Ministry of Defence

de&s

Defence Equipment & Support

OI/0080 – Logistic Support Bridge In-Service Support

ANNEX A – Statement of Requirement

Equipping and Supporting our Armed Forces

Issued by:

Fires, Infrastructure and Manoeuvre Support (FIMS)

Conditions for Release:

The information provided within this document is supplied without commitment or prejudice.

This information is released by the UK Government for Defence purposes only. It must be accorded the same degree of security protection as that accorded thereto by the UK Government.

Foreword

This Statement of Requirements (SOR) contains information which is proprietary to the Secretary of State for Defence and shall remain the property of the Secretary of State for Defence. It is issued in strict confidence and must not be seen by any unauthorised person. The SOR is supplied solely for the purpose of performance of the Contract and shall not be copied or reproduced or used for any other purpose whatsoever without the express prior written permission of the Secretary of State for Defence as represented by the Authority.

Technical data in this document refers to the edition current at the date of Contract unless otherwise stated.

This document applies to the Logistic Support Bridge - hereon in will be referred to as ‘LSB’.

Contents

Acronyms / Abbreviations

Acronym / Abbreviation	Definition
AESP	Army Equipment Support Publication
DA	Design Authority
DE&S	Defence Equipment and Support
GFE	Government Furnished Equipment
LSB	Logistic Support Bridge
MOD	Ministry of Defence
MS	Microsoft
PDS	Post Design Services
PSEP	Project Safety Environmental Panel
QAR	Quality Assurance Representative
SDM	Service Delivery Manager
SOR	Statement of Requirement
SPOC	Single Point of Contact
TAF	Tasking Form
UKAS	United Kingdom Accreditation Service

1. Requirements

1.1. This Statement of Requirement (SOR) details the activities to be performed by the role of the Logistic Support Bridge (LSB) Design Authority (DA) within the overall LSB In-Service Support Programme. It defines the Scope of Work that the DA shall be required to undertake as part of the overall support strategy for continued maintenance of the system.

2. Context

2.1. The UK Ministry of Defence (MOD)'s LSB Framework Programme is an arrangement that will facilitate individual tasks to be placed by the Authority as they are required.

2.2. This covers the period from 04-September 2023 to 03-September 2023 (5 years) - noting that the Authority has no obligation to place any tasking during this period. The Contractor shall be tasked by the Authority as required during this period. This could include, but not be limited to, activities such as: **design or technical support; management of drawings/artwork; ad-hoc meetings; improvement or modification of the bridge design, attendance at the Project Safety Environmental Panel (PSEP); support to Safety Management; Post Design Services (PDS); Provision of Customer Support.**

3. Aims

3.1. This SOR details the Authority's requirements which the Contractor shall undertake to the support of LSB. This framework arrangement contains no core element and Tasks shall be requested as and when required by the Authority.

4. Framework - Task Management

4.1. The Authority shall raise a Tasking Form (TAF) in accordance with the stated process at Appendix A of this Annex A, and the TAF's laid out in **OI/0080 Annex B** – *Tasking Form & Process*

4.2. The Contractor shall produce and deliver Task quotes and/or SOR to the Authority.

4.3. Prior to commencement of any Task, the Contractor shall provide to the Authority the following information with all Task proposals, as a TAF Part 2:

- Price complete with a detailed breakdown, including sub-contractor cost and supporting quotations.
- Option price for design incorporation of drawing build standard update (if appropriate).
- Task scope of work detailing the Tasks and Key Deliverables.

- If requested, a proposed dated project schedule provided in Microsoft (MS) Project, clearly displaying key milestones for the Task.
- Government Furnished Equipment (GFE) requirements (if applicable).
- Caveats or limitations, including risks.
- A completed & signed DEFFORM 177 (if appropriate).

4.4. The Contractor may request the re-scheduling of a Non-Core Task at any time, if they believe there are sound capability and/or resource reasons to do so. Such requests must be submitted to and approved by the Authority.

4.5. Similarly, the Authority may request the Contactor to re-align a Non-Core Task schedule to overcome or mitigate Authority departmental constraints or priorities.

4.6. Personnel employed under the Contract shall have appropriate qualifications and competence for Tasks on which they are engaged, and in all aspects are acceptable to the Authority. The Authority may only object on reasonable and demonstrable grounds.

4.7. The Contractor shall ensure deliverables for each Task are managed, reported and achieved in accordance with agreed tasking timescales. The Authority will monitor performance and highlight deficiencies to the Contractor for resolution as applicable.

4.8. As System DA, the Contractor shall manage and control all tasking, including that which is provided under sub-contracts by any sub-system DA or any other sub-contractor undertaking design duties.

5. Project Management

5.1. The Contractor shall appoint a Project Manager who shall act as the SPOC for the Authority to contact on all matters relating to the project.

6. Meetings and Reporting

6.1. There are no contracted Contractor meetings or reporting requirements. Contractor engagement will be tasked on an ad-hoc basis, as required by the Authority.

7. Documentation Management

7.1. All documentation and electronic information sent by the Contractor must be fully compatible with the Authority’s notified standard of software in either an MS Word document or in .pdf format.

7.2. All publications produced by the Contractor will be produced in accordance with the Defence Technical Documentation Guidance.

7.3. The Contractor shall complete all amendments to Army Equipment Support Publications (AESPs) as tasked by the Contractor and shall verify the content. Amendments shall comply with AESP-0100-P-Series: *Specification for AESPs*.

7.4. Documentation control procedures will be carried out in accordance with the Contract Terms and Conditions.

8. Drawings

8.1. Drawings are to be supplied/updated in both hardcopy (where hardcopy format exists) and electronic copy when required by ad-hoc PDS Tasks. All changes to drawings must be logged in accordance with the Authority's procedures and DEFSTAN 05-010 - *Product Definition Information* (parts 1 and 2).

9. Government Furnished Equipment (GFE)

9.1. If a specific Task requires GFE, the Contractor will hold a GFE List for the equipment held on behalf of the Authority for the duration of the task. This will be provided upon request for Audits conducted by the National Audit Office (NAO).

10. Safety

10.1. The Contractor shall consider all safety aspects for each Non-Core Task. The Contractor shall inform the Authority of any hazard arising from a modification, which will have an impact on the overall Equipment Safety Case.

10.2. Where the Contractor undertakes contracted activities on safety critical items, the requirements of DEFSTAN 05-61 (part 9) - *Independent Inspection Requirements for Safety Critical Items* shall be complied with.

11. Quality

11.1. The Contractor shall demonstrate certification to the **ISO 9001:2015** standard as accredited by a United Kingdom Accreditation Service (UKAS) recognised third party auditing body.

11.2. The scope of the certification should be applicable for the design and manufacture of bridging products and is to be maintained throughout the life of the contract, and for the location where the majority of the activities are undertaken, without the Authority incurring additional cost.

11.3. In accordance with **AQAP 2110 -** *NATO Quality Assurance Requirements for Design, Development and Production*, the Contractor shall provide assistance and facilities for quality audits undertaken by the Authority's Quality Assurance Representative (QAR) as and when required.

12. Non-Conformance

12.1. Where the Contractor seeks approval to deliver non-conforming product, the Contractor shall comply with the requirements of DEFSTAN 05-61 (part 1) - *Concessions.*

13. Counterfeit Avoidance System

13.1. Counterfeit Avoidance Management shall be managed in accordance with DEFSTAN 05-135 (issue 2) - *Avoidance of Counterfeit Materiel*.

14. Contractor Working Parties (CWP)

14.1. Where the Contractor is required to undertake specific tasks at a MOD establishment, facility or at external locations away from the Contractor's premises, the requirements of DEFSTAN 05-61 (part 4) - *Contractor Working Parties* shall be complied with.

15. Modification Kits

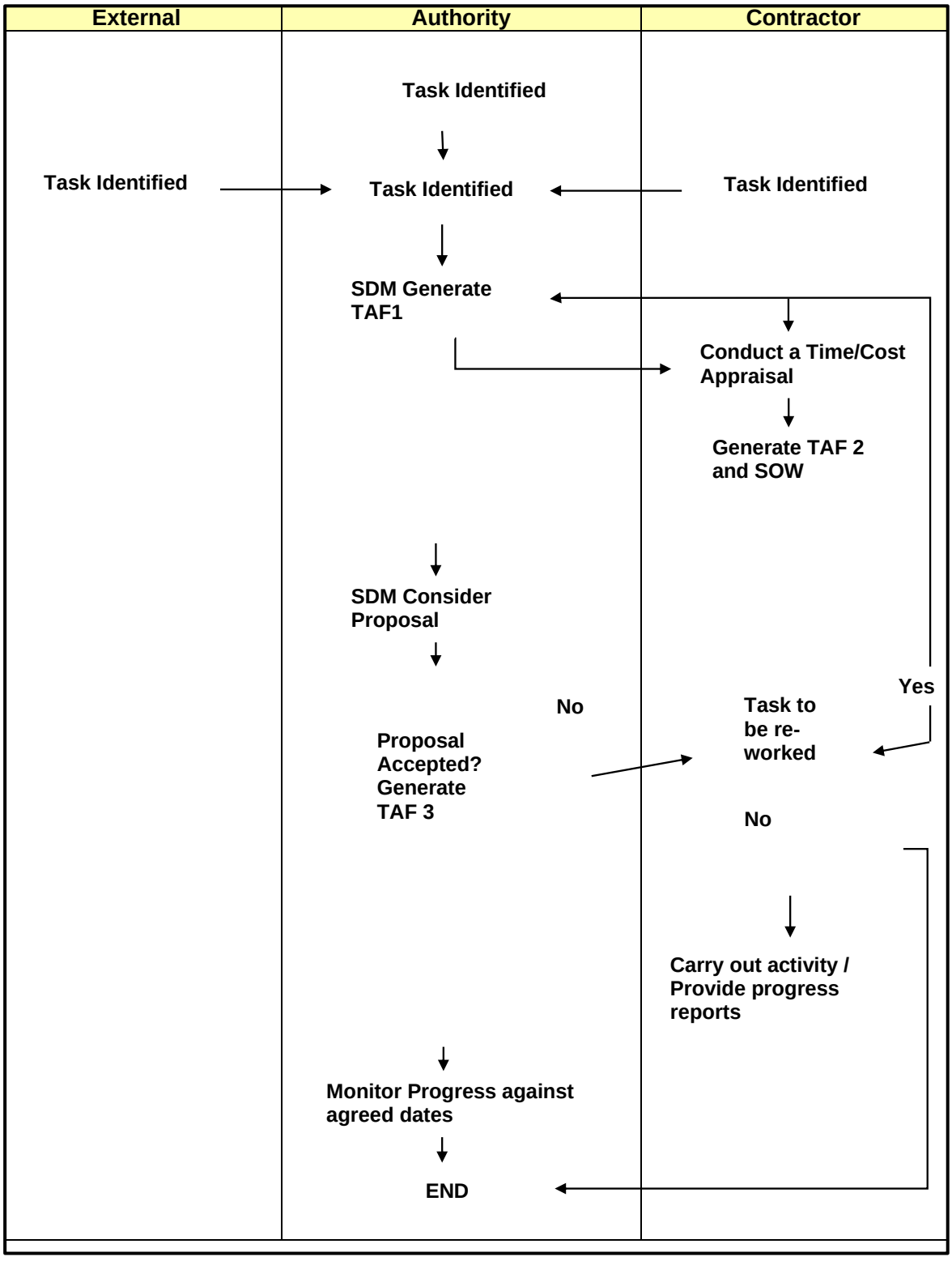
15.1. The Contractor may be tasked to design, procure and fit modifications to the Equipment in certain circumstances and under the specific direction from the Authority:

- Preparing service modification schedules and fitting instructions, as tasked.
- Recommending the range of spares and quantity of spares required to the equipment and if required, codifying the spares, as tasked.

16. Purchase of Capital Spares

16.1. The Contractor may be required to have the capability to manufacture and supply capital spares related to the equipment, as directed by the Authority. Should the Authority choose to invoke this option, a specific SOR will be produced by the Authority and agreed with the Contractor.

APPENDIX A : Tasking Process



Ministry of Defence

de&s

Defence Equipment & Support

OI/0080 – Logistic Support Bridge In-Service Support

ANNEX B – LSB Tasking Forms and Process

Equipping and Supporting our Armed Forces

Issued by:

Fires, Infrastructure and Manoeuvre Support (FIMS)

Conditions for Release:

The information provided within this document is supplied without commitment or prejudice.

This information is released by the UK Government for Defence purposes only. It must be accorded the same degree of security protection as that accorded thereto by the UK Government.

Foreword

This Contract Annex contains information which is proprietary to the Secretary of State for Defence and shall remain the property of the Secretary of State for Defence. It is issued in strict confidence and must not be seen by any unauthorised person. It is supplied solely for the purpose of performance of the Contract and shall not be copied or reproduced or used for any other purpose whatsoever without the express prior written permission of the Secretary of State for Defence as represented by the Authority.

Technical data in this document refers to the edition current at the date of Contract unless otherwise stated.

This document applies to the Logistic Support Bridge - hereon in will be referred to as ‘LSB’.

1. Application

1.1. This document sets out the processes and procedures, responsibilities and activities that shall be undertaken by both the Contractor and the Authority to initiate any Non-Core Tasking as defined in OIP/0080 Annex A - Statement of Requirement. Non-Core Tasking will be required as part of the overall support strategy for the continued maintenance of the LSB system.

2. Tasking Form Processes

2.1. When the Contractor or the Authority identify a requirement for Non-Core Tasking, the Authority will raise a Non-Core Tasking Form (TAF) Part 1.

2.2. Within ten working days of receipt of a TAF Part 1, the Contractor shall complete and return to the Authority a TAF Part 2 -Time/Cost Quotation form. If the Contractor requires an extension to this period, this shall be requested by the Contractor no later than 5 working days after the TAF Part 1 is received. The Authority will review any requests for extensions and, acting reasonably, will grant them where considered appropriate.

2.3. Where relevant, the Contractor's TAF Part 2 will be in accordance with the agreed rates stated in the Contract.

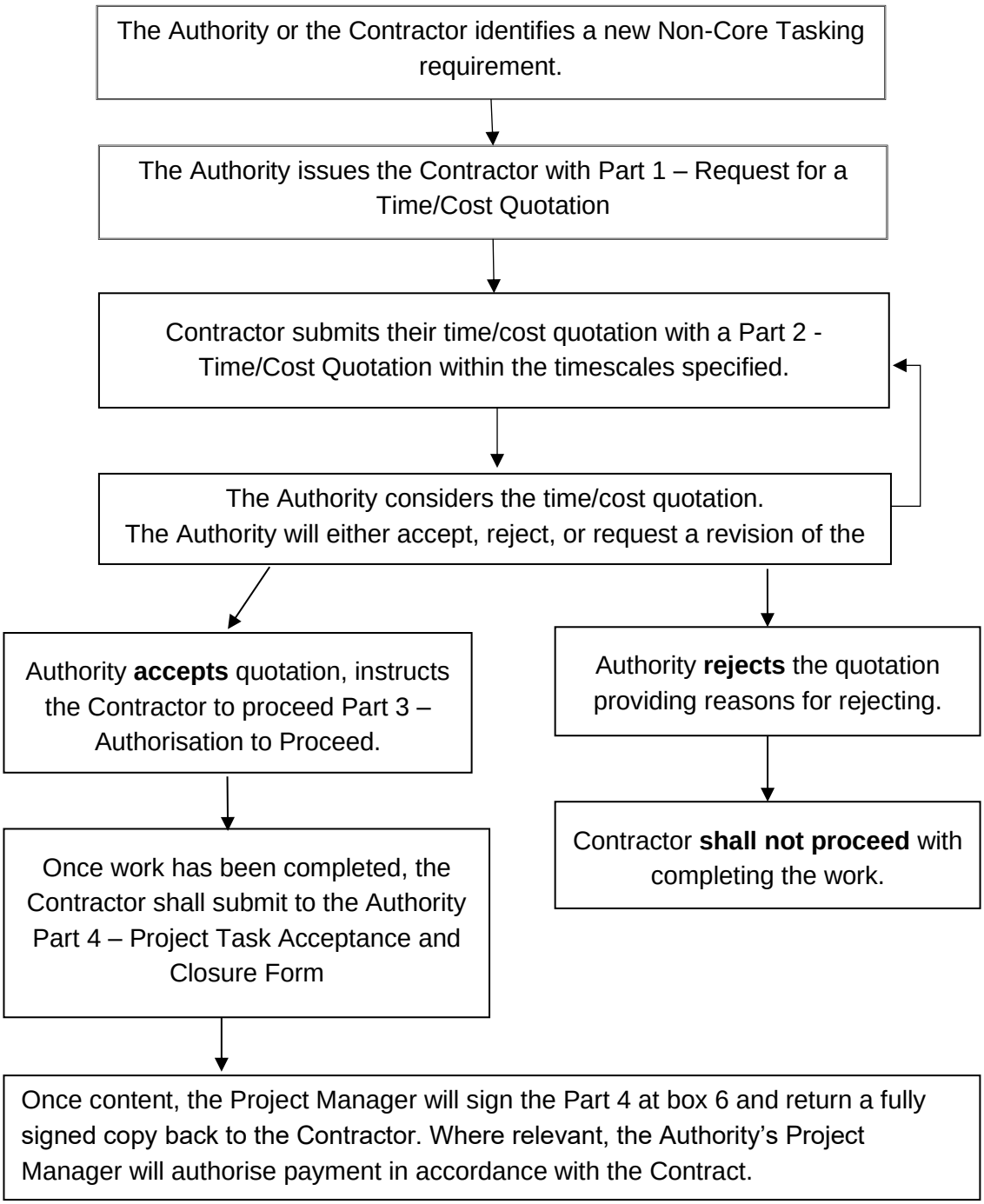
2.4. Upon Acceptance of the TAF Part 2 issued by the Contractor, the Authority will issue the Contractor with a TAF Part 3 as authorisation to proceed or cancel.

2.5. The Contractor's progress against the task shall be reported by the Contractor as requested by the Authority.

2.6. Upon completion of the task, the Contractor shall complete TAF Part 4 - Project Task Acceptance and Closure Form and submit to the Authority for task closure. This will confirm compliance against the agreed acceptance criteria as stated at TAF Part 1 and provide supporting evidence of compliance where appropriate.

2.7. Subject to satisfactory completion of the task, the Authority's Project/Service Delivery Manager will authorise payment in accordance with the terms and conditions of the Contract.

3. Post Design Services (PDS) Tasking Flowchart



TAF – Part 1

Part 1 – Request for Time/Cost Quotation

To be Completed by the Authority

To:		From:
Mabey Bridge Unit 9 Lydney Harbour Estate Harbour Road Lydney GL15 4EJ		Operational Infrastructure (OI) Fires, Infrastructure and Manoeuvre Support (FIMS) Defence Equipment and Support (DE&S) #4140, Elm 1C MOD Abbey Wood South Bristol BS34 8JH
Task No:	XXX	Contract Number: **OI/0080**
All intellectual property generated under this tasking will be subject to DEFCON 703 unless this box is checked and a completed DEFFORM 315 is attached.		☐
Task Title		
Priority	Standard /High (delete as appropriate)	
A. Description and scope of work:		
B. Security Classification [must be completed]:		OFFICIAL-SENSITIVE
C. Date:		

Signed: Project/Service delivery manager				
NAME:				

TAF – Part 2

Part 2 – Time/Cost Quotation

To be Completed by the Contractor

To:		From:	
Operational Infrastructure (OI) Fires, Infrastructure and Manoeuvre Support (FIMS) Defence Equipment and Support (DE&S) #4140, Elm 1C MOD Abbey Wood South Bristol BS34 8JH		Mabey Bridge Unit 9 Lydney Harbour Estate Harbour Road Lydney GL15 4EJ	
Task No:	XXX	Contract Number: **OI/0080**	
Assumed Start Date:		Est. Completion Date:	

A quotation for the work detailed in Part 1 is provided below. This Task can be undertaken without conflict with existing commitments.

Description of work to be completed:

	Hours/Qty	Rate	Total
Direct Labour (Firm man hour rates inclusive of profit & overheads) (Breakdown by grade should be attached separately)			
Material/Subsistence			
Bought out parts			
Sub-contracted work			
Other (e.g., sub-contractor costs – breakdown should be attached separately)			
Travel and Subsistence			
Hotel and Subsistence (breakdown should be attached separately)			
Mileage (per mile)			
Total Firm Price (excluding VAT)	-		
Name: **(Block Capitals)**	**Date:**		

TAF – Part 3

Part 3 – Authorisation to Proceed/Cancellation

To be completed by the Authority

To:		From:	
Mabey Bridge Unit 9 Lydney Harbour Estate Harbour Road Lydney GL15 4EJ		Operational Infrastructure (OI) Fires, Infrastructure and Manoeuvre Support (FIMS) Defence Equipment and Support (DE&S) #4140, Elm 1C MOD Abbey Wood South Bristol BS34 8JH	
Contract No:	**OI/0080**	Task No:	XXX

To be completed by OI Project/Service Delivery Manager:	
a.	Please proceed with the work to the total cost £ ……. **(VAT ex. firm price)** as quoted in Part 2 – time/cost quotation dated ……. All work to be completed by ……. Government Furnished Assets (GFA) has been identified and attached ……
b.	Please provide a **revised** Part 2 - time/cost quotation for Task No …….
c.	Please take no further action
d.	Please terminate work on this task and supply the cost of termination

Cost Control Officer:			
Signed:	Cost Control Officer (Block Capitals)	Tel:	
Name:		Date:	

Commercial Officer:			
Signed:	Commercial Officer (Block Capitals)	Tel:	
Name:		Date:	

Project/Service Delivery Manager:			
Signed:	Service Delivery Manager (Block Capitals)	Tel:	
Name:		Date:	

Payment Terms shall be as follows (Tick appropriate box):		
Payment on satisfactory completion of all work.		Stage Payments (as attached)
Please confirm receipt of this task authorisation. Once you have confirmed receipt, you should proceed with performance of the Task.		

TAF – Part 4

Part 4 - Project Task Acceptance and Closure Form

To be completed by the Contractor

<table>
<tr><td rowspan="11">To be Completed by the Contractor</td><td colspan="2">To:</td><td colspan="2">From:</td></tr>
<tr><td colspan="2">Operational Infrastructure (OI)
Fires, Infrastructure and Manoeuvre Support (FIMS)
Defence Equipment and Support (DE&S)
#4140, Elm 1C
MOD Abbey Wood South
Bristol
BS34 8JH</td><td colspan="2">Mabey Bridge
Unit 9
Lydney Harbour Estate
Harbour Road
Lydney
GL15 4EJ</td></tr>
<tr><td colspan="2">Task No: XXX</td><td colspan="2">Contract Number: OI/0080</td></tr>
<tr><td>#</td><td>Acceptance Criteria</td><td>Criteria Compliance offered</td><td>Evidence Supplied Y/N</td></tr>
<tr><td>1</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td></tr>
<tr><td>4</td><td></td><td></td><td></td></tr>
<tr><td>5</td><td></td><td></td><td></td></tr>
<tr><td>6</td><td></td><td></td><td></td></tr>
<tr><td>7</td><td></td><td></td><td></td></tr>
<tr><td colspan="4">I can confirm that Task OI/… is completed in its totality.</td></tr>
<tr><td colspan="4"><table><tr><td>Name:</td><td>Position:</td><td>Signature:</td><td>Date</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
<tr><td rowspan="3">To be Completed by the Authority</td><td colspan="4">I am content Task OI/…. is complete and can be closed. I can confirm that all deliverables have been received and that all payments have been made.</td></tr>
<tr><td colspan="4"><table><tr><td>Name:</td><td>Position:</td><td>Signature:</td><td>Date</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Copies to: OI Project/Service Delivery Manager, OI Commercial Officer

Ministry of Defence

de&s

Defence Equipment & Support

OI/0080 – Logistic Support Bridge In-Service Support

ANNEX C – Firm Rates

Contractor Labour Rates

GRADE	Payment Period from Service Commencement Date - Used in accordance with condition 2.3 of the Contract									
	Year 1		Year 2		Year 3		Year 4		Year 5	
	1 June 2023 To 31 May 2024		1 June 2024 To 31 May 2025		1 June 2025 To 31 May 2026		1 June 2026 To 31 May 2027		1 June 2027 To 31 May 2028	
	½ day	Full day	½ day	Full day	½ day	Full day	½ day	Full day	½ day	Full day
CAD	[redacted]									
Project Management	[redacted]									
Site Management UK	[redacted]									
Site Management International	[redacted]									
Engineer	[redacted]									

Travel and Subsistence

	Payment Period from Service Commencement Date - Used in accordance with condition 2.3 of the Contract				
	Year 1	Year 2	Year 3	Year 4	Year 5
	1 June 2023 To 31 May 2024	1 June 2024 To 31 May 2025	1 June 2025 To 31 May 2026	1 June 2026 To 31 May 2027	1 June 2027 To 31 May 2028
Hotel & Subsistence	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Mileage Rate (p/m)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Non-Core Firm Charging Rates

Non-Core Item	Payment Period from Service Commencement Date - Used in accordance with condition 2.3 of the Contract									
	Year 1		Year 2		Year 3		Year 4		Year 5	
	1 June 2023 To 31 May 2024		1 June 2024 To 31 May 2025		1 June 2025 To 31 May 2026		1 June 2026 To 31 May 2027		1 June 2027 To 31 May 2028	
	½ day	Full day	½ day	Full day	½ day	Full day	½ day	Full day	½ day	Full day
CAD	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Project Management	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Ministry of Defence

de&s

Defence Equipment & Support

OI/0080 – Logistic Support Bridge In-Service Support

Contract Appendix - Security Aspects Letter

Equipping and Supporting our Armed Forces

[redacted]

[redacted]

Operational Infrastructure
Defence Equipment & Support
NH4; Elm 1C
MOD Abbey Wood
Bristol
BS34 8JH

Mabey Bridge
Unit 9 Lydney Harbour Estate
Harbour Road
Lydney
Gloucestershire
GL15 4EJ

Date of Issue: 25-August 2023

Our Ref.: OI/0080

CONTRACT NUMBER & TITLE: OI/0080 - Logistic Support Bridge (LSB) In-Service Support

1. On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.

2. Aspects that constitute OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
Information listed in Schedule 4 (information notified by the Contractor to the Authority), which is acknowledged by the Authority.	OFFICIAL / OFFICIAL SENSITIVE
All Tender documents (and the information contained); All models / hardware or software.	OFFICIAL
All reports, meeting minutes and written deliverables.	OFFICIAL
All information stated in **Annex C** - UK OFFICIAL and OFFICIAL-SENSITIVE Contractual Security Conditions (as appropriate)	OFFICIAL / OFFICIAL SENSITIVE

3. Your attention is drawn to the provisions of the Official Secrets Act 1911-1989 in general, and specifically to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989). In particular you should take all reasonable steps to make sure that all individuals employed on any work in connection with this Contract have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply after completion or earlier termination of the contract.

4. **Will you please confirm that:**

a. This definition of the classified aspects of the referenced Contract has been brought to the attention of the person directly responsible for security of classified material.

b. The definition is fully understood.

c. Measures can, and will, be taken to safeguard the classified aspects identified herein in accordance with applicable national laws and regulations, and that the requirement and obligations set out above and in any contractual document can and will be met and that the classified information shall be protected in accordance with applicable national laws and regulations.

d. All employees of the company who will have access to classified information have either signed the OSA Declaration Form in duplicate and one copy is retained by the Company Security Officer or have otherwise been informed that the provisions of the OSA apply to all classified information and assets associated with this contract.

5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.

6. Classified Information associated with this Contract must not be published or communicated to anyone without the approval of the MOD Contracting Authority.

7. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON 76.

Yours faithfully

[redacted]

[redacted]

Commercial Officer, Operational Infrastructure

ANNEX C - UK OFFICIAL + UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

Purpose

1. This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: COO-DSR-IIPCSy@mod.gov.uk).

Definitions

2. The term *"Authority"* for the purposes of this Annex means the HMG Contracting Authority.

3. The term *"Classified Material"* for the purposes of this Annex means classified information and assets.

Security Grading

4. The SENSITIVE caveat is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading. The Contractor is not required to mark documents graded UK OFFICIAL unless they are transmitted overseas or generated by a Contractor based outside the UK in a third-party country.

Security Conditions

5. The Contractor shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. The Contractor shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract. The Authority must state the data retention periods to allow the Contractor to produce a data management policy. If you are a Contractor located in the UK your attention is also drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular.

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material

6. The Contractor shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

7. Once the Contract has been awarded, where Contractors are required to store or process UK MOD classified information electronically, they are required to comply with the accreditation requirements specified in ISNs, Defence Condition 658 and Defence Standard 05-138. Details can be found at the links below:

https://www.gov.uk/government/publications/industry-security-notices-isns.

http://dstan.gateway.isg-r.r.mil.uk/standards/defstans/05/138/000002000.pdf

https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

8. All UK classified material including documents, media and other assets must be physically secured to prevent unauthorised access. When not in use UK classified material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be controlled.

9. Disclosure of UK classified material must be strictly controlled in accordance with the *"need to know"* principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or sub-Contractor.

10. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any classified material issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 8 above, the Contractor shall not make use of any article or part thereof similar to the articles for any other purpose.

11. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.

12. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 34.

Access

13. Access to UK classified material shall be confined to those individuals who have a *"need-to-know"*, have been made aware of the requirement to protect the material and whose access is essential for the purpose of their duties.

14. The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE material have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by

the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf

Hard Copy Distribution

15. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed internally and externally of Contractor premises. To maintain confidentiality, integrity and availability, distribution is to be controlled such that access to documents is only by authorised personnel. They may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

16. Advice on the distribution of UK OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of UK OFFICIAL-SENSITIVE shall be sought from the Authority.

Electronic Communication and Telephony and Facsimile Services

17. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation are available at: https://www.ncsc.gov.uk/guidance/tls-external-facing-services

Details of the CPA scheme are available at: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

18. Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Authority require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the information.

19. UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so.

20. UK OFFICIAL information may be faxed to recipients located both within the country of the Contractor and overseas, however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

Use of Information Systems

21. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here in specific detail; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

22. The Contractor should ensure **10 Steps to Cyber Security** (Link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information. The Contractor should ensure competent personnel apply 10 Steps to Cyber Security: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

23. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

24. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum-security requirements for processing and accessing UK OFFICIAL-SENSITIVE information on IT systems.

a. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of *"least privilege"* will be applied to System Administrators. Users of the IT System (Administrators) should not conduct 'standard' User functions using their privileged accounts.

b. Identification and Authentication (ID&A). All systems are to have the following functionality:

(1). Up-to-date lists of authorised users.

(2). Positive identification of all users at the start of each processing session.

c. Passwords. Passwords are part of most ID&A security measures. Passwords are to be *"strong"* using an appropriate method to achieve this, e.g., including numeric and *"special"* characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control. All systems are to have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g., point to point computer links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 17 above.

f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

(1). The following events shall always be recorded:

(a) All log on attempts whether successful or failed,

(b) Log off (including time out where applicable),

(c) The creation, deletion or alteration of access rights and privileges,

(d) The creation, deletion or alteration of passwords.

(2). For each of the events listed above, the following information is to be recorded:

(a) Type of event,

(b) User ID,

(c) Date & Time,

(d) Device ID.

The accounting records are to have a facility to provide the System Manager with a hard copy of all or selected activity. There also must be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this, then the equipment must be protected by physical means when not in use i.e., locked away or the hard drive removed and locked away.

g. Integrity & Availability. The following supporting measures are to be implemented:

(1). Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g., viruses and power supply variations),

(2). Defined Business Contingency Plan,

(3). Data backup with local storage,

(4). Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software),

(5). Operating systems, applications and firmware should be supported,

(6). Patching of Operating Systems and Applications used are to be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

h. Logon Banners. Wherever possible, a *"Logon Banner"* will be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be:

"Unauthorised access to this computer system may constitute a criminal offence"

i. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections. Computer systems must not be connected direct to the Internet or *"un-trusted"* systems unless protected by a firewall (a software based personal firewall is the minimum, but risk assessment and management must be used to identify whether this is sufficient).

k. Disposal. Before IT storage media (e.g., disks) are disposed of, an erasure product must be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Laptops

25. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 17 above.

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites[1]. For the avoidance of doubt the term *"drives"* includes all removable, recordable media e.g., memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

27. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

28. Portable CIS devices holding the Authorities' data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and Incident Reporting

29. The Contractor shall immediately report any loss or otherwise compromise of any Defence Related Classified Material to the Authority. The term Defence Related Classified Material includes MOD Identifiable Information (MODDII) (as defined in ISN2016/05) and any information or asset that has been given a security classification by the UK MOD. The term also includes classified information and assets held by UK Defence Contractors which are owned by a third party e.g., NATO or another country for which the UK MOD is responsible.

30. In addition any loss or otherwise compromise of Defence Related Classified Material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the UK MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD's Chief Information Officer (CIO) and, as appropriate, the Contractor concerned. The UK MOD Defence Industry WARP will also advise the Contractor what further action is required to be undertaken.

UK MOD Defence Industry WARP Contact Details

Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)

RLI Email: defencewarp@modnet.r.mil.uk (MULTIUSER)

Telephone (Office hours): +44 (0) 30 6770 2185

Mail: Defence Industry WARP, DE&S PSyA Office

MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

31. Reporting instructions for any security incidents involving Defence Related Classified Material can be found in the Incident Reporting Industry Security Notice at: https://www.gov.uk/government/publications/industry-security-notices-isns

Sub-Contracts

32. Where the Contractor wishes to sub-contract any elements of a Contract to sub-Contractors within its own country or to Contractors located in the UK such sub-contracts will be notified to the Contracting Authority. The Contractor shall ensure that these Security Conditions are incorporated within the sub-contract document.

33. The prior approval of the Authority shall be obtained should the Contractor wish to sub-contract any UK OFFICIAL-SENSITIVE elements of the Contract to a sub-Contractor facility located in another (third party) country. The first page of Annex A (MOD Form 1686 (F1686) of ISN 2022/08 is to be used for seeking such approval. The MOD Form 1686 can be found at: ISN_2022-08_Subcontracting_or_Collaborating_on_Classified_MOD_Programmes.pdf (publishing.service.gov.uk)

34. If the sub-contract is approved, the Contractor shall flow down the Security Conditions in line with paragraph 32 above to the sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

Physical Destruction

34. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when the classified material cannot be destroyed or, unless already authorised by the Authority, when the Contractor considers its retention to be necessary or desirable. Unwanted UK OFFICIAL-SENSITIVE classified material which cannot be destroyed in such a way shall be returned to the Authority.

Private Venture Activities

35. Private Venture (PV) funded (i.e., non-MOD funded) defence related projects and technology fall within one of the following three categories:

[1] Secure Sites are defined as either Government premises or a secured office on the contractor premises.

- Variants. Variants of standard defence equipment under research, development or in production, e.g., aircraft, military vehicles or ships, etc., with non-standard equipment or fitments, offered to meet special customer requirements or to avoid security or commercial difficulties associated with the sale of an item in-Service with UK Armed Forces;
- Derivatives. Equipment for military or civil use that is not based on standard Service designs but is dependent upon expertise or technology acquired in the course of defence contracts;
- Freelance. Equipment of defence importance that is in no way based on information gained from defence contracts;

36. UK Contractors shall ensure that any PV activity that falls into one of the above categories has been formally security graded by the MOD Directorate of Security and Resilience. Please see PV guidance on the following website further information: https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets

Publicity Material

37. Contractors wishing to release any publicity material or display assets that arises from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the UK Government.

38. For UK Contractors where the exhibition assets relate to multiple Delivery Teams or for Private Venture defence related material where there is no defined Delivery Team, the Contractor shall request clearance for exhibition from the Directorate of Security and Resilience when it concerns Defence Related Material. See the MOD Exhibition Guidance on the following website for further information: https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets

Export sales/promotion

39. The MOD Form 680 (F680) security procedure enables HMG to control when, how, and if defence related classified material is released by UK Contractors to foreign entities for the purposes of promotion or sales of equipment or services. Before undertaking any targeted promotion or demonstration or entering into any contractual commitments involving the sale or release of defence equipment, information or technology classified UK OFFICIAL-SENSITIVE or above to a foreign entity, a UK Contractor shall obtain F680 approval from the Export Control Joint Unit (ECJU) MOD Team. This includes assets classified UK OFFICIAL-SENSITIVE or above either developed to meet a UK MOD requirement or Private Venture (PV) equipment, as formally advised in a Security Aspects Letter (SAL) issued by the relevant Contracting Authority, or PV Security Grading issued by the MOD Directorate of Security and Resilience. Guidance regarding the F680 procedure issued by ECJU can be found at: https://www.gov.uk/government/publications/ministry-of-defence-form-680-procedure-guidance

40. If a Contractor has received an approval to sub-contract, under an MOD Form 1686 (F1686), for development/production of parts of an equipment, that approval also permits the production of additional quantities for supply to an export customer, when the Contractor has MOD Form 680 approval for supply of the complete equipment, as long as:

a) they are identical, except for component obsolescence, to items produced under the UK programme that the approval to subcontract relates to; and

b) no additional OFFICIAL-SENSITIVE or above material is required to be released to the overseas subcontractor.

Interpretation/Guidance

41. Advice regarding the interpretation of the above requirements should be sought from the Authority.

42. Further requirements, advice and guidance for the protection of UK classified material at the level of UK OFFICIAL and UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at: https://www.gov.uk/government/publications/industry-security-notices-isns

Audit

43. Where considered necessary by the Authority the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractor's processes and facilities by representatives of the Contractor's National/Designated Security Authorities or the Authority to ensure compliance with these requirements.