) System configuration and maintenance;

2) System backup;
3) System recovery, etc.

8.4.7.6 The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of Sec OPs document as many times as necessary in order to obtain SAA approval.

8.4.8 Security Test and Verification Plan (STVP)

8.4.8.1 A Security Test and Verification Plan (STVP) is a description of the security testing and verification of the CIS Security measures to be implemented for the SEMARCIS.

8.4.8.2 The STVP for SEMARCIS DCIS shall be developed by the Contractor based on Purchaser's provided template and shall be approved by the SAA (through the Purchaser).

8.4.8.3 The STVP shall describe in details the tests which will demonstrate compliance with the security requirements for the SEMARCIS DCIS identified in the respective SSRS and Sec OPs.

8.4.8.4 The Contractor shall ensure that the STVP defines a complete and detailed sequence of steps to be followed to prove that the security mechanisms designed into SEMARCIS enforce the security requirements identified in the SEMARCIS SSRS.

8.4.8.5 For each security test the following details shall be identified:

1) The objective of the security test;

2) An outline description of the security test;

3) A description of the execution of the security test (too include technical instructions how to conduct the test);

4) The pass criteria for the security test.

8.4.8.6 The Contractor shall ensure that each and every security test is cross-referenced to the corresponding security requirements from the SEMARCIS SSRS (identified by the unique identifier) as well as to the tested security mechanisms (SMs).

8.4.8.7 The Contractor shall ensure all security requirements and security mechanisms identified for the SEMARCIS are planned for testing.

8.4.8.8 The Contractor shall execute the STVP for the SEMARCIS DCIS and develop respective Security Test and Verification Report (STVR).

8.4.8.9 Execution of STVP conducted at Purchaser's SHALL be witnessed by the Subject Matter Expert (SME) designated by the Purchaser. He /She is to countersign respective STVR(s).

8.4.8.10 The Contractor SHALL also develop, provide and maintain the initial and any updated Security Implementation Verification Procedures (SIVP) for the SEMARCIS DCIS as part of Security Tests.

8.4.8.11 These procedures SHALL consist of a set of software scripts and inspection procedures that SHALL allow a CIS Security Officer to verify that all components of the SEMARCIS DCIS have been installed and configured property and comply with the SSRS and SecOPs.

8.4.8.12 The Contractor SHALL take into account any comments from the SAA (provided to the Contractor through the Purchaser) and SHALL conduct update of STVP and/or SIVP documents as many times as necessary in order to obtain SAA approval.

8.4.9 Security Test and Verification Report (STVR)

8.4.9.1 A Security Test and Verification Report (STVR) is a description of the results for the every instance of security testing conducted based on STVP.

8.4.9.2 The Contractor SHALL develop STVR for every instance of security testing conducted based on STVP.

8.4.9.3 The STVR template for the SEMARCIS DCIS SHALL be developed by the Contractor based on Purchaser’s provided document.

8.4.9.4 For each security test the following details SHALL be identified in the STVR:

1) Test ID;

2) An outline description of the security test;

3) The pass criteria for the security test;

4) Detailed results of the security tests;

5) Test status (e.g. in progress, passed, failed)

6) Test completion (in per cent);

7) Failure severity (e.g. critical, serious, major, less important, none);

8) Test date;

9) An info about who conducted the test;

10) An information about who witness the test;

8.4.9.5 STVR SHALL contain overall test summary details:

1) Identification of the element under tests (SEMARCIS deployable kit(s));

2) Tests starting date;

3) Tests finishing date;

4) Amount of all tests to be conducted;

5) Amount of tests executed;

6) Tests passed;

7) Tests failed;

8) Tests still in progress;

8.4.9.6 Amount of findings with clear distinguish of their severity (e.g. critical, serious, major, less important).

8.4.9.7 As the part of the SVTR preparation, the Contractor SHALL also fill the Electronic Security Environment (ESE) Conformance Statement (ESECS) based on the Purchaser provided template (ref. 8.2.4.9). ESECS after the Purchaser approval (signature) will be provided together with the test results (in form of the STVR) to the SAA as required for Deployable CIS.

8.4.9.8 Detailed SEMARCIS deployable kit configuration SHALL be depicted in the associated ESECS. If virtual infrastructure is to be used, all deployed virtual machines SHALL be also identified.

8.4.9.9 A separate ESECS SHALL be filled be the Contractor for each SEMARCIS deployable kit.

8.4.9.10 ESECS is to be issued per deployable kit (regardless of configuration similarities between kits) as changes might be applied in the future for each kit separately.

8.4.9.11 The Contractor SHALL take into account any comments from the SAA (provided to the Contractor through the Purchaser) and SHALL conduct update of STVR (this might require some security tests to be re-conducted) and ESECS as many times as necessary in order to obtain SAA approval.

8.5 Responsibilities

8.5.1 Table below summarizes responsibilities related to the development of each document required for security accreditation process.

8.5.2 Column “Baseline/Guidance” lists available templates, relevant NATO Security Directives and Guidance, and similar documentation.

8.5.3 The Contractor shall undertake the work identified in the column ‘Contractor Responsibility’ in Table 1.

Document	Baseline/Guidance	Contractor Responsibility (The Contractor shall :)	Purchaser Responsibility
SAP	SAP template	None	Develop and update SAP Coordination with the SAA

CIS description	CIS description template	Based on the design adjust it to the CIS description template focusing on security aspects Develop CIS description	Provide applicable documents, templates and guidance to the Contractor Review Coordination with the SAA
SRA	[AC/35-D/1015] [AC/35-D/1017] Tool for formal SRA: NATO PILAR SRA Report template	Conduct SRA Provide the inputs to the SRA per system design. Provide assets identification. Provide safeguards (technical and organizational measures – information security) identification and valuation. Develop SRA Report	Support Contractor in conducting SRA Review Coordination with the SAA
SSRS	[AC/35-D/1015]	Develop SSRS Provide technical input to SSRS	Provide SSRS template to the Contractor. Indicate SSRS sections to be completed by the Contractor. Complete remaining SSRS sections. Provide guidance to the Contractor. Review Coordination with the SAA
SecOPs	[AC/35-D/1014]	Develop Sec OPs for users and system administrators	Provide Sec OPs template to the Contractor. Indicate Sec OPs sections to be completed by the Contractor. Complete remaining Sec OPs sections. Provide guidance to the Contractor. Review

			Coordination with the SAA
STVP	[AC/35-D/2005] STVP template	Develop STVP The STVP shall refer to SSRS Develop detailed STVP test procedures Execute STVP	Provide template and guidance to the Contractor Review Coordination with the SAA Witness the testing conducted by a contractor
STVR	STVR template	Develop STV Report	Provide template and guidance to the Contractor Review Coordination with the SAA
ESEC	ESEC template	Provide ESEC per CIS (kit)	Provide template and guidance to the Contractor Review Coordination with the SAA

Table 8-1 - Security Accreditation Documentation and Contractor Responsibility

SECTION 9. LIST OF ACRONYMS

Acronym	Description
ABDs	As Build Drawings
ABL	Allocated Base Line
ACMP	Allied Configuration Management Publication
AQAP	Allied Quality Assurance Publications
AfT	Approval for Testing
PBI	Breakdown Element Identifier
CAB	Change Advisory Board
CCB	Configuration Control Board
CCP	Configuration Change Proposal
CDR	Critical Design Review
CDRL	Data Requirement List
CI	Configuration Item
CIS	Communication and Information Systems
CLIN	Contract Customer Line Item Number

CM	Configuration Management
CMDB	Configuration Management Data Base
CMP	Configuration Management Plan
CMS	Configuration Management System
CoC	Certificate of Conformity
COTS	Commercial Off The Shelf
CSA	Configuration Status Accounting
CSCIs	Computer Software Configuration Items
CSR	Configuration Status Report
CSSC	CIS Sustainment Support Centre
CV	Curriculum Vitae
DMS	Diminishing Manufacturing Sources
DPs	Deficiency Reports
ECP	Engineering Change Proposals
EDC	Effective Date of Contract
ESE	Electronic Security Environment
ESECS	Electronic Security Environment Conformance Statement
FAST	First Article System Test
FCA	Functional Configuration Audit
FBL	Functional Base Line
FDR	Final Design Review
FMECA	Failure Mode Effects and Critical Analysis
FSA	Final System Acceptance
GUI	Graphics Unit Interface
GSE	Global Security Environment

ILS	Integrated Logistic Support
ILSP	Integrated Logistic Support Plan
IRC	Internet Relay Chat
IV&V	Independent Validation and Verification
LCM	Life Cycle Management
LORA	Level of Repair Analysis
LRUs	Line Replaceable Units
LSA	Logistics Support Analysis
LSE	Local security Environment
MDS	Material Data Sheet
MTA	Maintenance Task Analysis
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
NMCRL	NATO Master Cross Reference List
NNN	Non NATO Nation
NQAP	National Quality Assurance Representative
NSN	NATO Stock Number
RfD	Request for Deviation
OBL	Operational Base Line
OEM	Original Equipment Manufacture
OTS	Off the Self
PCA	Physical Configuration Audits
PFE	Purchaser Furnished Equipment
PFS	Purchaser Furnished Services
RfW	Request for Waiver

RTM	Requirement Traceability Matrix
PBL	Product Base Line
PHS&T	Packaging Handling S
PIP	Project Implementation Plan
PLT	Provisioning Lead Time
PM	Project Manager
PMP	Project Management Plan
PMS	Project Master Schedule
POE	Power Over Ethernet
PPR	Project Progress Report
PRM	Project Review Meeting
PSA	Provisional System Acceptance
PSR	Project Status Report
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QAP	Quality Assurance Plan
QC	Quality Control
RAMT	Reliability Availability Maintainability Testability
RCIL	Recommended Consumable Item List
RTTL	Recommended Spare Parts List
SAA	Security Accreditation Authority
SAP	Security Accreditation Plan
SDS	System Design Specification
Sec OPs	Security operations Procedures
SEMARCIS	Secure Maritime CIS

SIP	Session Initiation Protocol
SISRS	System Interconnection Security Requirement Statement
SIVP	Security Implementation Verification Procedures
SLCM	System Life Cycle Management
SMs	Security Mechanisms
SoW	Statement of Work
SRA	Security Risk Assessment
SRD	Security Related Documentation
SRS	System Requirements Specifications
SSRS	System Security Requirement Statement
SSD	Solid Security Drive
SSS	Schedule of Supplies and Services
STVP	Security Test and Verification Plan
STVR	Security Test and Verification Report
TAP	Test and Acceptance Plan
TAT	Turn Around Time
TP	Technical Publications
TPs	Technical Plans
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX A: SYSTEM REQUIREMENTS SPECIFICATION

A.1 GENERAL

A.1.1 Scope of this Appendix

A.1.1.1 This Appendix to the SEMARCIS SoW provides the System Requirements Specification (SRS) for the SEMARCIS capability.

A.1.1.2 For the background and introduction to the requirements please refer to SECTION 1, subsections 1.2.

A.1.2 Interpretation of requirements

A.1.2.1 When ‘include’ is used in a requirement this shall be interpreted as ‘include, but not be limited to’.

A.1.2.2 When ‘support’ is used in a requirement this shall be interpreted as including everything (such as hardware, software, firmware, licenses, and configuration) needed to meet the requirement.

A.1.2.3 When PoE (Power over Ethernet) is used in the requirements this shall be understood as PoE according to IEEE 802.3af or IEEE 802.3at.

A.1.3 Quantities

A.1.3.1 The equipment quantities in this SRS do not address spares. For the quantities of equipment to be delivered please refer to the SSS.

A.2 FUNCTIONAL REQUIREMENTS

A.2.1 WAN Connectivity

A.2.1.1 The connectivity between all locations (the SEMARCIS WAN) shall be based on PFS (please refer to 3.3.3.1), and is further detailed in the paragraphs below.

A.2.1.2 The implementation shall follow an IP addressing scheme provided by the Purchaser.

A.2.1.3 PFS Commercial Satcom Services

A.2.1.3.1 The SEMARCIS units for the ships shall each provide a satellite terminal capable of using the IP network services of the PFS Commercial Satcom Services.

A.2.1.3.2 The SEMARCIS satellite terminal shall provide all components required to access the PFS Commercial Satcom Services, including outdoor unit/ antenna, cabling, indoor unit/ transceiver, power supply etc.

A.2.1.3.3 The SEMARCIS satellite terminal shall support the local SEMARCIS user to switch between volume (commonly known as 'standard') and duration based transmission modes (commonly known as 'streaming') of the PFS Commercial Satcom Services.

A.2.1.3.4 The default transmission mode shall be volume based.

A.2.1.3.5 For the duration based transmission modes the SEMARCIS satellite terminal shall support the local SEMARCIS user in selecting, starting and stopping data rates of 32 kbps, 64 kbps and 128 kbps.

A.2.1.3.6 The SEMARCIS satellite terminal shall automatically stop the duration based transmission modes after 30 minutes.

A.2.1.3.7 When using the SEMARCIS satellite terminal to access the PFS Commercial Satcom Services the connectivity for SECRET file transfer shall use a transmission mode charged on the volume of data transferred rather than being duration based.

A.2.1.3.8 When using the PFS Commercial Satcom Services the connectivity for SECRET level voice (VoIP) shall use the duration based transmission (selected, started and stopped by the local SEMARCIS user).

A.2.1.3.9 The SEMARCIS capability shall for volume based billing schemes automatically resume connectivity through the PFS Commercial Satcom Services after access to the Commercial Satcom Services was interrupted and restored.

A.2.1.3.10 The control of the SEMARCIS satellite terminal through a GUI shall be possible using the handset for PSTN calls (please refer to A.7.2).

A.2.1.4 PFS Unclassified bearers

A.2.1.4.1 The SEMARCIS units for the ships shall each provide a commercial VPN device to support the use of PFS unclassified bearers that may already be present between the ships and the static land based location.

A.2.1.4.2 For the static land based location the Contractor shall provide a firewall and a commercial VPN device.

A.2.1.4.3 The configuration (in the meaning of 'settings') of the commercial VPN device and the firewall is outside the scope of this SoW.

A.2.2 PSTN access for ships

A.2.2.1 The SEMARCIS units for the ships shall provide PSTN access through the PFS Commercial Satcom Services (please refer to 3.3.3 for the PFS), accessed through the SEMARCIS satellite terminal (please refer to A.2.1.3.1).

A.2.3 SECRET level communications

A.2.3.1 The SEMARCIS units shall provide communications at SECRET level between any of the eight ships, and the static land based location.

A.2.3.2 Communications at SECRET level shall be protected by the use of the PFE NATO IP crypto (please refer to 3.3.4).

A.2.3.3 Direct ship-to-ship communications at SECRET level shall be possible independent of SECRET level systems outside the SEMARCIS systems of the communicating ships.

A.2.4 SECRET level capabilities

A.2.4.1 The SEMARCIS units shall provide a File Transfer capability, a Voice capability, and a Printing capability, all at SECRET level.

A.2.4.2 The File Transfer capability shall:

1) Be provided through browser based downloads using an HTTP server which is to be implemented on each SEMARCIS laptop.
2) Implement the HTTP server using the webserver (IIS) of the Windows operating system.
3) Support any file type and extension.
4) Be optimized for the use of the PFS WAN, please refer to A.2.5
5) Use URLs referring to ship names (rather than using IP addresses in the browser). These URLs shall follow a name to IP address mapping scheme which will be provided by the Purchaser.

A.2.4.3 The Voice capability shall:

1) Be provided through dedicated VoIP handsets (i.e. not through a laptop based softphone).
2) Power the VoIP handsets via PoE.
3) Operate through direct IP-dialling, i.e. without the need for any SIP server outside the phones.
4) Implement the direct IP-dialling through a directory with named ship identifiers on the handsets, rather than the user having to enter IP addresses.
5) Be interoperable with the Cisco 504G, using SIP and RTP.
6) Be optimized for the use of the PFS WAN, please refer to A.2.5.

A.2.4.4 The Printing capability shall:

1) Be provided through one printer per ship.

2) Be based on USB connectivity to the SEMARCIS laptops.

A.2.5 WAN Optimization

A.2.5.1 The Contractor shall configure and document settings for the operating system, applications and handsets in relation to the use of the Commercial SATCOM Services in such a way that:

1) The data rate required for the SECRET level voice is less than 32 kbps at the interface of the satellite terminal during a call, and no data is transmitted when there is no call or call setup.

2) File transfer response time and transfer time is as short as possible.

3) The cost of using the satellite capacity (i.e. required data rate, transferred volume, duration of a connection) is as low as possible

A.2.6 User devices

A.2.6.1 The SEMARCIS units shall at each ship provide:

1) Two SECRET level laptops

2) One SECRET level VoIP handset.

3) One SECRET level Ethernet switch to:

   a. Simultaneously connect at least two SECRET level laptops and one SECRET level VoIP handset to the NATO IP crypto. The switch port of the SECRET level VoIP handset may be used to connect (daisy chain) one SECRET level laptop.

   b. Power the VoIP SECRET level handset through PoE.

4) One handset for PSTN calls that is interoperable with the satellite terminal, PoE powered.

5) One SECRET level printer as per A.2.4.4

A.2.6.2 The SEMARCIS unit at the static land based location shall provide:

1) Two SECRET level laptops

2) Two SECRET level VoIP handsets.

3) One SECRET level Ethernet switch to:

   c. Simultaneously connect at least three SECRET level laptops and three SECRET level VoIP handsets simultaneously to the NATO IP crypto.

   d. Power the VoIP SECRET level handsets through PoE.

A.2.7 Media adaptation

A.2.7.1 The SEMARCIS units shall support connectivity at the ships between:

1) The handset for PSTN calls and the SEMARCIS satellite terminal:
   a. Over CAT6 cabling.
   b. Over OM2, OM3 and OM4 cabling with LC connectors.
2) The NATO IP crypto and the SEMARCIS satellite terminal:
   a. Over CAT6 cabling.
   b. OM2, OM3 and OM4 cabling with LC connectors.
3) The NATO IP crypto and the SECRET level Ethernet switch:
   a. Over CAT6 cabling.
   b. Over OM2, OM3 and OM4 cabling with LC connectors.

A.2.7.2 All media converters shall provide PoE to power the handsets.

A.2.7.3 The Ethernet switches shall be compatible with the connectivity as in A.2.7.1 point 3), so directly connect to the NATO IP crypto without media converter.

A.2.7.4 The support of CAT6 cabling and OM2, OM3 and OM4 cabling as per A.2.7.1 is not required simultaneously, so the Ethernet switch or media converters may use SFPs (to be provided by the Contractor) for media adaptation.

A.3 PHYSICAL REQUIREMENTS

A.3.1 Packaging

A.3.1.1 For each ship based SEMARCIS unit components shall for storage and transport be placed into at least two Transport Cases as follows:

1) CIS Transport Case: This case will include all CIS components (NATO IP crypto, laptops, printer, handset for secure voice communication, Ethernet switch, media converters, removable storage media, VPN device, cabling, mounting accessories, user manual(s), power supplies etc. etc).
2) SATCOM Transport Case: This case will include all components for using the PFS Commercial SATCOM Services (so satellite terminal, with all accessories, PSTN handset).

A.3.1.2 When the total weight of the CIS transport case exceeds the limits of A.3.3 a second CIS transport case shall be provided to transport the VPN device, with additional room available for the NATO IP Crypto.

A.3.1.3 Antenna poles and cable reels will be transported outside the Transport Cases.

A.3.1.4 The SEMARCIS unit shall be operated outside the Transport Cases.

A.3.1.5 The Transport Cases shall be equipped with lockable latches (i.e. through lock and key or combination lock).

A.3.1.6 The Transport Cases shall be stackable during transport and storage, as a minimum stacking six Transport Cases onto one vertical pile shall be supported.

A.3.1.7 The Transport Cases shall each feature a retractable extension handle, two wheels suitable for use on unpaved roads, and one properly placed carry handle for a one-man lift, and two additional carry handles on opposite sides of the Transport Case if the Transport Case with its components weighs more than 20 kg.

A.3.1.8 The Transport Cases shall be constructed such that:

1) Component removal from and addition to the Transport Cases is possible without tools.

2) Cushioning inside the Transport Cases is durable and permanently shaped to fit the components, e.g. using cut foam structures. Use of pick and pluck foam, loose fill, bubble wrap etc. is not permitted.

A.3.2 Installation

A.3.2.1 Installation accessories shall be provided for:

1) The indoor unit of the satellite terminal (including power supply) to enable mounting on a horizontal or vertical surface.

2) The satellite terminal handset (i.e. a cradle).

A.3.2.2 Installation shall be possible with generic tools.

A.3.2.3 The indoor SEMARCIS components shall feature non-slip rubber feet to prevent slipping and scratching.

A.3.2.4 All cables included in the Transport Cases shall be supplied with Velcro cable holders or similar.

A.3.3 Size and Weight

A.3.3.1 The weight of each Transport Case including contents shall not exceed 25 kg.

A.3.3.2 The diameter of the antenna unit (with enclosure) shall not exceed 35 cm.

A.4 OPERATIONAL REQUIREMENTS

A.4.1 Maintainability

A.4.1.1 The SEMARCIS equipment MTTR provided in this contract shall be: MTTR<30 min (for HL1-2/SL1-2) and MTTR<90 min (for HL3/SL3)

A.4.1.2 Mean Time To Repair (MTTR) shall be calculated for all kind of failures (critical and non-critical) and shall include fault isolation, access, disassembly, remove and replace, reassembly, configuration, check-out and start-up, and to exclude administrative and logistics delay times. Evidence to be provided through the MTA logistics database and deviation to this requirement shall be justified (if any).

A.4.1.3 The SEMARCIS equipment MTTRS provided in this contract shall be: MTTRS<20 min (for HL1-2/SL1-2) and MTTRS<60 min (for HL3/SL3)

A.4.1.4 Mean Time to Restore the System (MTTRS) shall be calculated for critical failures only and shall include fault isolation, access, disassembly, remove and replace, reassembly, configuration, check-out and start-up, and to exclude administrative and logistics delay times. Evidence to be provided through the MTA logistics database and deviation to this requirement shall be justified (if any).

A.4.2 Supportability

A.4.2.1 The SEMARCIS equipment provided in this contract shall have the following corrective maintenance levels apportionment (weighted with the relevant failure rate):

A.4.2.1.1 Critical and Non-Critical maintenance: [HL1-2/SL1-2]>80% and [HL3/SL3]<15% and [HL4/SL4]<5%;

A.4.2.1.2 Critical maintenance: [HL1-2/SL1-2]>90% and [HL3/SL3]<10% and [HL4/SL4]=0%

A.4.2.2 Evidence to be provided through the MTA logistics database and deviation to this requirement shall be justified (if any).

A.4.2.3 The SEMARCIS equipment provided in this contract shall have preventive hardware maintenance limited to HL1/SL1-2. Evidence to be provided through the MTA logistics database and deviation to this requirement shall be justified (if any).

A.4.2.4 The SEMARCIS equipment provided in this contract shall have corrective hardware maintenance HL2-3 field-replaceable, without specialised tools.

A.4.2.5 The SEMARCIS shall make use of COTS components. Parts such as cables, connectors, sockets and batteries, consumables and attaching parts shall be available as COTS through multiple sources.

A.4.3 Safety

A.4.3.1 The SEMARCIS components related to power supply shall meet the applicable standards for Electrical safety of the Low Voltage Directive (LVD), 2006/95/EC, or equivalent national or international standards.

A.4.4 Scalability

A.4.4.1 The SEMARCIS capability shall allow simultaneous SECRET file transfer between all ships (any to any).

A.4.4.2 The SEMARCIS capability shall allow each ship to make simultaneously one SECRET level voice call and one PSTN call.

A.4.5 Usability

A.4.5.1 The SEMARCIS components (including PFE) shall all have durable, clearly readable and understandable labels indicating ‘SEMARCIS’ followed by the SEMARCIS number and the (abbreviated) function (e.g. SEMARCIS1-PC1-PSU).

A.4.5.2 The SEMARCIS components shall be able to withstand the daily use by non-CIS military personnel including unpacking, complete setup, breakdown and packing during three years.

A.4.5.3 The Transport Cases shall be tagged using 36 point font size durable labels.

A.4.5.4 These labels and stencils shall be placed such that they are readable from all sides.

A.5 SECURITY REQUIREMENTS

A.5.1 TEMPEST

A.5.1.1 All data cables for shall be CAT6 SF/UTP.

A.5.1.2 All equipment for use at SECRET level shall be certified to TEMPEST level C for Radiated and Conducted Emissions, with the exception of the laptops which shall be certified to TEMPEST level B for Radiated and Conducted Emissions.

A.5.2 System Hardening Requirements

A.5.2.1 The Ethernet switches be unmanaged switches or shall be protected against unauthorized access. This includes:

1) Disabling of remote access.
2) Password protection of menu’s using non-default passwords.
3) Mitigations against published vulnerabilities.
4) Use of most recent firmware.

A.5.2.2 The terminals for the Commercial Satcom Services shall be protected against unauthorized access or use. This includes:

1) Disabling of USB and wireless interfaces.
2) Password protection of menu's and remote access using non-default passwords.
3) Mitigations against published vulnerabilities.
4) Use of most recent firmware.

A.5.3 Communication Security Requirements

A.5.3.1 For Communication Security all SECRET traffic shall pass through the PFE IP crypto.

A.5.3.2 The VPN device shall support NSA Suite B cryptography.

A.6 ENVIRONMENTAL REQUIREMENTS

A.6.1 General

A.6.1.1 The SEMARCIS units shall meet or exceed the requirements below for operation, transport and storage.

A.6.2 Vibration

A.6.2.1 Outdoor components, operational: Random spectrum 1.05 g rms x 3 axes: 5 to 20 Hz: 0.02 g2/Hz 20 to 150 Hz: -3 dB/ octave

A.6.3 Shock

A.6.3.1 The SEMARCIS Transport Cases and the protection to their contained components shall comply with the ISO 8768 Toppling Test (only non-operational).

A.6.3.2 These in-case shock requirements shall be met when the cases contain all their components and when they are only partially filled.

A.6.3.3 The laptop, shall comply with MIL-STD 810G, Method 516.6 Procedure IV (Transit Drop) but with 75 cm drop height, operational.

A.6.3.4 The satellite terminal shall comply with MIL-STD-810G, Method 516.6, Procedure I, 20g, 11 millisecond, half-sine, operational.

A.6.4 Temperature

A.6.4.1 The minimum requirement is an ambient temperature of:

1) +5 to +35 degrees Celsius for indoor components, operational.
2) -25 to +55 degrees Celsius for outdoor components, operational.

3) -40 to +85 degrees Celsius for outdoor components, non-operational.

4) -10 to +60 degrees Celsius for all components, storage and transportation.

A.6.4.2 **Dust and water**

A.6.4.3 The SEMARCIS Transport Cases and the protection to the components inside the cases shall comply with IP67 during transport and storage.

A.6.4.4 The SEMARCIS outdoor components shall be water proof according to IPX6 or better operational and non-operational.

A.6.4.5 The SEMARCIS components shall be cleanable with a cloth and not require opening for cleaning.

A.6.4.6 **Movement**

A.6.4.7 The antenna tracking shall be capable of handling:

1) Roll +/- 30 deg. per. 4 s.

2) Pitch +/- 15 deg. per. 3 s.

3) Yaw +/- 10 deg. per. 5 s.

4) Surge +/- 0.5g.

5) Sway +/- 0.5g.

6) Heave +/- 0.7g.

7) Turning rate +/- 36˚/s; Acc. 12˚/s².

A.7 EQUIPMENT MISCELLANEOUS REQUIREMENTS

A.7.1 Laptops

A.7.1.1 The SEMARCIS laptops shall meet the requirements listed below:

1) Screen size between 13 inch and 16 inch.

2) Minimum resolution 1366 x 768.

3) One Ethernet interface.

4) Minimum 8 GB RAM.

5) Minimum CPU Intel Core i5 8th generation.

6) QWERTY keyboard, US layout, spill resistant.

7) Touchpad.

8) Minimum 3 USB ports.

9) Integrated sound card with speaker(s).

10) Battery operation: minimum 3 hrs.

11) Non-reflective screen, minimum brightness 250 nits.

12) No permanent storage other than BIOS and a single Solid State Drive (SSD) of minimum 240 GB capacity

13) SSD removal/ insertion shall be possible without violation of the TEMPEST certification.

14) SSD removal/ insertion shall be possible without specialised tools.

15) Bluetooth and Wifi shall have been removed or disabled in the BIOS.

16) RS232 serial port (may be provided as USB based external adapter).

A.7.1.2 Each laptop shall be compatible with, and be provided with drivers for:

1) Microsoft Windows 10 Enterprise 64 Bit.

A.7.2 Satellite terminal with handset

A.7.2.1 The satellite terminal shall support phone (PSTN) and fax calls, volume based IP services and guaranteed data rate IP services of at least 32 kbps.

A.7.2.2 The satellite terminal shall run the most recent production ready firmware.

A.7.2.3 The handset shall support PSTN calls via the satellite terminal.

A.7.2.4 The handset shall be powered through PoE.

A.7.2.5 The satellite terminal shall provide through the handset a user interface which lets the user indoors control and monitor its operation without requiring the use of any additional devices.

A.7.2.6 To support testing and training at land each satellite terminal shall be provided with accessories to operate the antenna on a stable horizontal surface with cables connected (e.g. feet that can be screwed into the bottom of the antenna). These accessories shall be included in the Transport Case.

A.7.3 Printer with cartridges

A.7.3.1 The printer shall meet the following requirements:

1) Minimum paper size A4.

2) Minimum resolution of 1200 x 1200 dpi colour, 600 x 600 dpi black and white.

3) Suitable for frequent usage, transport and storage.

4) The printer drivers shall be included, and shall be compatible with the laptop hardware and software.

5) The printer shall feature no permanent data storage. Data shall not be retained after the printer is switched off and it is packed for transport.

6) Two sets of spare cartridges, and one set of printer head cleaning accessories shall be included with the printer.

7) Maximum weight 2.5 kg (excluding spare cartridges and cleaning accessories).

8) Maximum dimensions 37 x 20 x 10 cm

9) USB connectivity, a USB cable shall be included.

10) Any wireless interfaces of the printer shall have been removed or permanently disabled.

A.7.4 SECRET level handset

A.7.4.1 The handset for phone calls at SECRET level calls shall feature at least:

1) A codec and packet size settings suitable for meeting the bandwidth requirements as indicated in A.2.5.

2) A backlit display.

3) A LED indication for missed calls.

4) A speakerphone.

5) List of missed calls.

6) Microphone mute.

7) Directory dialling.

8) IP or URL dialling.

A.7.4.2 Power supplies shall be included

A.7.5 Set of transport cases

A.7.5.1 No Miscellaneous Requirements

A.7.6 Ethernet switch

A.7.6.1 No Miscellaneous Requirements

A.7.7 VPN device

A.7.7.1 The VPN device shall support EIGRP, MPLS and DMVPN.

A.7.7.2 No end of sale date shall have been announced for the VPN device by its manufacturer.

A.7.7.3 The minimum aggregate deterministic throughput as specified by the manufacturer shall be 50 Mbps.

A.7.7.4 The minimum aggregate deterministic throughput as specified by the manufacturer shall be upgradeable to 100 Mbps.

A.7.7.5 The VPN device shall feature at least one SFP port.

A.7.7.6 The VPN device shall feature at least two RJ45 ports.

A.7.7.7 The VPN device shall feature one serial console port and one USB console port.

A.7.7.8 The maximum dimensions are 44.55 x 369.57 x 294.64 mm.

A.7.7.9 The VPN device shall include all necessary accessories for 19” rack mounting of the device.

A.7.7.10 The VPN device shall be listed on the NCIA Approved Fielded Product List (AFPL) which currently includes the Cisco ASR1000 and Cisco ISR4000 series.

A.7.8 Firewall

A.7.8.1 A firewall, Palo Alto Networks PA-3220 shall be provided. The license for the firewall is PFE.

A.7.9 Ancillaries

A.7.9.1 LAN cabling

A.7.9.1.1 The Non-PFE CAT6 LAN cabling shall be snagless or otherwise protected against RJ45 clip damage.

A.7.9.1.2 The length of the non-PFE LAN cabling shall be at least two meter.

A.7.9.1.3 Both fiber optic and CAT6 cabling shall be provided.

A.7.9.2 Antenna mounts

A.7.9.2.1 A mast mount kit shall be provided for each satellite terminal to interface a 1½” tube.

A.7.9.3 Mains power socket adapter

A.7.9.3.1 A universal mains power socket adapter shall be provided for each SEMARCIS unit that fits sockets of at least Australia, Italy, UK and US and allows the connection of a CEE7/7 plug.

A.7.9.4 Antenna poles

A.7.9.4.1 Poles must be of 316 stainless steel.

A.7.9.4.2 Pole outer diameter 48.3 or 50.0 mm, wall thickness sufficient to support the satellite terminal antenna on a vessel in all weather conditions.

A.7.9.4.3 Length 145- 150 cm.

A.7.9.4.4 Protective end caps on pole.

A.7.9.4.5 Steel clamps to attach the pole supporting the antenna to poles of 25 to 115 mm. May be provided as a combination of multiple size ranges (e.g. 25 -50 mm and 50-115 mm).

A.7.9.4.6 Minimum two clamps per antenna pole.

A.7.9.4.7 One set of spare nuts and bolts per clamp.

A.7.9.4.8 Padded carry bag with room for clamps (fishing rod bag).

A.7.9.5 Encrypted Removable Storage Media

A.7.9.5.1 Encrypted Removable Storage Media shall be delivered with the following specifications:

1) For each ship:
   a. 1 x Viasat Eclypt Freedom 600 1TB HDD (FET-IL6-100050UM)
   b. 2 x KeyStone User Tokens (EKS-02USBH)
   c. 1 x Un-Programmed Key Token (FSEKM01)
   d. 2 x Serialised Holographic Tamper Evident Label (LFXS000186)
2) For all ships combined:
   a. 1 x Eclypt Universal Key Management Kit (FSECCKU)

A.7.9.6 Antenna cabling

A.7.9.6.1 With each satellite terminal antenna cabling shall be provided with mounted connectors and according to electrical specifications recommended by the satellite terminal manufacturer.

A.7.9.6.2 The length of the antenna cabling for each ship shall be at least twenty meter.

A.7.9.6.3 Antenna cabling and connectors shall be watertight and salt water and UV resistant.

A.7.9.6.4 In addition 6 x 100 meter LMR600-DB cable on reels shall be provided together with 60 male TNC connectors for LMR600 type EZ-600-TM-X.

A.8 ELECTRICAL POWER REQUIREMENTS

A.8.1 Mains power

A.8.1.1 The SEMARCIS unit shall be operated from mains power of 90 – 240V, 47 – 63Hz.

A.8.1.2 The SEMARCIS unit shall provide power distribution to power all components from a single mains power outlet (when all components are located together).

A.8.1.3 The SEMARCIS unit shall feature an IEC C14 power inlet.

A.8.1.4 The length of the power cord from the SEMARCIS unit to the mains power outlet shall be 3 meter or more.

A.8.1.5 The power cord from the SEMARCIS unit to the mains power outlet shall feature a CEE7/7 plug and an IEC C13 plug.

A.8.1.6 All devices shall be delivered with power cords with a CEE7/7 plug.

A.8.1.7 For operating the satellite terminal and two media converters away from the main SEMARCIS unit a power strip with IEC C14 power inlet shall be included with every SEMARCIS unit.

A.8.2 Maintenance

A.8.2.1 Any fuses or circuit breakers inside the components shall be field resettable or replaceable.

A.8.2.2 Spare fuses shall be provided for each SEMARCIS unit.

APPENDIX B: PFE NATO IP ENCRYPTION DEVICE SPECIFICATION

B.1 INTRODUCTION

B.1.1 Specification interpretation

B.1.1.1 The specifications below are an approximate indication of functions, interfaces, weight and dimensions for initial design purposes.

B.1.1.2 Detailed specifications will be provided to the Contractor after Contract award.

B.1.2 IP encryption device model

B.1.2.1 The IP encryption device is the Thales TCE621 BLACK, and will be provided as PFE.

B.1.3 Included accessories

B.1.3.1 The NATO IP encryption device includes as PFE all required accessories for its operation (a power supply with power cables, Ethernet cables and media converters).

B.2 FUNCTIONAL SPECIFICATIONS

B.2.1. The NATO IP encryption device shall for design and testing assumed to behave similar to an IP VPN device with the following functional specifications:

1) Static routing and addressing only
2) IPSEC encryption, AES 256 bits in tunnel mode
3) NAT transparency/ traversal with static translation only

B.3 PHYSICAL SPECIFICATIONS

B.3.1 The dimensions of the NATO IP encryption device are 440 x 44.4 x 250 mm

B.3.2 The dimensions of the power supply are 90 x 45 x 25 mm.

B.3.3 The weight of the NATO IP encryption device with all accessories shall be assumed to be 4.1 kg.

B.4 POWER SUPPLY

B.4.1 A 90 – 240V, 47 – 63Hz power supply is included.

B.5 CABLING

B.5.1 Ethernet

B.5.1.1 Two Ethernet cables are included.

B.5.1.2 The connector type is RJ45 on one end and snatch connector on the other end.

B.5.1.3 The bending radius is 150 mm.

B.5.1.4 The cable length is 3 meters.

B.5.2 Power

B.5.2.1 One mains power cable and one DC power cable (PSU to IP encryption device) are included.

B.5.2.2 The mains power cable plug type is CEE7/16.

B.5.2.3 The length of each cable is 2 metres.

B.5.3 Fiber Optic

B.5.3.1 Media converters are included that can be directly mounted to the NATO IP encryption device.

B.5.3.2 The media converters provide a 100BASE-FX interface with LC connectors.

APPENDIX C: MAINTENANCE AND SUPPORT CONCEPT

C.1 SCOPE

This Appendix specifies the Maintenance Levels, the Support Levels and the relevant activities to be carried on by the involved actors.

The SOW specifies who is responsible for what, at the various Maintenance/Support levels from PSA to the End of Warranty.

Before PSA the responsibility of any maintenance/support activity is and remains with the Contractor.

C.2 MAINTENANCE CONCEPT

C.2.1 General

C.2.1.1 A Maintenance Concept is a definition of the maintenance objectives, line of maintenance, indenture levels, maintenance levels, maintenance support and their interrelationships.

C.2.1.2 A Maintenance Concept is applied both for hardware and software and produces maintenance tasks that will be performed on site, at civil or military maintenance facilities, at industry (OEM, Contractor) maintenance facilities.

C.2.1.3 The Maintenance concept identifies who-does-what-at-what-level in accordance with the Maintenance levels and definitions defined below.

C.2.2 Maintenance Levels (line of maintenance)

C.2.2.1 A maintenance level is the position in an organization where specified levels of maintenance are to be carried out. The line of maintenance is characterized by the skill level of the personnel, the facilities and tools provided, the location, etc. There are four (4) maintenance levels to ensure the highest possible availability of the Product.

C.2.2.2 Maintenance Level 1: implies a fast and easy exchange of Maintenance Significant Items (MSIs) performed on the product by organizational personnel when a malfunction occurs;

C.2.2.3 Maintenance Level 2: implies exchange of MSIs and/or the replacement of modules, performed on the product by organizational personnel when a malfunction occurs;

C.2.2.4 Maintenance Level 3: implies the repair of subassemblies, modules and MSIs after their replacement at maintenance level 1 and level 2. Testing on test-benches or integration tests can be included. This maintenance level can be performed either on product (e.g. on-site) or at specific repair shops/facilities;

C.2.2.5 Maintenance Level 4: all repairs and overhaul activities beyond level 1 to level 3 capabilities must be ensured (e.g.: repair of subassemblies, modules and LRUs after their replacement at maintenance level 1 to level 3; major modifications to improve the design and/or operational activities will be prepared and, if necessary, embodied at this level).

C.2.3 Hardware Maintenance and Hardware Change

C.2.3.1 The hardware maintenance is:

- Corrective:
  - Deferred: maintenance carried out to perform a Remove & Replace action of a faulty item not affecting system operation. It is done in a time slot that does not further impact the Operational Availability (e.g. during a schedules maintenance downtime period) or on "live" equipment if this is possible (e.g. when active redundancy or hot stand-by are implemented).
  - Run-to-failure: maintenance carried out to perform a Remove & Replace action of a faulty item affecting system operation (critical failure). The action is done as soon as all the resources (skills, tools and spares) are available to minimise the System downtime.
- Preventative:
  - On-condition: maintenance carried out to mitigate degradation and reduce the probability of failure after analysis of system conditions through defined indicators assessed on a periodic basis.
  - Scheduled (planned): maintenance carried out on a periodic basis (time-related or number-of-occurrences-related).

C.2.3.2 The hardware maintenance concept shall be based on the modularity of the equipment. The items to be removed from the system/equipment for replacement, to be repaired or to be replaced/refilled for preventative maintenance shall be defined MSIs (Maintenance Significant Items), with the following characteristics:

- Include those items in the Logistic Breakdown Structure (LBS) which are significant for maintenance at the Organisational Level.
- Include all the candidate items of the spare parts and consumables lists.
- Are subdivided into the following categories:

  1) LRU (Line Replaceable Unit)

     a) Its failure can be detected and indicated by a BIT (Built In Test System) system or by abnormal condition/failure display/alarm, in conjunction with TMs and general-purpose test equipment and troubleshooting procedures;

     b) It is easily accessed for replacement purposes;

c) It is easy to replace, through the use of a plug-in connector, screwed terminal, nut/bolt fixing or similar connector;

d) It has minimal adjustment/alignment requirements, such as voltage level settings, SW/FW installations/adaptations etc.;

e) Adjustments may be carried out with the BIT or with general-purpose HW/SW tools and test equipment;

f) When only one LRU has failed, its replacement returns the system/equipment to full operational status.

LRUs are subdivided into the following two categories:

- Statistical (LS): This category includes (but it's not limited to) the items subject to faults that occur with a statistical probability (most of them are electronic items) e.g. IF/RF strips/boards, SBCs, PPCs, Computers/Servers/Workstations and theirs components/peripherals, Networking equipment (Routers, switches), Power Supplies, electric/electronic components in general etc.
- Limited Life (LL): This category includes (but it's not limited to) the items whose faults are due to ageing (most of them are electromechanical items) e.g. TWTs, Rotary Joints, Slip Rings, Engines, T/R switches, Fans and Fan Assemblies, etc.

2) Insurance Item (II): This category includes (but it's not limited to) those items that have a very low failure rate and whose replacement may be necessary as a consequence of deterioration or fault by accident e.g. passive elements (attenuators, couplers, circulators, terminations), circuit breakers, patch panels, cables, metallic frames/cabinets/chassis etc.

3) Consumable Items: subdivided into the following three categories:

a) Technical Consumables (C[T]): This category of consumables includes (but it's not limited to) Fuses, Bulbs, Lamps, Gaskets, o-rings, EMI/Tempest seals, Surge Protectors, gas dischargers, Batteries and, in general, any other item replaced in case of preventive or corrective maintenance on the System etc.

b) Technical Consumables (C[NT]): This category of consumables includes (but it's not limited to) all POLs (Petrol, Oils, Lubricants), adhesive, sealing paste, gas and, in general, any other item replaced in case of preventative or corrective maintenance on the System etc.

c) Technical Consumables (C[G]): This category of consumables includes (but it's not limited to) ink cartridges, toners, printing paper, print ribbons, generic cleaning material and in general all the materials whose consumption cannot be predicted (e.g. is not associated to any preventative or corrective maintenance on the System) etc.

4) Attaching Parts (AP): items reported in the Corrective and Preventative Maintenance Procedures and in the Illustrated Parts Breakdown such as screws, gaskets, nuts, bolts, washers etc.

C.2.4 **Hardware Maintenance Levels**

C.2.4.1 The hardware maintenance levels used are generally known as HL1, HL2 HL3 and HL4.

C.2.4.2 Organizational Maintenance (HL1) is Hardware maintenance capable of being carried out:

- on-site;
- by relatively low technical skill level personnel performing preventive maintenance and changing Line Replaceable Units (LRU) and Insurance Items (IIs) on the basis of diagnostic outputs;
- using Built-In-Test (BIT) facilities for start-up and on-line diagnostics, by referring to main equipment Technical Manuals (TM);
- no Special Tools and Test Equipment (TTE) are envisioned to be used;
- typical tasks will include visual inspection, preventative maintenance tasks, manual reconfiguration if necessary, external adjustments, removal and replacement of LRUs/IIs;
- includes system failure recovery by the application of simple on-line diagnostics or technician initiated restart of the system and the use of off-line diagnostics which do not require external test module support;
- Generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

C.2.4.3 Organizational Maintenance (HL2) is Hardware maintenance capable of being carried out:

- on-site;
- by higher technical skill level personnel performing preventive maintenance and changing Line Replaceable Units (LRU) and Insurance Items (IIs) on the basis of diagnostic outputs;
- using Built-In-Test (BIT) facilities for start-up and on-line diagnostics, simple Tools and Test Equipment (TTE) (standard and special-to-type) in addition to BIT as a means for on-line and off-line diagnostics, and by referring to main equipment Technical Manuals (TM) to perform exhaustive fault isolation;
- simple either commercial or special-to-type TTE are envisioned to be used (e.g.: screwdrivers, multimeters, oscilloscope, adapters, peculiar support equipment);
- where the fault is beyond the capabilities of HL1 technical support, HL2 activities will be performed by Support Site personnel (through on-site intervention);
- where remote fault management is not feasible, technicians from the host site will travel to the remote site hand carrying relevant spares to perform maintenance tasks;

- Generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

C.2.4.4 Intermediate Maintenance (HL3) is Hardware maintenance capable of being carried out:

- at maintenance facilities and through technical support and assistance or on-site intervention/work by maintenance personnel with skills enabling tasks to be accomplished within the relevant technologies;
- by higher technical skill level personnel performing:
- repairing, testing and calibrating Line Replaceable Units (LRU), Shop Replaceable Units (SRU)and secondary spare parts (SSPs);
- on-site investigations and major scheduled servicing/overhaul, detailed inspection, major equipment repair, major equipment modification, complicated adjustments, system/equipment testing;
- failure trend analysis including reporting to relevant Purchaser authorities and Post Design Services (PDS);
- repair tasks will be performed using Automatic Test Equipment (ATE), general purpose and special-to-type TTE, calibration equipment, any applicable support software, and the necessary equipment TMs and a Technical Data Package (TDP);
- where the fault is beyond the capabilities of HL1/2 technical support, HL3 activities will be performed by Support Site personnel (through on-site intervention) or by the Contractor;
- Generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

C.2.4.5 Depot Maintenance (HL4) is Hardware maintenance capable of being carried out:

- at maintenance facilities (industry or military, OEMs) and through technical support and assistance or on-site intervention/work by maintenance personnel with skills enabling tasks to be accomplished within the relevant technologies;
- where the fault is beyond the capabilities of HL1-3 technical support, HL4 activities will be performed by the Contractor;
- Generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

C.2.5 Software Maintenance and Software Change

C.2.5.1 The software maintenance is a modification for the purposes of software fault removal, adaptation to a new environment, or improvement of performance.

C.2.5.2 The software maintenance for the purposes of software fault removal can be:

- Corrective/Unscheduled - it refers to tasks necessitated by actual errors in a software product. If the software product does not meet its requirements, corrective maintenance is performed. It is a Reactive modification of a software product performed after a new version is made available (patch/update) to correct the discovered problem(s). This activity is linked to Configuration Management, change management (contractor initiated ECP), new SW release(s) and Product baseline (PBL) change.

- Preventative/Scheduled – it refers to tasks necessitated for detecting potential errors in a software product or anticipate and avoid potential failures (daily checks, DBs clean up/integrity checks, cache cleaning, rebooting/restarting etc.). The task can lead, if latent failures are discovered, to a modification of a software product after delivery to detect and correct latent faults in the software product before they become effective faults (leading to a deferred corrective action).

C.2.5.3 The software maintenance for the purposes of adaptation to a new environment, or improvement of performance is a software change that enhances the software product. These changes are those that were not in the original design specifications or in the originally released software and are subject to purchaser initiated ECPs:

- Adaptive maintenance: software maintenance for the purposes of adaptation to a new environment (e.g.: a new environment could be a new type of hardware or a new operating system on which the software is to be run). Adaptive refers to a change necessary to accommodate a changing environment. Adaptive changes include changes to implement new system interface requirements, new system requirements, or new hardware requirements. This is a modification of a software product performed after delivery to keep a software product usable in a changed or changing environment.

- Perfective maintenance: software maintenance performed to improve the performance, maintainability, or other attributes of a computer program (e.g.: maintenance that adds new required functions is often referred to as enhancement). Perfective refers to a change that improves the software product's performance. A perfective change might entail providing new functionality improvements for users or reverse engineering to create maintenance documentation that did not exist previously or to change existing documentation. This is a modification of a software product after delivery to improve performance or maintainability.

C.2.6 Software Maintenance Levels

C.2.6.1 The software maintenance levels used are generally known as SL1, SL2 SL3 and SL4.

C.2.6.2 Organizational Maintenance (SL1) is Software maintenance capable of being carried out with the same characteristics highlighted for HL1. SL1 are those functions/tasks in support of the on-site software that are within the capabilities of site maintenance personnel. This includes software failure recovery by the application of simple diagnostics, or site maintenance personnel initiated restart.

C.2.6.3 Organizational Maintenance (SL2) is Software maintenance capable of being carried out with the same characteristics highlighted for HL2 e.g. SW settings, simple SW customizations (per site/instance), SW reloading/installation with automated or detailed procedures reported in the TMs, execution of scripts, management of users/profiles. SL2 are those functions/tasks in support of the on-site software that are within the capabilities of a System Administrator.

C.2.6.4 Intermediate Maintenance (SL3) is Software maintenance capable of being carried out with the same characteristics highlighted for HL3 e.g. SW/FW fine tuning (per site/instance), SW/FW bugs recording and reporting, SW/FW troubleshooting including Operating Systems. SL3 (on-site intervention) comprises those functions/tasks in support of the on-site software that require specialist intervention (SW System architects, SW programmers, experienced Systems' Administrators, Network specialists). The tasks can be performed either by software personnel visiting the site or by remote diagnostics if enabled by the System and allowed by Security.

C.2.6.5 Depot Maintenance (SL4) is Software maintenance capable of being carried out with the same characteristics highlighted for HL4 e.g. SW/FW debugging, re-coding and testing (both in simulated and emulated environments), SW/FW patches creation and deployment. The tasks can be performed by software engineers in properly configured environments (SW development and testing facilities) under strict Configuration Control.

C.3 SUPPORT CONCEPT

C.3.1 General

C.3.1.1 A Support Concept is a definition of the support objectives (scenarios) in relation with maintenance levels, maintenance support and their interrelationships.

C.3.1.2 This is peculiar for IT/SW-intensive and IT/SW-driven systems and shall be implemented in conjunction and coordination with the Maintenance Concept.

C.3.2 Support levels

C.3.2.1 There are (4) support levels in addition to the support level zero (LoS_0) that represents the operator.

C.3.2.2 LoS_1 – First level support (on-site, non-specialised)

- It consists of simple routine administration and activities. This level is user facing and is the first line of technical support. A single point of contact inside the NCI Agency central Service Desk is provided to customers for the implemented services. The Service Desk will log, categorise, prioritise, diagnose and resolve incidents within the boundaries of their training and permissions. The pertinent NCI Agency CIS Support Units (CSUs) carry out this level of support, in coordination with the NCI Agency Centralised Service Desk.

- The 1st Level Support Process implements the Incident Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;
- As part of the Incident Management, the Service Desk receives the issue from the user, puts it into a standard format (Trouble Ticket, TT), performs an initial assessment and distributes it to the predefined actors to solve it.

C.3.2.3 LoS_2 – Second level support (centralised)

- It provides escalated technical support to incident investigation and diagnosis. This level delivers advanced expertise to process services related to centralised system operations, fault isolation, system administration, management of maintenance services, system configuration, including reconfiguration of data sources and data connectivity to restore operations, assistance to first level and on-site support. This level performs end-to-end service monitoring and takes actions to resolve the incident and recover the services impacted.
- The 2nd Level Support Process implements the Problem Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;
- The Problem Management process receives the TT from the Service Desk and performs the following tasks:
  - (Re-)evaluation of TT category, criticality and priority,
  - Identification of the root cause of the issue (e.g. by issue replication testing),
  - Identification of workarounds,
  - Identification and initial planning of possible short, medium and long-term solutions (e.g. Workarounds, Patches, or new Baseline or CI Releases),
  - Create Problem Analysis Report and Change Request (CR) incl. schedule of implementation, and synchronisation with the Baseline Maintenance process;
  - Presentation of the Problem Analysis Report and CR to the Change Control Board (CCB) for approval,
  - Monitor and Control the approved CR during implementation,
  - Trigger 3rd Level Support and/or 3rd Level Maintenance process to implement the CR;

- Perform the post- CR implementation review;

C.3.2.4 LoS_3 – Third level support (centralised)

- It consists of central service management, central problem isolation and resolution, system-level maintenance, local repairs or spares provision, and management of deficiencies and warranty cases, beyond the capability of the second level support.
- The 3rd Level Support Process implements the Deployment and Release Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.
- The Deployment and Release Management process receives the approved Change Request from the 2nd Level Support and performs the following tasks:
  - Release of the solution (release unit/record)
  - Development of the solution (e.g. new CI Fix, Repair, Replacement, Patch, or Release),
  - Testing of the solution (e.g. Regression testing, issue/deficiency replication testing),
  - Update of Baseline content and status,
  - Delivery and deployment of the solution.

C.3.2.5 LoS_4 – Fourth level support (OEM/vendor)

- It consists of off-site factory/vendor problem resolution and maintenance, beyond the capability of third level support.

C.3.3 Support scenarios

C.3.3.1 The support concept is the apportionment of maintenance activities:

- NATO Maintenance Task (NMT) will be performed by NATO personnel (military or civilian),
- Industry Maintenance Task (IMT) will be performed by industry personnel under Warranty or Post Warranty Arrangement arrangement.

C.3.3.2 Theoretically there are four possible scenarios:

- NONO – NATO Owned / NATO Operated. If this approach is chosen the solution would be procured as a system and would be operated and maintained by NATO. The responsibilities for NATO maintenance levels are defined in the Maintenance Concept.
- COCO – Contractor Owned / Contractor Operated. If this approach is chosen NATO would have the solution delivered by a contractor as a Service.

- NOCO – NATO Owned / Contractor Operated. With this approach NATO would procure a system, but would “outsource” the Operation and Maintenance of it.
- CONO – Contractor Owned / NATO Operated. This approach exists and is usually called “Financial leasing”.

C.3.3.3 For NONO and CONO scenario the Contractor needs to agree with the Purchaser on maintenance levels commitments and develop a tailored logistic support concept based on a blend sharing of maintenance levels (following an e.g.:):

- Hardware Maintenance (Levels HL1, HL2) + Software Maintenance (Levels SL1) are NMT
- Hardware Maintenance (Level HL3) + Software Maintenance (Level SL2) are IMT with a learning curve versus NMT
- Hardware Maintenance (Levels HL4) + Software Maintenance (Levels SL3, 4) are IMT

C.3.3.4 For NOCO and COCO scenario the Contractor is responsible for the following maintenance levels when developing the logistic support concept: Hardware Maintenance (Levels HL1, HL2, HL3 and HL4) and Software Maintenance (Levels SL1, SL2, SL3 and SL4).

C.4 MAINTENANCE AND SUPPORT ALLOCATION

Hereafter an example of the table that summarize the maintenance and support allocation post warranty.

MAINTENANCE AND SUPPORT			**MAINTENANCE LEVELS**			
			HL1/SL1	**HL2/SL2**	**HL3/SL3**	**HL4/SL4**
LEVELS OF SUPPORT	**NMT**	**LoS_0**	Troubleshooting	▨	▨	▨
		LoS_1	HW/SW	Troubleshooting	▨	▨
		LoS_2	HW/SW (if any)	HW/SW	Troubleshooting	▨
		LoS_3	▨	HW/SW (if any)	HW/SW	Troubleshooting
	IMT	**LoS_4**	▨	HW/SW (exceptions in Support concept or under CLS)	HW/SW (exceptions in Support concept or under CLS)	HW/SW