Ministry of Defence

de&s

Maritime Command and Staff Trainer (MCAST)

SoW Appendix E: Data Item Description

Version: 1.2

Date: December 2023

Defence Equipment & Support

Document Prepared by

Name	Signature	Appointment	Date
[redacted]	[redacted]	[redacted]	May 23

Reviewed by

Name	Appointment	Date
[redacted]		May 23
[redacted]	[redacted]	18/05/2023
[redacted]	[redacted]	16/05/2023

Approved by

Name	Signature	Appointment	Date
[redacted]	[redacted]	[redacted]	16/05/2023
[redacted]	[redacted]	[redacted]	18/05/2023

Amendment Control

Version	Date	Authors	Purpose of Change
1.1	8 June 2023	[redacted]	Re-naming of DID-Op-001 to Architecture and Design of the Training System to match the description of the document and the title in the Contract Deliverables CD 3.4
1.2	13 Decembe 2023	[redacted]	**DID-PM-001** – Project Management Plan 7.6 - Requirement for Transition Reports. **DID-PM-002** – Risks, Issues and Opportunities (RIO) Management Plan 7.2 - To include DID-Sy-006 **DID-PM-007** – Exit Management Plan 7.4 - Requirement for Transition Phase reports. **DID-PM-008** – Target Operating Model (TOM) **DID-PM-005** – Benefits Realisation Management Plan **DID-SM-001** – Service Delivery Plan 7.1 - Specification of Service Delivery **DID-SM-002** – Business Continuity Plan 7.6 - Requirement for issues management reports. **DID-SM-009** Service Development Plan 7.7 - To include Mission Development **DID-EM-003** – Human Factors Integration Plan 7.6 - HFI Case Report requirement. **DID-SP-001** – Integrated Support Plan

			7.2 - R&M Case Report requirement 7.3 - Maintenance Log requirement 7.7 - Obsolescence Management Plan (OMP) requirement 7.8 - Software Support Plan requirement 7.9 - Modelling & Simulation Plan requirement 7.10 - Tech Doc Management Plan requirement Removal of: NCSISS - Technical Report

MCAST Commercial Team
Birch 1b, #3133,
MOD Abbey Wood,
Bristol,
BS34 8JH.

Security Notice

THIS DOCUMENT IS THE PROPERTY OF HIS BRITANNIC MAJESTY'S GOVERNMENT, and is issued for the information of such persons only as need to know its contents in the course of their official duties. Any person finding this document should hand it in to a British Forces Unit or to a Police Station for its safe return to the MINISTRY OF DEFENCE, (Dsy(Pol)), MAIN BUILDING, WHITEHALL, LONDON, SW1A 2HB, with the particulars of how and where found.

THE UNAUTHORISED RETENTION OR DESTRUCTION OF THE DOCUMENT IS AN OFFENCE UNDER THE OFFICIAL SECRETS ACT OF 1911-1989.

Contents

Introduction :

1.1 To ensure standardisation, Data Item Description's (DID's) are used for certain items contained in Appendix D. By adopting a consistent format representative of current policy and best-practice, DE&S will be able to assimilate and analyse the data faster and more efficiently. Standardisation will also bring benefits to the Contractor; seeking to reduce the number of reports whilst increasing coherency.

1.2 A DID defines the content, format and timescales for a specific deliverable. Failure to demonstrate compliance to the DIDs will result in the deliverable being rejected by the Authority until such time that the deliverable is redelivered in an acceptable format.

1.3 The deliverable set has been tailored for the provision of a Service vice procurement of equipment. This recognises both engineering and management functions that fall to the end user (owner) rest with the Service provider.

1.4 Therefore the Engineering and Logistic elements are subordinate to the Service Delivery Plan and are there to inform the Authority that the Service will be managed and delivered appropriately.

ITN Draft Deliverables:

2.1 It is understood that artefacts will develop through the course of the service and subsequently through agreement via the Contract Management Board. This will include a review process prior to issue and periodical updates as specified within the Contract Deliverables Document. (Appendix D to SoW).

2.2 As such Draft versions of Deliverables have been deemed acceptable at the ITN Tendering Stage.

2.3 Draft in this context will mean a deliverable provided of a sufficient maturity that will provide the Authority confidence that the tenderer will be able to fulfil the relevant requirement. A suggested maturity of 80% of the finalised artefact is provided as guidance.

Use/Relationship:

3.1 The Authority will use the ITN Contract Deliverables to:

3.1.1 Gain confidence that the full scope of work related to the Project Contractual requirements have been identified.

3.2.2 Gain confidence that the Contractor has appropriate procedures in place to manage the project effectively.

3.2 Review and assess the Contractor's proposal for:

3.2.1 Compliance with the requirements of the Contract

3.2.2 The ability to deliver effectively against each detailed Contract Deliverable and the provision of the MCAST Service.

Informative Applicable Standards, Governance & Reference Documentation:

1	MCAST Project Annex A Statement of Work
2	MCAST Project Appendix A Contract Deliverables Documentation.
3	Knowledge in Defence (www.kid.mod.uk)
4	Association for Project Management (APM) *APM Body of Knowledge 7th edition* 2019
5	PCF-COR-INS-0022. Develop and manage risk instruction.
6	PM Project Risk Analysis and Management (PRAM) guide.
7	APM Interfacing Risk and Earned Value guide.
8	PM Prioritising Project Risks guide.
9	DEF STAN 00-056, Part 1 Issue 7 - Safety Management Requirement for Defence Systems - Requirements and Guidance.
10	ISO31000:2018 - Risk Management Guidelines.
11	APM Body of Knowledge Section 2.2 stakeholder management
12	Association for Project Management (APM) *Earned Value Management: APM Guidelines (2008)*
13	The Earned Value Management Compass (APM,2010)
14	The Earned Value Management Handbook (APM,2013)
15	A Guide to Conducting Integrated Baseline Reviews (IBR) (2016]
16	Electronic Industries Alliance 748 (EIA-748) EVMS Standard
17	DE&S Guide: EVM – Contract Performance Report Completion Guidance
18	DCMA Fourteen Point Schedule Health Check.
19	International Organisation for Standardisation (ISO) 21508:2018 Earned Value Management in Project and Programme Management.
20	APM (Association of Project Management) Body of Knowledge Section 4.7 Configuration management.
21	APM (Association of Project Management) Body of Knowledge Section 3.5 Change control.
22	DEF STAN 05-057, Issue 7 – Configuration Management of Defence Material.
23	ACMP-2100 Ed. A Ver. 2 - Configuration Management Contractual Requirements.
24	Defence Contract Management Agency (DCMA) Fourteen Point Schedule Health Checks

Preparation Instructions:

5.1 The data item shall comply with the general format, content and preparation instructions contained in this DID.

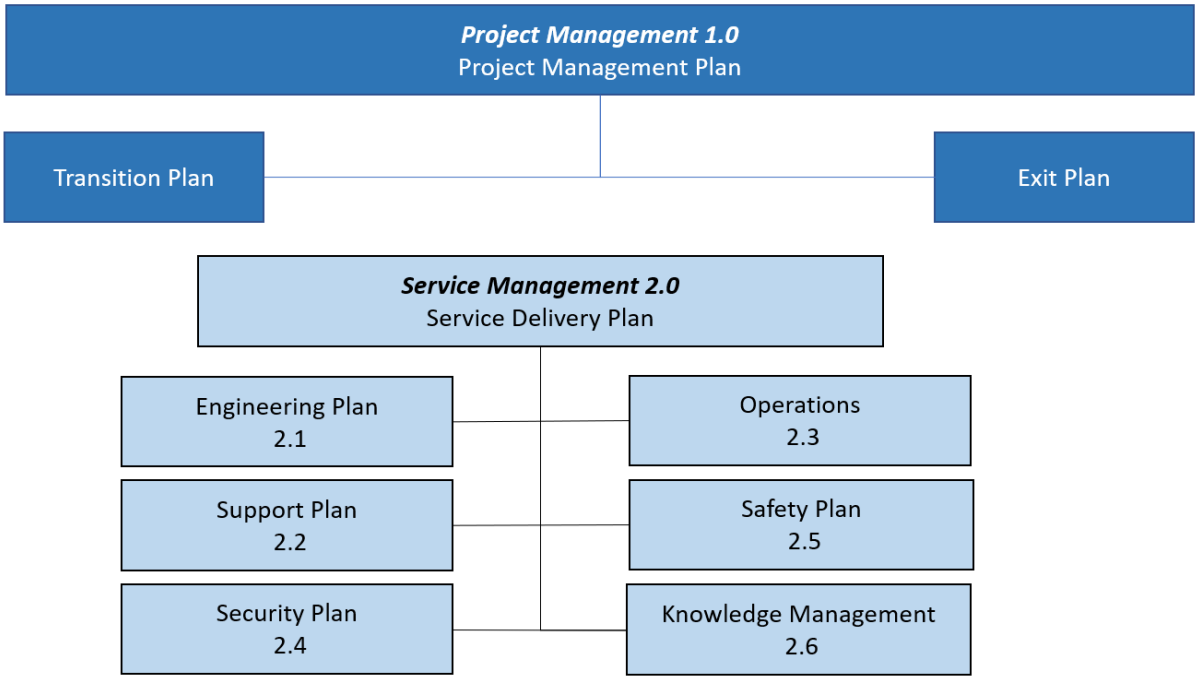
5.2 Referenced procedures and any related instructions shall be delivered as attachments to each Contract Deliverable.

5.3 The content requirements of each data item should be considered as the minimum standard that is required. It is not intended to constrain or otherwise restrict the inclusion of any content required to effectively develop the plan or implement the requirements of the Contract.

Data Format & Delivery Instructions:

6.1 Responses shall be prepared and submitted in Microsoft Office (word, excel etc.) format. Font Arial 11.

Data Item Description Structure:



1.0 Project Management

DID-PM-001 – Project Management Plan

1. **Title:** Project Management Plan (PMP)
2. **Number:** DID-PM-001
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:**

   6.1 The PMP is the controlling document that provides a coherent source of information that defines the project and how it will be managed. It provides the baseline against which the progress and conduct of the project are assessed.

7. **Requirements**: The Project Management Plan shall contain as a minimum but not be limited to:

   7.1 Background to the project

   7.2 Project objectives and / or requirements, scope and exclusions, constraints

   7.3 Stakeholders, including analysis of their influence and attitude towards the project

   7.4 Dependencies

   7.5 Risks, issues and assumptions, likely to refer to the related registers

   7.6 Description of project approach, including project management lifecycle and its relationship with other applicable lifecycles such as the acquisition lifecycle; to include a transition plan (start of Service) to show how BAU will be achieved and Transition Reports until IOC is achieved.

   7.7 Organisation Breakdown Structure (OBS) showing project organisation, including key role descriptions, terms of reference and authority levels. As well as showing all sub-contractors.

   7.8 Acceptance plan

   7.9 Work Breakdown Structure (WBS)

   7.10 Strategies / plans and toolsets for acceptance; assurance; risk management; issue resolution; assumption management; stakeholder engagement and communications; project monitoring and control, including change control; project reporting; information and data management.

   7.11 High level project plan / schedule, including key products, activities and resources including funding

   7.12 Service Board provision in accordance with agreed Terms of Reference. Formal minutes to be maintained, recording decisions and actions of each meeting.

   7.13 High level project plan / schedule, including key products, activities and resources including funding

DID-PM-002 – Risks, Issues and Opportunities (RIO) Management Plan

1. **Title:** Risks, Issues and Opportunities (RIO) Management Plan
2. **Number:** DID-PM-002
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:**

6.1 A RIO enables a formal risk process to be managed in conjunction with the Authority and defines roles, responsibilities, methodology (process), tools and techniques specific to the project and how threats and opportunities are to be managed through life as part of the overall project management strategy.

7. **Requirements:** The RIO shall contain as a minimum but not be limited to:

7.1 In the RIO, the Contractor must take due cognisance of the scope of the project (performance, cost and time) to establish a mutually agreed risk appetite (agreed tolerances) that enables the contractor to develop their scoring criteria for cost, time and performance.

7.2 The PM RIO should also encompass requirements contained within DID-Sy-006 - Security RIO.

7.3 The process shall:

7.3.1 Establish ownership for significant project risks;

7.3.2 Reduce overall project risk exposure;

7.3.3 Ensure all scope is considered to give a balanced view of risk;

7.3.4 Deliver information in support of the overall project decision making and governance processes.

7.3.5 Enable quantitative analysis to support forecasts of project cost and schedule out-turn.

7.4 Formal Reports -In support of the risk management process the following reports are required:

7.4.1 Risk and Opportunities Register (ROR) - Full risk register for contracted scope, defining risk (case, event, consequence), owner, proximity, current and target impact (probability and cost/schedule/performance impact) and associated management responses. The register shall cover both risks (threats) and opportunities.

7.4.2 Schedule Risks Analysis (SRA) - Identification of which risks were used in the analysis, which points of the Work Breakdown Structure / schedule they were applied to (Risk Network), Tornado Chart and sensitivity analysis. The schedule network used for SRA will be representative of the current progressed schedule, with the basis of the uncertainty applied explained.

7.4.3 Risk & Opportunities Change Report - Standard Report of risks that have been escalated to higher level for action / information.

7.4.4 Risk profile - Risk exposure profiled over duration of contract.

7.4.5 Risk / opportunity pre- & post mitigation response - Waterfall charts highlighting reduction in risk as a result of mitigation actions.

7.4.6 Risk & Opportunities Process Health metrics report - Information reported from the last thirty days and includes; total number of risks, risks added, closed, updated, review planned, review overdue, scoring updated - increased - decreased, risk escalated / deescalated, plan added - updated, responses added, response completed before due date, response completed after due date, response completed before trigger date, response completed after trigger date, responses updated.

DID-PM-003 – Stakeholder & Communication Management Plan

1. **Title:** Stakeholder & Communication Management Plan (SCMP)
2. **Number:** DID-PM-003
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:**

6.1 The SCMP will be the controlling document of how Stakeholders will be effectively managed through Design, Manufacture and In-Service and the communication methods to keep them appraised. It will provide the means of minimising the likelihood of stakeholders becoming a risk to project success.

7. Requirements:

7.1. The Authority will use the Stakeholder & Communication Management Plan to:

7.1.1 Gain confidence that all Stakeholders and the way they will be communicated with and managed has been identified.

7.2. Review and assess the Contractor's proposed Stakeholder & Communication Management Plan for:

7.2.1 Compliance with standard Stakeholder Management & Communications practice.

7.2.2 The plan's ability to support effective and ongoing Stakeholder Management.

7.3 The SCMP shall contain as a minimum but not be limited to:

7.3.1 Purpose.

7.3.2 Stakeholder identification.

7.3.3 Key stakeholders.

7.3.4 Communication principles.

7.3.5 Measures of success.

7.3.6 Management process.

7.3.7 Responsibilities.

7.3.8 Tools and techniques.

DID-PM-004 – Earned Value Management Plan

1. **Title:** EARNED VALUE MANAGEMENT PLAN (EVMP)
2. **Number**: DID-PM-004
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms**: N/A
6. **Description:**

   6.1 The EVMP documents the Contractor's plans, methodologies and processes for ensuring compliance with the EVMS requirements of the Contract. The EVMP shall include a description of the system structure and data flows, Project Controls System Description (PCSD), plans for implementation and subsequent review and maintenance of the Contractor's EVMS.

   6.2 The EVMP is subordinate to the Project Management Plan (PMP) where this document exists.

7. **Requirements:**

   7.1. EVMP Overview

   7.1.1. The EVMP shall describe the objectives, scope, constraints, risks and assumptions associated with the Contractor's EVMS activities related to this contract. Any risks identified with the Contractor's EVMS implementation and operation shall be documented in the EVMP and shall describe the risk management strategies associated with any EVMS implementation and operation related risks.

   7.1.2. Configuration Management to be defined within the context of EV within the EVMP.

   7.2. EVM Implementation

   7.2.1. The EVMP shall describe the processes and schedule to meet the contractual requirements and dates that the Contractor intends to use to implement the EVMS including:

   7.2.1.1. a description of the areas of non-compliance between the Contractor's current project management system and the EVMS contractual requirements

   7.2.1.2. the corrective actions planned to be undertaken to rectify the areas of non-compliance, including the timeframes involved.

   7.2.1.3. identification of any new or modified procedures, an overview of the scope of the new or modified procedures, and the responsibilities and timeframes for developing and approving these procedures;

   7.2.1.4. identification of areas of risk to the proposed EVMS implementation and proposed mitigation strategy;

   7.2.1.5. a summary of the implementation schedule, with the full implementation schedule being provided as part of the Contractor Master Schedule (CMS);

7.2.1.6. a description of the activity to ensure Subcontractor implementation of EV related contract requirements.

7.3. EVMS Description

7.3.1. The EVMP shall provide a description of the Contractor's EVMS that demonstrates compliance with the requirements of the contract covering all relevant EV Criteria as defined by the applicable standard. Where Contractor generated processes are referenced, copies are to be provided to the Authority. These will include, but not be limited to, processes for Work Authorisation, Scheduling, Risk Management, Change Management, Cost Control, and Accounting processes

7.4. Contractor EVMS Assurance

7.4.1. The EVMP shall describe the Contractor's EVMS quality assurance strategy to ensure that the EVMS remains compliant with the requirements of the Contract, including:

7.4.1.1. The criteria to determine that an EVMS Review is required; and,

7.4.1.2. the company roles/personnel involved in the reviews/activities.

7.4.2. Details of any continuous improvement process the company utilises. Results of Contractor Internal EVMS Assurance reviews and processes shall be shared with the Authority.

7.5. EVM Performance Reports

7.5.1. The EVMP shall describe the EVMS performance reporting processes and timescales used by the Contractor. The EVMP shall confirm adherence to the Contract Terms & Conditions by describing the reporting levels, structures and variance thresholds for the provision of CPRs including the standard reporting levels by CWBS elements.

7.5.2. The EVMP shall detail the variance thresholds that, when exceeded, require the provision of CPR Format 5 and at what level of the CWBS.

7.5.3. The EVMP shall describe any variations to the reporting levels and variance thresholds as the Contract progresses or the risk profile change.

7.5.4. The EVMP shall confirm the electronic formats to be used for the provision of EVMS data to the Authority in order to facilitate data transfer and analysis.

7.5.5. The EVMP shall describe the level and methodology to produce trend data.

7.6. Data Integrity Checks

7.6.1. The EVMP shall detail the methodology and frequency of data, schedule and EV health checks.

7.6.2. The EVMP shall define the process through which it will be possible to reconcile the financial data within the system back to the contract value (price).

7.7. EVM Related Reviews

7.7.1. The EVMP shall describe the facilities and support that will be provided to the Authority in support of IBRs. This should include but is not limited to:

7.7.1.1. The provision of supporting documentation to the Authority review team no later than forty-two days prior to a review;

7.7.1.2. All documentation shall be delivered electronically to the Authority;

7.7.1.3. Documentation delivered in support of a review shall be the final version that will be presented at the review unless otherwise agreed by the Authority;

7.7.1.4. Selected Control Account Managers (CAM) and Project Management & Control staff shall be available to support pre-planned interviews; and,

7.7.1.5. Access provisions are to be made for the review of documentation in electronic formats such as EVMS process and procedures, schedules, CPR CAM documentation and any related data requested to support the review.

7.8. EVM Flow Down to Major Subcontractors

7.8.1. Unless otherwise agreed by the Authority, the requirement for an EVMS (including EVMP, CWBS, CMS and CPRs and Subcontractor PMB shall be flowed down to the appropriate material level agreed with the Authority to represent a Managerially Significant breakdown of the work where the Subcontract or group of Subcontracts requires effort:

7.8.1.1. in excess of 12 months and the Subcontract price exceeds £20m;

7.8.1.2. represents more than 20% of the contract value; or

7.8.1.3. as directed by the Authority. Authority direction will be based on a risk assessment of the scope of work being undertaken in the subcontract.

7.8.2. The EVMP will detail a list of all significant Subcontracts (where the subcontractor portion of the overall contract cost is => 20% or £20M) incorporating the following information:

7.8.2.1. Subcontract title and description;

7.8.2.2. Subcontract type;

7.8.2.3. Subcontract value and Duration;

7.8.3. Subcontractor EVMS experience including standards that applied and any formal recognition of the applied EVMS.

7.8.4. The EVMS Description of Flow Down arrangements to each Subcontract shall include the following information:

7.8.4.1. Contractors Plans for assessing EV maturity to meet the Authority's EV Standards and Contract Requirements, including plans for Subcontractor Reviews and Surveillance. Note the Authority shall be given the opportunity to participate in these reviews in accordance with the Contract terms.

7.8.4.2. Plans for subcontract report data incorporation against WBS (CPR Format 1), Baseline Change (CPR Format 3), Variance Analysis (CPR Format 5), Schedule Reports (CPR Format 6).

7.8.4.3. Proposed timing of Subcontract data incorporation.

DID-PM-005 – Configuration Management Plan

1. **Title:** Configuration Management Plan (CMP)
2. **Number:** DID-PM-005
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:**

6.1 The CMP is the controlling document of how Configuration will be managed from requirements through Design, Manufacture, In-Service and Disposal, as well as being the control mechanism used to manage product, component and document evolution.

6.2 The CMP will demonstrate how the Integrity of Design (IoD) will be maintained. Requirements are under CM from the time they are established, and the CMP provides the baseline against which all configuration Items are measured against.

6.3 Any configuration change needs to be traceable back to a valid or new requirement.

7. **Requirements:**

7.1. The Contractor shall provide configuration management of the exercise systems and content throughout the service lifecycle. This shall include control of the design of the service, technical solutions, procedural elements, documents and registers and the exercise designs and specifications. Configuration management of data, software, exercise content and records shall be maintained and managed throughout the service lifecycle.

7.2. The Configuration Management Plan (CMP) shall be completed and delivered by the Contractor within 3 months of contract commencement and a formal configuration management process put in place. The configuration of MCAST systems shall be placed under a Configuration Baseline and thereafter configuration changes shall be tracked at the level of Configuration Items (CI). The following shall be developed and maintained for the MCAST systems but not limited to:

7.2.1 Configuration Item Register (CIR);

7.2.2 Change Request Register (CRR);

7.2.3 Local Change Register (LCR); and

7.2.4 Incident Report Register (IRR).

7.3. Configuration Status Accounting (CSA) procedures shall be put in place by the Contractor and a Configuration Status Record (CSR) maintained. The configuration management documents shall be accessible to the Authority to support audits and security accreditation of the MCAST system.

7.4. System interfaces (internal and external), gateways and integrations shall be documented in formal Interface Control Definition (ICD) documents and placed under configuration control to enable federation and system-of-systems testing and accreditation.

7.5. Configuration baseline standards shall be maintained for the software and hardware required to support routine MCAST training events and controlled configuration adjustments to support non-routine MCAST training events. Secure document registers of all classified configuration management records shall be maintained. Secure gateways shall be configured and managed to provide protection from infection by unauthorised undesirable programmes in accordance with Defence Security Policies and Procedures.

DID-PM-006 – Contractor Master Schedule

1. **Title:** Contractor Master Schedule (CMS)
2. **Number:** DID-PM-006 (EVM DID-EV-003)
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:** The CMS describes the contracted activities, milestones and decision points to enable the objectives and deliverables of the contract to be satisfied. The CMS will define the project schedule status through a comparison of the current schedule status and appropriate accepted baseline schedule.
7. **Requirements:**

7.1. The CMS relates to the following documents required within the contract:

7.1.1 Earned Value Management Plan (EVMP);

7.1.2 Project Management Plan (PMP); and,

7.1.3 Contract Work Breakdown Structure (CWBS).

7.2 The CMS shall be traceable and integrated with:

7.2.1 The CWBS (DID-EV-002) – all activities and milestones on the schedule will be coded to the lowest level of the CWBS that represent the scope to which the activity pertains;

7.2.2 Contract Milestones – shall be clearly identifiable within the logic linked activity network;

7.2.3 The Contractor's EVMS – the integration of scope, schedule and budget will be undertaken around the CWBS, which will form the primary structure for EV Performance reporting; and,

7.3 Each submission of the CMS shall be consistent with the associated Contract Performance Report (CPR) delivered within this Contract.

7.4 The CMS shall be capable of comparing planned and current forecast data and being displayed in a variety of formats to include;

7.5 A Gantt chart

7.6 A listing of all tasks, together with planned (baseline and current progress including forecast) and actual start and finish dates

7.7 A listing of project milestones (to include all contract milestones) together with original, rescheduled, forecast and actual completion dates

7.8 All activity durations within the schedule shall be in days unless otherwise agreed by the Authority.

7.9 All resource units within the schedule shall be in hours and costs shall be in Great British Pounds Sterling unless otherwise agreed by the Authority.

7.10 The CMS shall be capable of being displayed at the following levels:

7.10.1 Summary Level – The Summary level of the CMS shall provide a graphical display of Contract activities, key events, and milestones at a managerial significant level of the WBS.

7.10.2 Intermediate Level – The Intermediate Level of the CMS shall provide a graphical display of Contract activities, key events, and milestones at the control account level of the WBS. A CMS generated at the Intermediate Level shall be able to be rolled up to, and shall provide visibility of, the Summary Level.

7.10.3 Detailed Level – The Detailed Level of the CMS shall provide a graphical display of Contract activities, key events, and milestones at the work-package level of the WBS. A CMS generated at the Detailed Level shall be able to be rolled up to, and shall provide visibility of and access to, both the Intermediate Level and the Summary Level.

7.11 The CMS shall identify the following aspects:

7.11.1 Activities and associated durations

7.11.2 Milestones, including Contract Milestones, Payment Milestones and significant project events

7.11.3 The relationships and dependencies of activities and associated milestones that are to be completed within the scope of this contract.

7.11.4 Earliest and latest start and finish dates for all activities and associated milestones

7.11.5 Total float and free float of the overall schedule

7.11.6 Critical Path, list of activities on the critical path and those that are near the critical path from start through to completion of the contract.

7.11.7. Resource Profiles, depicting manpower, materials and equipment.

7.11.8. The baseline budget for all activities aggregating to the total Performance Measurement Baseline (PMB), allowing a roll-up to work package and control account levels.

7.11.9. Subcontracting schedules to include all major sub-contract activities and outputs at the appropriate level of detail, reflecting complexity and risk.

7.11.10. Required Government Furnished Items (GFX) to include Government Furnished Equipment (GFE), Government Furnished Assets (GFA), Government Furnished Information (GFI), Government Furnished Structures (GFS) if applicable, together with ‘required by’ dates and ‘end of loan dates’.

7.11.11. All non-working time such as holidays and known disruptions

7.12 A Basis of Schedule (BOS) shall be produced and maintained under configuration control. The BOS should include the following;

7.12.1 How the CMS has been produced;

7.12.2 Detail methodologies used to establish estimated durations;

7.12.3 Key assumptions and exclusions;

7.12.4 Details of the standard working time and calendar that has been included;

7.12.5 Risks, including risk analysis techniques used, and any mitigations embedded in the schedule;

7.12.6. The standards used to establish duration lengths and use of constraints, ensuring no open-ended activities and compliance with DE&S Schedule guidance;

7.12.7. The basis of estimate and associated assumptions for the cost and duration of baseline activities, covering both labour and materials. This may take the form of a master data and assumptions list; and,

7.12.8. The Configuration and assurance procedures that will be used to manage and ensure the ongoing integrity of the CMS.

8. **CMS Reports** - The following reports, which collectively comprise CPR Format 6, are required:

8.1 Baseline Reports (Performance Measurement Baseline)

8.1.1. Reports that describe and reflect the initial baseline

8.1.2. Subsequently approved changes that caused a revision of the baseline.

8.1.3. A Schedule narrative shall be provided with the original baseline and any subsequent baseline revisions outlining how the schedule has been constructed, the key assumptions together with the basis of estimate and logic of milestone selection and a description of the critical and near critical paths.

8.1.4. A set of Authority agreed schedule health metrics.

8.1.5. Schedule Risk Analysis shall be conducted on the Contractor schedule, at least quarterly and on the Authority's request, a Schedule Risk Analysis Report and electronic copies of the SRA schedule and the Contractor SRA models shall be provided to the Authority.

8.2 Progress Reports (Statused Current Working Schedule)

8.2.1. Electronic copy of the progressed schedule each reporting period that has formed the basis of the CPR for that period.

8.2.2. A Schedule narrative shall be provided with the progressed schedule outlining, the key assumptions underlying the progress and forecast together with the basis of estimate for key forecast activities where this is significantly different to the baseline, the impact and rationale of any significant logic changes and the resulting change to the schedule risk implications, and the resulting impact on key (including Contract) milestone and deliverables, if any. The analysis shall include a narrative description of the current Critical and near Path Analyses.

8.2.3. Milestone Report. Agreed milestones to be shown with the baseline and current forecast dates. Report to provide RAG status and indication of float. Note that there shall be clear definitions and acceptance criteria for reporting milestones.

8.2.4. Critical Path, Sub-Critical Path and Float Erosion Analysis Reports. Critical path analysis against the baseline and current forecast dates within the CMS. Summary/ variance commentary of movements/changes to the critical path to be reported.

8.2.5. Interdependencies (Give/Get Milestones) Table. To indicate key interdependencies between supply chain, MoD and contractor schedules. Report should indicate movements in the period relating to both the baseline schedules and the current forecast version of these schedules. Variance commentary to be provided.

8.2.6. A set of agreed schedule health metrics for the submitted progressed schedule.

8.2.7. Schedule Risk Analysis shall be conducted on the Contractor schedule with a Schedule Analysis Report and copies of the SRA schedule being provided to the Authority. SRA will be provided together with associated confidence figures for the deterministic baseline considering both uncertainty and risk (against a submitted risk register) and uncertainty.

DID-PM-007 – Exit Management Plan

1. **Title:** Exit Management Plan
2. **Number**: DID-PM-007
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:** An Exit Management Plan shall be prepared and maintained to detail the activities and processes that will be followed to achieve transition.

7. **Requirements:**

   7.1. The Contractor shall manage the Transition Phase and any extensions to achieve the objective of transitioning the service to new provider arrangements without interrupting the flow of Exercises delivered.

   7.2. More frequent management meetings may be required, and an Exit Management Plan shall be prepared and maintained to detail the activities and processes that will be followed to achieve transition.

   7.3. The Exit Management Plan should be produced in light of the Authorities Exit Management Plan Annex C – Exit Management Plan which in turn is to be read in conjunction with Clause 43 (Exit Plan) of this contract.

   7.4. Formal Reports - In support of the Transition Phase, the following reports are required:

      7.4.1. Enumeration List

      7.4.2. Federation Object Model (FOM Data)

      7.4.3. Model Data Pack

      7.4.4. Interface Information Pack

      7.4.5. Exit Report

DID-PM-008 – Target Operating Model (TOM)

1. **Title:** Target Operating Model
2. **Number**: DID-PM-008
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:** The Contractor shall develop a Target Operating Model (TOM) at the beginning of the Service describing the objectives for the Service to achieve by Full Operating Capability (FOC).
7. **Requirements:**

7.5. TOM developed at the beginning of the Service as the objective for the Service to achieve by Full Operating Capability (FOC). To be presented for approval by the Authority within 3 months of contract commencement.

7.1. The Contractor shall provide documented planning routines for the scheduling, organisation, design, delivery and support of Exercises. These planning routines shall be represented in the MCAST Service Delivery Manual (known as an MCAST Handbook) which is to be presented for Approval by the Authority within 6 months of contract commencement and made available in interactive electronic format for stakeholders to use and apply.

7.2. The Contractor shall plan conferences and meetings with the Authority representatives and stakeholders, and the tasks to deliver the Training Plan during the exercise lifecycle, including endorsement of the Exercise Plan (EXPLAN) by the Authority and closing-down each exercise.

7.3. Two elements of planning are required for each Exercise; an initial planning period 12 to 8 months before an exercise, during which key decisions about the exercise are taken by the TDA and venues and resources are booked. This is required to meet the timelines of the personnel management process and for site bookings. A later period of planning, closer to the exercise start, will complete the planning and OSW needed to run the Exercise.

7.4. MCAST Service Delivery Manual (MCAST Handbook) to include planning routines. To be presented for Approval by the Authority within 6 months of contract commencement and updated at least annually.

DID-PM-009 – Benefits Realisation Management Plan

1. **Title:** Benefits Realisation Management Plan
2. **Number**: DID-PM-009
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to MCAST Project Annex A Statement of Work (SoW) Appendix D Contract Deliverables Documentation.
5. **Applicable Forms: N/A**
6. **Description:** A Benefits Realisation Management Plan enables the formal monitoring of benefits throughout the service contract.
7. **Requirements:**

7.1 The Contractor shall monitor benefits realisation throughout the Service contract. Benefits measuring includes, but is not limited to:

- 7.1.1 No. of Exercise days delivered
- 7.1.2 No. of Training Audience Days delivered
- 7.1.3 Ratio of White Force Days to Training Audience Days delivered
- 7.1.4 No. of workdays required for design and development of each Exercise Day delivered
- 7.1.5 Achievement of CTOs (improvement scores based on pre- and post-exercise surveys of Training Audience
- 7.1.6 Measure of Training Effectiveness
- 7.1.7 Real life operational training saved (no. of platforms, personnel, fuel consumed, flying hours reduced, steaming hours reduced (ships and submarines), reduced ammunition consumption, safety hazards mitigated, CO2 consumption reduced.

7.2 Exact methods of calculation, collection and reporting of the benefits realisation shall be defined in a Benefits Realisation Management Plan that is maintained.

7.3 The Benefits will form some of the Service KPIs.

7.4 Formal Report - In Support of the Benefits Realisation Plan the following reports are required:

7.4.1 Benefits Realisation Reports to be provided quarterly.

2.0 Service Management

DID-SM-001 – Service Delivery Plan

1. **Title:** Service Delivery Plan
2. **Number:** DID-SM-001
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:**
   - 6.1. The Service Delivery Plan sets out how the Contractor will manage the Service operation and Technical/Engineering Support of the MCAST system in order to provide the training output to the end user as described in the SOW. It will build on the Transition Plan (start-up) cover creating business as usual for the delivery of the training output against the Statement of Training Task, address continuous improvement (Development Plan) and establish the conditions for a smooth transition into the Exit Plan.
   - 6.2. The MOD will only own and operate the GFA but as part of the Contract Management will need to understand the engineering and logistics planning of the Contractor and the management of its contracted/employed staff associated with the Service Delivery.
7. **Requirements:** The Service Delivery Plan shall contain as a minimum but not be limited to:
   - 7.1. **Service Delivery**. The plan shall outline Service Start Up, achieving Business s Usual (Post IOC / FOC), Continuous Improvement and outline Exit Plan.
   - 7.2. **Engineering Management**. The plan shall outline how the MCAST Technical Support will develop and sustain the hardware and software systems that comprise the MCAST Technical solution. The Engineering Management Plan (EMP) should be developed in order to define the functional aspects of the technical solution engineering and associated records and registers to enable effective through-life management of the capability. It must address continuous improvement and obsolescence of systems, application or supporting services.
   - 7.3. **Support Management**. The plan shall outline how the delivered capability will be supported through-life and based on supportability analysis. It shall address hardware and software reliability and maintainability, disposals, the generation of documentation sets to support the engineering and training processes through-life and into the Exit Management Plan. The plan must also indicate how the SQEP workforce resources will be sustained for the duration of the Contract.
   - 7.4. **Operations**. The Service Delivery Plan should explain how the MCAST Operating Service will develop, manage, and deliver the training capability. It should also cover Business Continuity, Continuous Improvement (through a development plan) and the development (in conjunction with the end user (JTEPS)) of an operations manual that details how the full exercise cycle will be jointly managed through a provider-user relationship.
   - 7.5. **Security**. MCAST will operate up to SECRET UK Eyes Only. Security management is essential to Capability success. Security plans must cover interfaces, notable to OPNET, to ensure such links do not compromise the integrity and security case of systems federated through MCAST. They must also cover all processes to gain accreditation, Cyber-attack

resilience, the protection, storage, and disposal of classified data and material, and the security clearances of Contractor permanent and temporary staff.

7.6. **Safety**. Safety shall address how the Contractor will operate its own systems (this may be by reference to appropriate corporate plans adapted to the service provided), tailored safety training for military personnel supporting exercises/training as White Force augmentees operating MCAST core systems and peripherals, and the management of safety within GFA accommodation and exercise venues.

7.7. **Knowledge Management.** MCAST will generate a valuable and reusable Capability knowledge, and data analytics, in terms of the Project Management, Engineering, Support and Operations along with all the associated artefacts. This knowledge will support operations, sustainment and set the conditions for business continuity and continuous improvement and set the conditions for the Exit Plan.

For ITN the requirements detailed above should be supported at a minimum by the Plans, Registers and Case Reports detailed within this DiD, and highlight where additional artefacts will be developed during Transition (start-up).

DID-SM-002 – Business Continuity Plan

1. **Title:** Business Continuity Plan
2. **Number:** DID-SM-002
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** See KiD.
6. **Description:**

   6.1 Business Continuity Management utilises multiple Business Continuity Plans (BCPs) to ensure the recovery of an overall team, capability or service following a business continuity incident. It is the effectiveness of each individual BCP that ensures successful recovery of operations.

   6.2 The BCP shall Identify each function, capability, service and asset that is critical for the operation of the overall capability, service or team's equipment covered by this BCP.

   6.3 An assessment of risks should be undertaken and ways to manage or mitigate the risks should be identified in a risk register.

7. **Requirements**: The Business Continuity Plan shall contain as a minimum but not be limited to:

   7.1. Power Supplies. Disruption to core systems and or exercise venues.

   7.2. Data Storage. Secure storage and/or and access to electronic exercise data and artefacts.

   7.3. Network Resilience. Effects of Cyber-attack on exercise network or bearer systems.

   7.4. System Integrity. Effects of deliberate attack or software malfunction preventing exercise development or delivery**.**

   7.5. Workforce. Coverage of critical roles and ability to cover absences.

   7.6. Provision of Management Reports in response to issues identified during delivery. The purpose, contents, format and timing of each report shall be agreed with the Authority Service Manager and are to be submitted to the Project Progress Meeting for endorsement following investigation of an issue.

DID-SM-003 – Data Management Plan

1. **Title:** Data Management Plan
2. **Number:** DID-SM-003
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A.
6. **Description:**

   6.1 Data Management is a golden thread throughout Knowledge Management. It covers the records, registers, processes, simulation data and exercise artefacts. The data may be physical, and electronic that defines the capability, its operation and the information required for Business Continuity to extend or replace the Capability.

   6.2 The Data Management Plan must be aligned to the Security Plan to ensure all classified material is correctly stored and managed.

   6.3 The Plan shall also cover proposals for how the data will be analysed and presented in order to monitor and improve the Service.

7. **Requirements**: The Data Management Plan shall contain as a minimum but not be limited to:

   7.1 System Design. To cover system architecture, software, simulation and exercise artefacts interfaces, and the associated configuration control.

   7.2 Support Solution. To cover management through life including access via software licences, back-ups and warranties of data storage arrangements.

   7.3 Operations. To cover workforce breakdown, operating procedures and processes, Exercise design, development, data analysis during and after exercises, records, and Learning from Experience

   7.4 Security. To cover the security management system, accreditations and associated artefacts, records, and registers.

   7.5 Safety. To cover the safety management system, accreditations and associated artefacts, records, and registers.

   7.6 Management. To cover how data and artefacts are generated to drive monitoring of KPIs and management reports.

DID-SM-004 – Intellectual Property Register

1. **Title**: Intellectual Property Register
2. **Number**: DID-SM-004
3. **Version**: 1.0
4. **Delivery Schedule**: Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms**: N/A
6. **Description**:
   - 6.1. The Intellectual Property Register will detail all IPR used within the MCAST capability.
   - 6.2 The register shall support compliance with JSP 939, business continuity and transition out at end of contract.
7. **Requirements**: The Intellectual Property Register shall contain as a minimum but not be limited to:
   - 7.1 Hardware.
   - 7.2 Software and applications/tools developed for the Capability.
   - 7.3 Artefacts generated for the synthetic environment, exercise and training events.
   - 7.4 Operating manuals (Service and Training Operations).

DID-SM-005 – Disposal Log

1. **Title**: Disposal Log
2. **Number**: DID-SM-005
3. **Version**: 1.0
4. **Delivery Schedule**: Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms:** MOD Form 102 may be used to register and manage classified documentation.
6. **Description**:

   6.1 The Disposal Log provides a record of equipment, software and physical classified artifacts. It provided a record supporting asset management, and security management for hardware and classified material subject

7. **Requirements**:

   7.1 Simulation Hardware should have a unique item number that will be used as a reference within the disposal log. Hardware that has stored or processed classified data must be disposed of in accordance with MOD security regulations.

   7.2 Classified material generated through the Service Management and Exercises, or Events shall be disposed of in accordance with MOD security regulations.

DID-SM-006 – Warranties Register

1. **Title:** Warranties Register
2. **Number:** DID-SM-006
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms:** N/A
6. **Description:**
   6.1. The Warranties Register shall document the warranties provided by the Contractor for MCAST Capability.
7. **Requirements**: The Warranties Register shall include, but not limited to:
   7.1 Service Delivery and Equipment and Consumables that are delivered as part of the service.
   7.2 Warranties transferred to the Authority during the Transition Phases (Start-up and Exit).

DID-SM-007 – Software Licence Register

1. **Title:** Software Licence Register
2. **Number:** DID-SM-007
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms:** N/A
6. **Description:** The Register shall document all obtained to deliver the MCAST capability. All licences should be purchased as MOD-user to enable transition at the end of contract. The use of MOD Enterprise licences should also be included.
7. **Requirements**: The Register shall include, but not limited to licences for:
   - 7.1 COTS software used to develop and deliver the Capability.
   - 7.2 Software and applications developed as part of the Service Delivery.
   - 7.3 Applicable MOD Enterprise licences.

DID-SM-008 – Compliance Plan

1. **Title**: Compliance Plan
2. **Number**: DID-SM-008
3. **Version**: 1.0
4. **Delivery Schedule**: Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms**: N/A
6. **Description**:
   - 6.1 The Contractor shall formally seek, apply for, and certify compliance with applicable standards used to support architecture, system design, system management, service delivery and service management.
   - 6.2 Periodic Compliance Reports are required to first establish and subsequently track changes in applicable legislation, regulations, and standards during the life of the service and plan for updates and realignment with newly available legislation, regulations, and standards.
7. **Requirements**: Compliance will include, but not be limited to compliance method, conformity with and confliction resolution with:
   - 7.1 National and local regulations.
   - 7.2 Legal requirements (e.g. H&SAW Act).
   - 7.3 Standards.
   - 7.4 Intellectual Property requirements (e.g. patents and software licencing).

DID-SM-009 Service Development Plan

1. **Title:** Service Development Plan
2. **Number:** DID-EM-xx
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms:** N/A
6. **Description:**
   - 6.1 The Service Development Plan Register supplements the Transition (Start-up) Plan and covers capability development through to FOC, and continuous improvement processes to the Technical Solution and Operating Processes throughout the contract.
   - 6.2 The Plan shall be reviewed annually.
7. **Requirements**: The Plan shall include, but not limited to opportunities and necessities for changes in:
   - 7.1 Hardware configuration.
   - 7.2 Software architecture including interfaces.
   - 7.3 Applications developed as part of the Service Delivery.
   - 7.4 Simulation regional settings, artefacts, and vignettes.
   - 7.5 Operating processes and procedures.
   - 7.6 MCAST Operating and Technical Services workforce and efficiencies.
   - 7.7 Mission Development

2.1 Engineering Plan

DID-EM-001 – Engineering Management Plan

1. **Title:** Engineering Management Plan (EMP)
2. **Number:** DID-EM-001
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms:** N/A
6. **Description:**
   - 6.1 The EMP shall set out the Contractor's approach to top-level management, governance and assurance of the project's Engineering activities. While the Project Management Plan (PMP) addresses general project management tasks, the Engineering Management Plan (EMP) outlines the technical plans and systems engineering activities that will be used to develop, integrate, test, validate, and operate the capability.
   - 6.2 The EMP shall be developed by the Contractor at the beginning of the contract as part of the Service Delivery Plan. It shall be updated to reflect changes in management arrangements and reviewed at least every six months.
7. **Requirements:** The EMP should be written to support the delivery of a Service, not procurement of equipment. The EMP shall be based upon recognised Systems Engineering standards and processes and shall describe the lifecycle and approach being applied to the project. It shall contain as a minimum but not be limited to:
   - 7.1 The schedule of all technical activities which must be undertaken to deliver the contract.
   - 7.2 Relationship to other strategies and plans.
   - 7.3 Project lifecycle approach and stages.
   - 7.4 Project Engineering approach.
   - 7.5 Project Engineering governance and control.
   - 7.6 Project Engineering reviews and reporting.
   - 7.7 Technical risks, opportunities, challenges and corresponding management approach.
   - 7.8 Engineering resourcing and management of capability / Suitably Qualified and Experienced Persons (SQEP).

DID-EM-002 – Interface Management Plan

1. **Title:** Interface Management Plan
2. **Number:** DID-EM-002
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms:** N/A
6. **Description:**
   - 6.1. The Plan shall detail the configuration control and administration of interfaces between MCAST core subsystems and the MCAST system to OPNET/OPCIS and JMNIAN as defined in the Networks Interface Control Definition (ICD) prepared during the system design phase.
   - 6.2. The plan shall cover local Exercise computer network and technical infrastructure serving the Training Audience, White Force, video conferencing, voice communications, and Exercise management team. It shall also identify site-to-site network requirements that will normally be provided over existing Authority networks.
7. **Requirements**: The Plan shall include, but not limited to:
   - 7.1 Intra-MCAST Interfaces. The design of interfacing of MCAST applications and programs.
   - 7.2 MCAST-OPNET Interface.
   - 7.3 MCAST-JMNIAN Interface. To be included if JMNIAN is used as part of the Capability Wide Area Network.
   - 7.4 Security Accreditation and Management of interfaces.

DID-EM-003 – Human Factors Integration Plan

1. **Title:** Human Factors Integration Plan (HFIP)
2. **Number:** DID-EM-003
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to MCAST Project Annex A Statement of Work (SoW) Appendix D Contract Deliverables Documentation.
5. **Applicable Forms:** N/A
6. **Description:** The HFIP shall clearly set out how the HFI process will be managed and what technical and management activities will be completed in each phase of the programme for the MACST Operating System with the exception of user OPNET terminals.
7. **Requirements:** The Plan shall include as a minimum, but not limited to:
   - 7.1 A description of how HFI management will be conducted through the project life cycle
   - 7.2 An organisation chart identifying the individuals who will be responsible for HFI and their roles and responsibilities.
   - 7.3 Details of Human Factors analytical methods, tools and techniques that the Contractor intends to use.
   - 7.4 A description of how People-Related considerations in the HFI Risks, Issues and Opportunities (RIO) Register will be managed.
   - 7.5 A description of the inter-relationships with other project documents including Integrated Logistics Support (ILS) Plan, Integrated Test, Evaluation and Acceptance (ITEA) Plan, Training Needs Analysis TNA), Project RIO, Project Safety Case.
   - 7.6 Formal Reports - An HFI Case report is required to report at the first Project Progress Meeting. Subsequently Service Delivery reporting through Project Progress Meetings.

2.2 Support Plan

DID-SP-001 – Integrated Support Plan

1. **Title:** Integrated Support Plan (ISP)
2. **Number:** DID-SP-001
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms:** N/A
6. **Description:**

   6.1 The ISP documents the Contractor's management plans for data gathering and analysis; task management, control and execution; and interface of the Integrated Logistic Support (ILS) task(s). The Contractor's management plans will demonstrate that integration of the new system will satisfy all supportability criteria.

   6.2 The Plan shall be based on supportability analysis and reviewed annually.

7. **Requirements**: The Plan shall include, but not limited to:

   7.1 The Support System Concept. This section shall contain a summary of the system characteristics relevant to ILS, the support process and explanation of how the system will be supported in its intended operational role.

   7.2 A Reliability and Maintainability Plan and ongoing Case Report requirement during the contract period to include the identification of the resources (e.g. people, equipment and facilities) required to undertake R&M activities, and the R&M activities.

   7.3 Maintenance Plan to cover how the system will be supported to ensure availability and the obsolescence management of hardware and software with any corresponding activities to be recorded in a Maintenance Log and reported on quarterly.

   7.4 Supply Support Plan detailing the provision of hardware and software when required.

   7.5 Disposal Plan define the policies, procedures, and responsibilities for disposal through-life, to ensure that the MCAST System can be disposed of at any stage of the through-life cycle, in accordance with extant policies and regulations.

   7.6 Packaging, Handling, Storage and Transportation (PHS&T) Plan. The Contractor shall manage the transport and transportability, including Packaging, Handling, Storage and Transportation (PHS&T) arrangements for all components of the system that need to move to Exercise venues. A PHS&T plan shall be delivered 6 months after contract commencement and maintained throughout the service life.

   7.7 Obsolescence Management Plan (OMP). The Contractor shall manage obsolescence of hardware and software to ensure the service is maintained and available (KPI) throughout the contract.

   7.8 Software Support Plan. The plan should at a minimum detail how the Contractor will maintain COTS software, licence management and introduction and testing of software upgrades. It should also detail processes for fault rectification management and software change requests.

   7.9 Modelling and Simulation (M&S) Plan. The M&S plan shall detail the development of the M&S architecture and how entities, settings and scenarios are created, maintained, modified and validated.

   7.10 Technical Documentation Management Plan. The Contractor shall maintain technical documentation to enable through life management of the system, support the system security and safety cases and

configuration control, and when necessary inform Federate system management (interface control) and the Exit Plan.

2.3 Operations

DID-Op-001 – Architecture and Design of the Training System

1. **Title**: Architecture and Design of the Training System
2. **Number**: DID-Op-001
3. **Version**: 1.0
4. **Delivery Schedule**: Refer to Appendix D to SoW – Contract Deliverables.
5. **Applicable Forms**: N/A
6. **Description**: The architecture and design of the MACST system shall provide the detail of the local Exercise computer network and technical infrastructure serving the Training Audience, White Force, video conferencing, voice communications, and Exercise management team.
7. **Requirements**: The Architecture and Specification shall at a minimum detail:
   - 7.1 The system hardware, software and peripherals that comprise the MCAST Capability.
   - 7.2 System Requirements Review when conducted.
   - 7.3 Preliminary Design Review when conducted.
   - 7.4 Critical Design Review and when conducted.
   - 7.5 Design and systems changes when introduced.

2.4 Security Plan

DID-Sy-001 - Security Management Plan

1. **Title:** Security Management Plan (SyMP)
2. **Number:** DID-Sy-001
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** There is no defined template for a SyMP
6. **Description:**
   - 6.1. This Data Item Description (DID) contains the requirements, content and format for the MCAST SyMP.
   - 6.2. The purpose of the SyMP is to identify all security elements that need to be considered, developed and implemented, including identification of when these are scheduled to occur.
   - 6.3. The SyMP can be as simple or as intricate as necessary to fully encompass the aspects of security (in this case for a High Business Impact Level System) and how it is to be managed and controlled throughout the service and will correspond with the perceived security complexity of the system.
   - 6.4. Provide an outline of how Security will support other project activities and disciplines, for example Safety, ILS and Training.

7. **Requirements / Composition:**
   - 7.1. The SyMP shall contain as a minimum but not be limited to:
     - 7.1.1. A short description of the project.
     - 7.1.2. A summary of the programme management organisation (including Policy Authorities, Research Authorities, Project Security Officer, Security Assurance Coordinator etc.).
     - 7.1.3. Identification of the requirement for development of programme security grading guidance or reference to the sources of grading guidance for the programme.
     - 7.1.4. Identification of any use of project reference number(s), codewords, national caveats, descriptors, special handling instructions, etc. (e.g. Export Controls, ATOMIC, PSA, NNPPI, etc.) together with their classification and references to any relevant security policies/instructions.
     - 7.1.5. Details of all planned Security activities, including the approach to Security adopted across the supply chain and through each stage of the system lifecycle
     - 7.1.6. Detail a Baseline Security Control set which will be incorporated in the system; as a minimum BS EN ISO/IEC 27001:2017 Controls 5, 6, 7 ,8, 9, 13, 14.3, 16 & 18 or equivalent security standard

7.1.7. The extent of co-operation or collaboration with other countries and details of the appropriate security clauses in the Memorandum of Understanding (MOU), if available.

7.1.8. An Equipment Delivery Plan (EDP) that Shall demonstrate that security is maintained in the entire supply chain and in the transition from a Secure Development Environment (List X managed) to a Secure Operational Environment for both UK and Overseas.

7.1.9. Any special security measures to be adopted for storage of classified hardware.

7.1.10. Levels of security clearance required by personnel associated with the project.

7.1.11. The need for access lists, confidentiality agreements or other restrictions for personnel within the project.

7.1.12. Any special Security Operating Instructions necessary for the protection of sensitive features or capabilities.

7.1.13. Identification of any particular information security requirements including document control procedures, record management, storage and transmission requirements both within the UK and overseas.

7.1.14. Identification of any special procedures for release of equipment information covering defence sales activity, displays, exhibitions and press releases, as well as the visits policy and overseas visitors' clearance procedures.

7.1.15. Mechanisms to securely backup/restore information in accordance with ISO/IEC 24762:2008 clearly defined in SyMP.

7.1.16. Communications security (COMSEC), including the requirements for secure communication devices, teleprinter facilities and authentication tables (including links with Contractors).

7.1.17. Any electronic emission security requirements (may need to be an annex to the main PSP).

7.1.18. Computer Security (COMPUSEC) including installation procedures and data links (including links with Contractors).

7.1.19. Trials Security Instruction (TSI) requirements, including:

a) Trials programme and Trials Conducting Authority.
b) Overall trial classification
c) Special security conditions during trials.
d) Responsibility for the preparation of a trial's security plan/instruction.
e) Security grading for sea, ground and air aspects, as appropriate.
f) Physical security of trials hardware both pre-trail and post-trial.
g) Avoidance of trials forewarnings.
h) Recovery of classified hardware, including accidental loss.
i) Secure transmission of data, including telemetry, both in the UK and overseas
j) Use of secure data links, casual couriers, etc.

k) Processing of classified film.
l) Electronic emission security.

7.1.20. Commercial security interests, including aspects that should carry the descriptor “Commercial”.

7.1.21. Identification of any potential foreign ownership or origin issues.

7.1.22. EDP in accordance with DID-MD-001

7.1.23. Supply Chain Security Risk Assessment Report (SCSyRA Report) in accordance with approved Supply Chain Risk Assessment methodology.

7.1.24. Identification of the procedure for reporting and dealing with security breaches and other security incidents, including but not limited to:

a) Computer Network Defence (CND) notification systems
b) Computer Emergency Response Team (MODCERT)
c) List-X Notices
d) Information Systems and Services (ISS) Web Site
e) Defence Information Assurance Notices (DIANS)
f) Industrial Security Advisory Notices (ISNs)
g) National Cyber Security Centre (NCSC) Threat and Vulnerability Reports
h) Defence Intelligence (DI) Threat Reports
i) Limits on input/export of data except where specified in system functionality.
j) COMPUSEC/INFOSEC protective measures

7.1.25. Disposal requirements of classified hardware (to be also captured in Secure Disposal Plan as required).

DID-Sy-002 - Security Aspects Letter (SAL) - Response

1. **Title:** Security Aspects Letter (SAL) - Response
2. **Number**: DID-Sy-002
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms: N/A**
6. **Description:**

   6.1 Notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.

7. **Requirements**

   7.1 Provided as part of the tenderer's response to the ITN requesting confirmation as stipulated within that artefact.

DID-Sy-003 - DEFFORM 47 Annex G Memorandum of Security for Ministry of Defence (MOD) Contractors

1. **Title:** DEFFORM 47 Annex G Memorandum of Security for Ministry of Defence (MOD) Contractors
2. **Number**: DID-Sy-003
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:**
6. **Description:**

   6.1 This Memorandum outlines the security precautions and requirements which must be taken by companies who are required to access or hold MoD classified information at the SECRET or above level; or who are taking part in tender exercise or contract negotiations.

7. **Requirements:**

   7.1 Request for Confirmation of Security Status of Contractors

   7.2 Provided as part of the tenderer's response to the ITN requesting confirmation as stipulated within that artefact.

DID-Sy-004 - DEFFORM 47 Annex L Supplier Assurance Questionnaire (SAQ)

1. **Title:** DEFFORM 47 Annex L Supplier Assurance Questionnaire (SAQ)
2. **Number**: DID-Sy-004
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms: N/A**
6. **Description:**

   6.1 Mandatory requirement of the Cyber Security Model.

7. **Requirements**

   7.1 Requirement for the completion of the SAQ and submission to the Defence Cyber Protection Partnership (DCPP) Team.

   7.2 Provided as part of the tenderer's response to the ITN requesting confirmation as stipulated within that artefact.

DID-Sy-005 - Security RIO

1. **Title:** MCAST Security RIO (SyRIO) Register
2. **Number:** DID-Sy-005
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** May be incorporated within - DID-PM-002 – Risks, Issues and Opportunities (RIO) Management Plan.
6. **Description:**
   - 6.1. This Data Item Description (DID) contains the requirements, content and format for the MCAST Security (Sy) Risks, Issues and Opportunities Register (SyRIO Register).
   - 6.2. The SyRIO forms a key part of accreditation and should be reviewed in context with the Risk Management and Accreditation Document Set (RMADS).
   - 6.3. The purpose of the MCAST security RIO Register is to provide an audit trail of security Risks, Assumptions, Issues, Dependencies and Opportunities through the course of the programme.

7. **Requirements:**
   - 7.1. The SyRIO Register is a living document, which shall be updated regularly through the course of the programme. This shall involve updating the security Consideration entries with progress including reference to technical evidence, the identification and addition of new considerations derived through security activity carried out within the programme, including those raised by the Authority.
   - 7.2. The SyRIO Register shall be reviewed at every Security Working Group (SyWG). Closure of Security Considerations Shall only be achieved with the agreement of the Authority at the SyWG and recorded in the meeting ROADS.
   - 7.3. The SyRIO shall, as a minimum, contain the following information fields:
     - 7.3.1. Unique Identifier.
     - 7.3.2. Title.
     - 7.3.3. Brief Description of the security Consideration.
     - 7.3.4. Raised by (who raised the Consideration).
     - 7.3.5. Date Raised.
     - 7.3.6. Owner (who owns the Consideration).
     - 7.3.7. Status.
     - 7.3.8. Source.
     - 7.3.9. Classification (Risk, Issue or Opportunity).
     - 7.3.10. Applicable DLOD.
     - 7.3.11. Applicable security area. i.e. COMSEC, COMPUSEC, TEMPEST, Supply chain
     - 7.3.12. Requirement to which the Consideration relates.

7.3.13. Likely Impact (on cost, timescale, or performance. applicable to Risk, Issue and Opportunity).

7.3.14. Probability (of risk occurring or of opportunity being realised).

7.3.15. Mitigation strategy (applicable to risks, issues and opportunities).

7.3.16. Response Plan and associated actions.

7.3.17. Action owner.

7.3.18. Status (Draft, Open, Deferred, Closed).

7.3.19. Rational for closure of the security consideration (reference to evidence describing the solution/resolution as appropriate).

7.3.20. Last Review Date.

7.3.21. Subsystem/equipment (where the consideration is particular to a specific subsystem/equipment e.g. displays, software. Countermeasures, etc).

DID-Sy-006 - Security Roles and Responsibilities

1. **Title:** Security Roles and Responsibilities
2. **Number**: DID-Sy-006
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:**

   6.1 In order for the Information Security objectives to be met, there must be an implementation of clear leadership and accountability, therefore the relevant stakeholders that oversee the Security Accreditation / Assurance of the program should be formally identified. It is best practice to allocate these roles as early as possible in order to promote a good security posture from project initiation.

7. **Requirements:**

   7.1 The key security stakeholder roles shall be formally identified: these may include but are not limited to the following -

   a. **Senior Information Risk Owner (SIRO) -** Responsible for implementing and manging the information risks within the program.
   b. **Security Assurance Coordinator (SAC) -** Provides expert technical advice on security issues and risks to the relevant key stakeholders. Works in conjunction with the Accreditor to provide a clear roadmap to accreditation.
   c. **Information Asset Owners (IAO's) -** Senior/responsible individuals whose roles are to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to clearly understand and address risks to the information.
   d. **Cyber Defence and Risk (CyDR) Accreditor –** Provides expertise and knowledge in order to assess the overall security of the project whilst facilitating the route to accreditation.
   e. **Senior Engineers -** responsible for the implementation of required technical security controls

   7.2 The tenderer shall clearly define what the responsibilities of the chosen roles are (as above) in order to provide a clear picture of competency and accountability within the project.

DID-Sy-007 – Risk Management and Assurance Document Set (RMADS)

1. **Title:** Risk Management and Assurance Document Set (RMADS)
2. **Number:** DID-Sy-007
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms**: GEAR Security Case Template
6. **Description**:
   6.1 The RMADS will be a living document which will define all aspects of security, as required for the continual assurance process.
7. **Requirements:**
   7.1 RMADS Delivered and managed in accordance with the following guidance –
      7.1.1 NCSC Good Practice Guide 47 – Information Risk Management
      7.1.2 Government Security Policy Framework
      7.1.3 BSI BS EN ISO/IEC/27001
      7.1.4 Def Stan 21-088
   7.2 RMADS must be approved by the Authority.
   7.3 RMADS are to be produced in accordance with the latest issue GEAR security case template.
   7.4 RMADS are to include (but not be limited to) –
      7.4.1 Security Risk Assessment Outcome
      7.4.2 Security Design Document
      7.4.3 Security Configuration Model
      7.4.4 Security Operating Instructions
   7.5. RMADS will be maintained as a live document which will define all aspects of security and be reviewed regularly.

2.5 Safety Plan

DID-S+E-001 - Safety and Environmental Management Plan

1. **Title:** Safety and Environmental Management Plan (SEMP)
2. **Number:** DID-S+E-001
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms: N/A**
6. **Description:**

   6.1 The SEMP to be delivered should describe the management of risk and impacts associated with the Safety and Environmental Protection issues relating to the Maritime Command and Staff Trainer (MCAST) Project.
7. **Requirements:**

   7.1 The SEMP should be produced in light of the Authorities MCAST SEMP and adhere to those requirements stipulated within that artefact.

DID-S+E-002 - Safety and Environmental Case Reports

1. **Title:** Safety and Environmental Case Reports (SECR)
2. **Number:** DID-S+E-002
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms:** N/A
6. **Description:**

   6.1 An integrated programme of safety and environmental activities will be ensured through hazard, safety and environmental protection management documentation including Safety and Environmental Case Reports (SECR).

7. **Requirements:**

   7.1 Produce Safety and Environmental Case Reports (SECR's) which summarise the Safety and Environmental Case (S&EC) at a specific point in time. The S&ECR shall be suitable for endorsement by the Authority.

   7.2 SECR's shall contain as a minimum but not be limited to:

   7.2.1 Accident Record

   7.2.2 Accident Register

   7.2.3 Hazard Log

   7.3 SECRs are required;

   7.3.1 In readiness to support Initial Operating Capability (IOC).

   7.3.2 To reflect significant changes to the MCAST systems.

   7.3.3 To support Full Operating Capability (FOC).

   7.3.4 Annually or at major changes to the systems.

   7.3.5 At the start and end of each transition phase.

   7.4 The Safety and Environmental Committee shall take actions to reduce hazards and environmental impacts and shall approve Safety Case documentation. Members of the Safety and Environmental Committee shall also provide SQEP representation at relevant reviews where the Authority deems it appropriate.

   7.5 The SECR should be produced in light of the Authorities MCAST SEMP and adhere to those requirements stipulated within that artefact.

DID-QM-001 – Service Quality Management Plan

1. **Title:** Service Quality Management Plan (SQMP)
2. **Number:** DID-QM-001
3. **Version:** 1.0
4. **Delivery Schedule:** Refer to Appendix D to SoW – Contract Deliverables
5. **Applicable Forms: N/A**
6. **Description:**

   6.2 The SQMP in accordance with AQAP 2105 is the document that provides the Authority with confidence that the Contractor can deliver to meet the Quality demands required for the MCAST Service. It should contain coherent information that clearly articulates how the Quality Management System is implemented during the product lifecycle. The Contractor shall manage the Service under a formal Quality Management Plan within the Contractor's ISO9001:2015 accredited Quality Management System.

7. **Use:**

   7.1 The Authority will use the Service Quality Management Plan to:

   7.2 Gain confidence that the quality of work related to developing and delivering the service has been identified.

   7.3 Gain confidence that the Contractor has appropriate procedures in place to ensure a robust Quality Management System.

8. **Applicable Standards:**

   8.1 BSI BS EN ISO 9001: 2015 - Quality Management Systems — Requirements.
   8.2 AQAP-2110 Ed. D ver. 1 - NATO Quality Assurance (QA) Requirements for Design, Development and Production.
   8.3 AQAP-2210 Ed. A ver. 2 - NATO Supplementary Software QA Requirements to AQAP 2110 or AQAP-2310.
   8.4 AQAP 2105 (Ed. 2) - NATO Requirements for Deliverable Quality Plan.
   8.5 DEF STAN 05-061, Part 1 Issue 6 - Quality Assurance Procedural Requirements – Concessions.
   8.6 DEF STAN 05-135, Issue 2 - Avoidance of Counterfeit Materiel.
   8.7 DEF STAN 05-061, Part 4 Issue 3 - Quality Assurance Procedural Requirements - Contractor Working Parties.
   8.8 DEF STAN 05-061, Part 9 Issue 5 - Quality Assurance Procedural Requirements - Independent Inspection Requirements for Safety Critical Items.

9. **Requirements:**

   The Service Quality Management Plan Shall contain but not be limited to:

   9.1 A formal quality assurance process of the Service shall be carried out in accordance with DSAT Training Quality requirements. This will include recording and addressing non compliances against formal quality assurance procedures and continual improvement based on the capture of user feedback and service provider feedback.

   9.2 List of procedures and processes that detail how the Quality Management System Shall be used to deliver the contract requirements.

9.3 Arrangements for quarterly Quality Management reviews.

9.4 Details of the Contractors accreditation.

9.5 Details of the organisation and relevant interfaces.

9.6 List of Quality resource their SQEP and the level of resource commitment to the project.

9.7 Supply base codes of practice, interfaces and standards policy.

9.8 Configuration control arrangements.

9.9 List of applicable standards, specifications, Quality Audit/Quality Control documentation and certification records.

9.10 Specific arrangements for assurance of the quality of supplies from Suppliers and Sub-suppliers and the compliance measures to be adopted.

9.11 Arrangements for avoidance of counterfeit materials.

9.12 Programme of internal audits.

9.13 Arrangements for Concessions and Non-conformances.

9.14 In support of the Service Quality Management Plan the following reports are required:

9.14.1 The Contractor shall prepare a Quality Manual for the MCAST service. This shall be compliant with BS ISO 9001:2015 requirements and maintained throughout the life of the Service. Reviewed at least annually with International Organization for Standardization (ISO) accreditation audits.

9.14.2 The Contractor shall record Non-Conformances/non-compliances in accordance with the Quality Management System requirements.

9.14.3 The Contractor shall prepare and maintain a Regulatory Compliance Document and record of certificates or statements of compliance and any non-conformances shall be maintained in accordance with the Quality Management System.