DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Order Form

This Order Form is for the provision of the Call-Off Deliverables. It is issued under the DIPS Framework Contract with a unique reference number starting with RM6249. The DIPS Framework and this Call-Off Contract are to be for the delivery of Outcomes only. This Framework is not for the request and delivery of resource. If specific resources are needed alternative sourcing methods must be used.

During the Call-Off Contract Period, the Requirement Holder and the Supplier may agree and execute a

1a. Identification

Call-Off Lot	Lot 2 - Dev, Apps, UX, Dev Ops, Sys Design & Support				
Call-Off Reference	RM6249 PS432	Version Number	2.3	Date	05 December 2024
Business Case Reference	Original FBC Number	VMDS FBC6 (BC-00023416), SbD FBC 3 (BC - 00021057), SID RN3 (BC-00019397)			
	Amendment FBC Number	n/a			
Project / equipment for which Services are in support	MODFlow, CAAT, SCPS-AT, SCPS-MI, Vigilant (O&S)	Urgent Capability Requirement (UCR)	n/a		
Call-Off Contract title:	CRP MODCloud Service Wrap				
Call-Off Contract description:	Provision of a service wrap for multiple Cyber Resilience Programme (CRP) products hosted on MODCloud.				
Call-Off Contract Start Date	01 February 2025				
Call-Off Contract Duration	24 Months				
Call-Off Contract Expiry	31 January 2027				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Call-Off Contract Value	Total Contract Value of £2,601,735.12 (ex VAT) made up of: [redacted]

Statement of Work (in the form of the template set out in Appendix 4 to this Framework Schedule 6 (Order Form Template, Statement of Requirements Template)). Upon execution of any Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

The Parties agree that when the Requirement Holder seeks further Deliverables within the initial scope of the original Call-off contract from the Supplier that are not provided for in this Call-Off Contract, the Requirement Holder and Supplier will agree and execute a Call-Off Variation Form.

All capitalised terms in this Order Form shall have the meanings set out in Joint Schedule 1 (Definitions) unless otherwise stated.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Call-Off Optional Extension Period	None

1b. Contact details

Government Directorate / Organisation Title	Ministry of Defence, Defence Digital	Name of Supplier	BAE Systems (Operations) Limited
Name of Requirement Holder's Authorised Representative	[redacted]	Name of Supplier's Authorised Representative	[redacted]
Post title	[redacted]	Post title	[redacted]
Requirement Holder's Address	Building 405 MOD Corsham Wiltshire SN13 9NR	Supplier Address	Victory Point, Lyon Way Frimley Camberley GU16 7EX
Postcode		Postcode	
Telephone	[redacted]	Telephone	[redacted]
Email	[redacted]	Email	[redacted]
Unit Identification Number (UIN)	PA0025	Value Added Tax (VAT) Code	*GB 641 4071 69*
Resource Accounting Code (RAC)	NNB004		
Name of Requirement Holder's Project Lead	[redacted]		
Requirement Holder's Secondary Contact Name	[redacted]	Supplier Secondary Contact Name	[redacted]
Requirement Holder's Secondary Contact Role	[redacted]	Supplier Secondary Contact Role	[redacted]
Requirement Holder's Secondary Contact Email	[redacted]	Supplier Secondary Contact Email	[redacted]

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Date that the Statement of Requirements was issued	11 Sep 2024	**Deadline for Requirement Holder's receipt of Supplier's Call-Off Tender**	*As per tender docs*

1c. Statement of Requirements (SOR) (This section 1c. to be completed in full OR a complete SOR to be attached in Appendix 7 of this document)

Please refer to Appendix 7 of this document

List all Requirement Holder Assets applicable to the Services that shall be issued to the Supplier and returned to the Requirement Holder at termination of the Call-Off Contract
1. MODNET accounts and Laptops 2. Access to MODCloud ICE environments 3. Access to MODCloud D2S environments 4. Access to MOD Corsham 5. Access to RAF Wyton 6. Software Bill of Materials (SBOM) for each application and environment. 7. Architectural components: Certificates, Keys, Secrets, and Credentials for all integrations.
Additional quality requirements & standards (in addition to any quality requirements & standards detailed in the addition to the Call-off Schedules)
From the Call-Off Start Date, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards, including those referred to in Framework Schedule 1 (Specification). The Requirement Holder requires the Supplier to comply with the following additional Standards for this Call-Off Contract: The supplier shall provide services in accordance with the Defence Digital Service Management Framework (SMF) The supplier shall have a working knowledge and understanding of the following: • DD Service Management Framework (SMF) • DD SIAM framework • DD Operational Service Management (OSM) Minimum Dataset • DD Authority Toolset • DD OSM OCM Policy • ITIL v3 2011 • ITIL v4 2019
Project and risk management
The Supplier shall appoint a Supplier's Authorised Representative and the Requirement Holder shall appoint a Requirement Holder's Authorised Representative, who unless otherwise stated in this Order Form shall each also act as Project Manager, for the purposes of this Contract through whom the provision of the Services and the Goods shall be managed day-to-day. Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract. The Supplier shall develop, operate, maintain and amend, as agreed with the Requirement Holder, processes for: (i) the identification and management of risks; (ii) the identification and management of issues; and (iii) monitoring and controlling project plans.

1d. Key Deliverables

Please refer to the full Statement or Requirement in Appendix 7 of this call-off contract

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

2. Call-Off Incorporated Terms

The following documents are incorporated into this Call-Off Contract. Where numbers are missing those schedules are not being used in this Call-Off Contract. If the documents conflict, the following order of precedence applies:

1 This Order Form including the General Conditions in section 2(b) and the Call-Off Special Terms in section 2(c).

2 Joint Schedule 1 (Definitions)

3 Any Statement(s) of Work (in the form of the template set out in Appendix 4 to this Framework Schedule 6 (Order Form Template, Statement of Requirements Template)) executed by the Requirement Holder and the Supplier with a corresponding Call-Off Contract reference

4 [Framework Special Terms]

5 The following Schedules in equal order of precedence:

- Joint Schedules
  - Joint Schedule 2 (Variation Form) ○ Joint Schedule 3 (Insurance Requirements) ○ Joint Schedule 4 (Commercially Sensitive Information) ○ Joint Schedule 5 (Corporate Social Responsibility) ○ Joint Schedule 10 (Rectification Plan) ○ Joint Schedule 11 (Processing Data)
- Call-Off Schedules
  - Call-Off Schedule 3 (Continuous Improvement) ○ Call-Off Schedule 5 (Pricing Details and Expenses Policy) ○ Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) ○ Call-Off Schedule 8 (Business Continuity and Disaster Recovery) ○ Call-Off Schedule 9 (Security) ○ Call-Off Schedule 10 (Exit Management) ○ Call-Off Schedule 13 (Implementation Plan and Testing) ○ Call-Off Schedule 14 (Service Levels) ○ Call-Off Schedule 17 (MOD Terms)
  - Call-Off Schedule 25 (Ethical Walls Agreement) ○ Call-Off Schedule 26 (Cyber)

6 Core Terms (DIPS version)

7 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Requirement Holder (as decided by the Requirement Holder and Commercial) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

2a. Strategy for procurement and evaluation

Further competition	☒	Competitive award criteria to be used for undertaking evaluation of proposal(s)	ıs per tender documents		
Direct award	☐				
		Weighting (Technical)	As per tender docs	Weighting (Price)	As per tender docs

2b. General Conditions

Additional general DEFCON/conditions and DEFFORMs applicable to providing the Deliverables, are to be listed here: *Additional Conditions:* [redacted]	☒

2c. Call-Off Special Terms

The following Special Terms are incorporated into this Call-Off Contract:
See [9. Annex C Service Levels: Amendments to DIPS Call-Off Schedule 14] within Appendix 7 (Statement of Requirement) of this Call-Off Order Form.

2d. Call-Off Charges

Capped Time and Materials (CTM)	☐
Incremental Fixed Price	☐
Time and Materials (T&M)	☐
Firm Price	☒
A combination of two or more of the above Charging methods	☐
T&S is applicable	☒

Reimbursable Expenses

[redacted]

2e. Payment Method

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

BACS payment

Requirement Holder's Invoice Address
Defence Digital
Strategic Services
Building 405, MOD Corsham, Westwells Road,
Corsham,
SN13 9NR

Requirement Holder's Authorised Representative
[redacted]
Project Manager UKStratCom DD-IES-CC-Cyber-PD003
[redacted]
Building 405
MOD Corsham
Wiltshire
SN13 9NR

[redacted] 2f Milestone Payments Schedule

[redacted]

DIPS Order Form / Statement of Requirements Template
(Framework Schedule 6)

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

2g. Maximum Liability

The limitation of the Supplier's liability for this Call-Off Contract is stated in Clause 11.4 of the Core Terms.

2h. Requirement Holder's Environmental Policy

Available online at: Management of environmental protection in defence (JSP 418) - GOV.UK (www.gov.uk)

This version is dated 18th August 2023.

2i. Requirement Holder's Security Policy

Please refer to the Security Aspects Letter included in Appendix 6 of this Order Form.

2j. Progress Reports and meetings

Progress Report Frequency	As per the SoR (Annex C Service Levels)	Progress Meeting Frequency	As per the SoR (Annex C Service Levels)

2k. Quality Assurance Conditions

According to the product or scope of the work to be carried out, the Supplier shall meet the following requirements:

Manage quality in accordance with their approved Quality Management Plan (QMP) and be compliant with the following:

1. The Primary Quality Assurance Standard Requirements:
   - AQAP 2110 Edition D Version 1 NATO Quality Assurance Requirements for Design, Development and Production.
   - CoC shall be provided in accordance with DEFCON 627.
2. Developmental Software
   - NCSC Secure Development and Deployment Guidance
   - NIST SP 800-218 (Secure Software Development Framework v1.1)
3. Concessions
   - Concessions shall be managed in accordance with Def Stan. 05-061
   - Part 1, Issue 7 - Quality Assurance Procedural Requirements - Concessions.
4. Contractor Working Parties
   - Any contractor working parties shall be provided in accordance with Def Stan. 05-061 Part 4, Issue 4 - Quality Assurance Procedural Requirements - Contractor Working Parties. 5. Avoidance of Counterfeit Materiel
   - Processes and controls for the avoidance of counterfeit materiel shall be established and applied in accordance with Def Stan. 05-135, Issue 2 – Avoidance of Counterfeit Materiel.
6. Informative Quality Assurance Standards
   - For guidance on the application and interpretation of AQAPs refer to the appropriate AQAP Standards Related Document (SRD).

Where GQA is performed against this contract it will be in accordance with AQAP 2070 Edition B Version 4.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Allied Quality Assurance Publications (AQAP) 2110 – North Atlantic Treaty Organization (NATO) Quality Assurance Requirements for Design, Development and Production. Certificate of Conformity shall be provided in accordance with DEFCON 627 (*Edn12/10*).			☒
Deliverable Quality Plan requirements:			
DEFCON 602A (*Edn 12/17*) - Quality Assurance with Quality Plan	☐	DEFCON 602B (*Edn 12/06*) - Quality Assurance without Quality Plan	☐
AQAP 2105:2 – NATO Requirements for Deliverable Quality Plans			☐
Software Quality Assurance requirements			
Allied Quality Assurance Publications (AQAP) 2210 – North Atlantic Treaty Organization (NATO) Supplementary Software Quality Assurance Requirements to AQAP-2110 shall apply			☐
Air Environment Quality Assurance requirements			
Defence Standard (DEF STAN) 05-100 – Ministry of Defence Requirements for Certification for Aircraft Flight and Ground Running (Mandatory where flying and/or ground running of issued aircraft is a requirement of the Task)			☐
Relevant MAA Regulatory Publications (See attachment for details)			☐
Additional Quality Requirements (See attachment for details)			☐
Planned maintenance schedule requirement			
Not Applicable			☐

2l. Key Staff

[redacted]

2m. Key Subcontractor(s)

[redacted]

2n. Commercially Sensitive Information

Data in relation to employees/individuals.

2o. Cyber Essentials

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Cyber Essentials Scheme: The Requirement Holder requires the Supplier to have and maintain a Cyber Essentials Plus Certificate for the work undertaken under this Call-Off Contract, in accordance with Call-Off Schedule 26 (Cyber).	☒

2p. Implementation Plan

Implementation Plan requirements in accordance with paragraph 1.1 of Call-Off Schedule 13 (Implementation Plan).	☒

3. Charges

Total Contract Value of £2,601,735.12 (ex VAT) made up of:

[redacted]

4. Additional Insurances

Not Applicable

5. Guarantee

Not Applicable

6. Social Value Commitment

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)

7. Requirement Holder Commercial Officer Authorisation

Order Form approved by (Name in capital letters)	[redacted]	Telephone	[redacted]
Directorate / Division	[redacted]	Email	[redacted]
Organisation Role / Position	[redacted]	Date	05/12/2024
Approver's signature	[redacted]		

8. Acknowledgement by Supplier

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Order Form acknowledged by (Name in capital letters)	[redacted]	Telephone	[redacted]
Supplier Name	[redacted]	Email	[redacted]
Supplier Role / Position	[redacted]	Date	04/12/2024
Approver's signature	[redacted]		

9. Final Administration

On receipt of the Order Form acknowledgement from the Supplier, the Commercial Manager (who placed the order) **must** send an electronic copy of the acknowledged Order Form, together with any applicable Appendix 3 to this Schedule 6, directly to ***DIPS Professional Services Team*** at the following email address: ukstratcomdd-cm-cct-dips-mail@mod.gov.uk

Appendix 1

Addresses and Other Information

Not Used – See Section 1b

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Appendix 2

Appendix 2 – Supplier's Quotation - Charges Summary

Please refer to Section 2f (Milestone Payment Schedule) and Call-Off Schedule 4 (Call-Off Tender)

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Appendix 3 (Statement of Works)

Where applicable, the first Statement(s) of Works shall be inserted into this Appendix 3 as part of the executed Order Form. Thereafter, the Requirement Holder and Supplier may complete and execute Statement of Works (in the form of the template Statement of Work in Appendix 4 to Framework Schedule 6 (Order Form Template, Statement of Work Template).

Not Used - Please refer to Statement of Requirement (Appendix 7)

DIPS Order Form / Statement of Requirements Template
(Framework Schedule 6)

Appendix 4 (Template Statement of Work)

The Requirement Holder and Supplier may propose and execute additional Statement of Work (in the form of the **Statement of Work Template** to be obtained from PS Commercial Officer).

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Appendix 5 Confidentiality Undertaking

[**Requirement Holder guidance**: Appendix 5 is for use where required pursuant to clause 15.3 of the Core Terms]

Employee:

Name of Employer:

MOD Contract/Task No:

Title:

1. I, the above named employee, confirm that I am fully aware that, as part of my duties with my Employer in performing the above-named Contract, I shall receive confidential information of a sensitive nature (which may include particularly commercially sensitive information), whether documentary, electronic, aural or in any other form, belonging to or controlled by the Secretary of State for Defence or third parties. I may also become aware, as a result of my work in connection with the Contract, of other information concerning the business of the Secretary of State for Defence or third parties, which is by its nature confidential.

2. I am aware that I should not use or copy for purposes other than assisting my Employer in carrying out the Contract, or disclose to any person not authorised to receive the same, any information mentioned in paragraph 1 unless my Employer (whether through me or by alternative means) has obtained the consent of the Secretary of State for Defence. I understand that "disclose", in this context, includes informing other employees of my Employer who are not entitled to receive the information.

3. Unless otherwise instructed by my Employer, if I have in the course of my employment received documents, software or other materials from the Secretary of State for Defence or other third party for the purposes of my duties under the above Contract then I shall promptly return them to the Secretary of State for Defence or third party (as the case may be) at the completion of the Contract via a representative of my Employer who is an authorised point of contact under the Contract and (in the case of information referred to under paragraph 1 above) is also authorised under paragraph 2. Alternatively, at the option of the Secretary of State for Defence or the third party concerned, I shall arrange for their proper destruction and notify the above authorised point of contact under the Contract to supply a certificate of destruction to the Secretary of State for Defence. Where my Employer may legitimately retain materials to which this paragraph applies after the end of the

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Contract, I shall notify the authorised representative of my Employer to ensure that they are stored, and access is controlled in accordance with my Employer's rules concerning third party confidential information.

4. I understand that any failure on my part to adhere to my obligations in respect of confidentiality may render me subject to disciplinary measures under the terms of my employment.

Signed:

Date:

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Appendix 6

Security Aspects Letter

Strategic Command
Defence Digital

F1, Building 405
MOD Corsham
Corsham
SN13 9GB

Email: [redacted]
File reference: 20240909 PS432 MCSW Security Aspects Letter v1.1

Insert Date: 13/11/2024

BAE Systems (Operations) Limited
Victory Point, Lyon Way, Frimley
Camberley
GU16 7EX
United Kingdom

PS432: MODCloud Service Wrap

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 ITT that constitute classified material.

Aspects that constitute 'SECRET Matter' for the purpose of the DEFCON 659A Security Clause and OFFICIALSENSITIVE 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
Existence of CRP MODCloud Service Wrap	OFFICIAL
CRP MODCloud Service Wrap Requirements	OFFICIAL-SENSITIVE
CRP MODCloud Service Wrap Tender Documentation	OFFICIAL-SENSITIVE-COMMERCIAL
CRP MODCloud Service Wrap scope, aims and objectives.	OFFICIAL-SENSITIVE
CRP MODCloud Service Wrap delivery & operational risks.	OFFICIAL-SENSITIVE

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Management Information (KPIs etc) concerning the performance of CRP MODCloud Service Wrap	OFFICIAL SENSITIVE
Details of the personnel performing duties within CRP MODCloud Service Desk that support service development, delivery and capability.	OFFICIAL-SENSITIVE-PERSONAL
Any information that could identify an individual as having enough CRP MODCloud Service Desk System privileges, or access rights, to potentially compromise the PADS capability.	OFFICIAL-SENSITIVE-PERSONAL
Personal Identifiers contained in operation of CRP MODCloud Service Desk	OFFICIAL-SENSITIVE-PERSONAL
Existence & Description of VIGILANT	OFFICIAL-SENSITIVE
Existence & Description of CAAT	OFFICIAL-SENSITIVE
Existence & Description of SCPS-MI	OFFICIAL-SENSITIVE
Existence & Description of SCPS-AT	OFFICIAL-SENSITIVE
Existence & Description of MODFlow	OFFICIAL-SENSITIVE
Operation and logical location of VIGILANT	OFFICIAL-SENSITIVE
Operation and logical location of CAAT	OFFICIAL-SENSITIVE
Operation and logical location of SCPSMI	OFFICIAL-SENSITIVE
Operation and logical location of SCPSAT	OFFICIAL-SENSITIVE
Operation and logical location of MODFlow	OFFICIAL-SENSITIVE
Existence & Description of Vigilant (S)	OFFICIAL SENSITIVE
Operation & logical location of Vigilant (S)	SECRET
All data and data products contained within Vigilant (S)	SECRET
Management Information (KPIs etc) concerning the performance of Vigilant (S)	OFFICIAL SENSITIVE
Supplier information contained within SCPS-AT	OFFICIAL-SENSITIVE-COMMERCIAL
Inter-Supplier to Authority Communication.	AS INDIVIDUALLY AND APPROPRIATELY CLASSIFIED

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Your attention is drawn to the provisions of the Official Secrets Act 1989 and the National Security Act 2023. In particular you should take all reasonable steps to make sure that all individuals employed on any work in connection with this ITT have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply should the ITT be unsuccessful.

Will you please confirm that:

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

The definition is fully understood.

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

All employees of the company who will have access to classified material have either signed an OSA/NSA 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/NSA apply to all classified information and assets associated with this ITT.

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.

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

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 Security Officer (PSyO) in accordance with DEFCON 76.

If you require access to information or assets classified SECRET or above at the tender stage you must provide the MOD Contracting Authority with the personal details of the other members of your company to whom you need to disclose information classified SECRET or above in order to complete your Tender. The number of such other individuals should be restricted to the fewest possible, and they should not in any case be allowed access to information or assets classified SECRET or above until they have been granted the appropriate security clearances.

Contact details for the MOD Project Security Officer (PSyO) (responsible for the co-ordination of effective security measures throughout the Project/Programme) are included below:

Yours
faithfully

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Copy via email to:
ISAC-Group (MULTIUSER)
COO-DSR-IIPCSy (MULTIUSER)
UKStratComDD-CyDR-CySAAS-021

Issued 15 April 2024

UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

Purpose

This document provides guidance for Defence Suppliers where classified material provided to or generated by the Defence Supplier is graded UK OFFICIAL or UK OFFICIALSENSITIVE. 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

The term "Authority" for the purposes of this Annex means the UK MOD Contracting Authority.

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

Security Grading

The SENSITIVE marking 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 Defence Supplier, or which is to be developed by it, under this Contract. The Defence Supplier shall mark all UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading. The Defence Supplier is not required to mark documents graded UK OFFICIAL unless they are transmitted overseas or generated by a Defence Supplier based outside the UK in a third-party country.

Security Conditions

The Defence Supplier shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. The Defence Supplier 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.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Where a Defence Supplier is based outside the UK in a third-party country the national rules and regulations of the third-party country take precedence over these conditions only if the third-party country has an extant bilateral security agreement or arrangement with the UK.

The Authority shall state the data retention periods to allow the Defence Supplier to produce a data management policy.

If you are a Defence Supplier located in the UK, your attention is also drawn to the provisions of the Official Secrets Act 1989 and the National Security Act 2023.

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material

The Defence Supplier 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 Defence Supplier shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

Once the Contract has been awarded, where the Defence Supplier is required to store or process UK MOD classified information electronically, they shall comply with the 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.
https://www.dstan.mod.uk/toolset/05/138/000003000.pdf
https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

All UK classified material including documents, media and other assets shall 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 OFFICIALSENSITIVE 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.

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

Except with the consent in writing of the Authority the Defence Supplier 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 9 above, the Defence Supplier shall not make use of any article or part thereof similar to the articles for any other purpose.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

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

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 shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 37.

Access

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

The Defence Supplier shall ensure that all individuals requiring access to UK OFFICIAL and 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 Defence Supplier; 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

UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed internally and externally of Defence Supplier premises. To maintain confidentiality, integrity and availability, distribution shall 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.

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

UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIALSENSITIVE 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

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

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 and CPA scheme are available at:

https://www.ncsc.gov.uk/guidance/tls-external-facing-services
https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

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.

UK OFFICIAL and UK OFFICIAL-SENSITIVE information may be discussed verbally on corporate telephones and other corporate electronic devices with persons located both within the country of the Defence Supplier and overseas. UK OFFICIAL-SENSITIVE information should only be discussed where there is a strong business need to do so.

UK OFFICIAL information may be faxed to recipients located both within the country of the Defence Supplier 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

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.

The Defence Supplier 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.

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

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

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.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Users of the IT System (Administrators) should not conduct 'standard' User functions using their privileged accounts.

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

Up-to-date lists of authorised users.

Positive identification of all users at the start of each processing session

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.

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

Data Transmission. Unless the Authority authorises otherwise, UK OFFICIALSENSITIVE 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 20 above.

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

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.

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.

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

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

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

Defined Business Contingency Plan,

Data backup with local storage,

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

Operating systems, applications and firmware should be supported,

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.

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".*

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.

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).

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.

Portable Electronic Devices

Portable Electronic Devices holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 20 above.

Unencrypted Portable Electronic Device 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.

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

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

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. Portable Electronic 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 Portable Electronic Device 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

The Defence Supplier shall immediately report any loss or otherwise compromise of any Defence Related Classified Material to the Authority. The term Defence Related Classified Material includes 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 Suppliers which are owned by a third party e.g., NATO or another country for which the UK MOD is responsible.

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 Defence Supplier concerned. The UK MOD Defence Industry WARP will also advise the Defence Supplier 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) 3001 583 640
Mail: Defence Industry WARP, DE&S PSyA Office
MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

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

Subcontracts

Where the Defence Supplier wishes to subcontract any elements of a Contract to Subcontractors within its own country or to Subcontractors located in the UK such subcontracts will be notified to the Authority. The Defence Supplier shall ensure that these Security Conditions are incorporated within the subcontract document.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

The prior approval of the Authority shall be obtained should the Defence Supplier wish to subcontract any UK OFFICIAL-SENSITIVE elements of the Contract to a Subcontractor facility located in another (third party) country. The first page of MOD Form 1686 (F1686) is to be used for seeking such approval. The MOD Form 1686 can be found in the "Subcontracting or Collaborating on Classified MOD Programmes ISN" at the link below: https://www.gov.uk/government/publications/industry-security-notices-isns

If the subcontract is approved, the Defence Supplier shall flow down the Security Conditions in line with paragraph 34 above to the Subcontractor. Defence Suppliers located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

Physical Destruction

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 its retention is considered by the Defence Supplier 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

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

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.

UK Defence Suppliers 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-exhibitionclearance-information-sheets

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Publicity Material

Defence Suppliers 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 Defence Supplier'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.

For UK Defence Suppliers where the exhibition assets relate to multiple Delivery Teams or for Private Venture defence related classified material where there is no defined Delivery Team, the Defence Supplier shall request clearance for exhibition from the Directorate of Security and Resilience. See the MOD Exhibition Guidance on the following website for further information:

https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibitionclearance-information-sheets

Export sales/promotion

The MOD Form 680 (F680) security procedure enables MOD to control when, how, and if defence related classified material is released by UK Defence Suppliers 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 Defence Supplier 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 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-procedureguidance

If a Defence Supplier has received an approval to subcontract, 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 Defence Supplier has MOD Form 680 approval for supply of the complete equipment, as long as:

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

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

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

Interpretation/Guidance

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

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

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

Appendix 7 Statement of Requirement (SoR)

1.1. Purpose of Statement of Requirement

This Statement of Requirement (SoR) provides detailed requirements for the Managed Service Provision for the MODFlow platform, Cyber Activity and Assurance Tracker (CAAT), Supplier Cyber Protection System – Automation Tooling (SCPS-AT), Vigilant and Supplier Cyber Protection System – Management Information (SCPS-MI) applications.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

The Cyber Resilience Programme (CRP) was established to fix known vulnerabilities, raise cyber awareness, ensure Defence understands assets to be secured and to build secure foundations for the future including building capabilities secure by design. CRP will deliver outcomes that will protect MOD's critical data, information, systems and platforms to reduce cyber security risk.

Tools developed in the programme are now moving into operational use and the Authority requires a supplier to manage a service wrap. The diagram below shows existing MOD platforms with the addition of the new MODFlow platform. The Cyber Activity and Assurance Tracker (CAAT) and Supplier Cyber Protection System – Automation Tooling (SCPS-AT) will be hosted on MODFlow. Vigilant and the Supplier Cyber Protection System – Management Information (SCPSMI) applications are also within scope of the Managed Service.

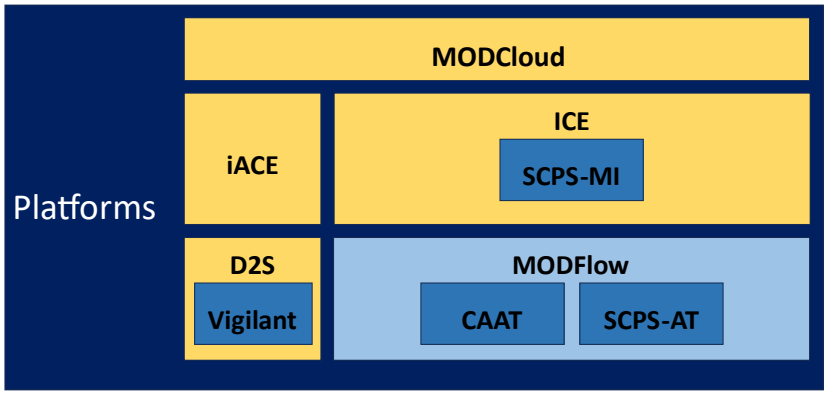

Fig 1. MODFlow platform and Apps indicated in blue requiring a service wrap.

The table below provides more information about each of the products.

MODFLOW	CAAT	SCPS-AT	SCPS-MI	Vigilant	
MODFlow	**Cyber Activity and Assurance Tracker**	**Supplier Cyber Protection Service - Automation Tooling**	**Supplier Cyber Protection Service - Management Information**	**Vigilant O**	**Vigilant S**
Description					
Platform for hosting internal and external applications / web portals. Includes Application compliance documentation/annexes	Self-registration and selfassessment. Assessor assurance. Tailored dashboards and reporting for Delivery Teams and TLBs.	The SCPS-AT is a service to automate Cyber Security Model (CSM) related processes, providing a primary interface for CSM users and enabling interaction between buyers and suppliers in Defence's supply chain.	The SCPS-MI is a service to exploit data collected via the SCPS-AT (and additional sources) to measure, monitor and report on supply chain cyber risk factors, informing risk-based decision making.	Vigilant is the new vulnerability management and alerting system, upgrading the MODCERT process. The system provides rapid dissemination of vulnerability information and analysis of vulnerability return data.	
Technology					

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

<table>
<tr><th>ServiceNow platform hosted in MODCloud ICE (AWS)</th><th>Application using the ServiceNow CSM Module on the MODFlow platform</th><th>ServiceNow CSM Module Hosted on MODFlow platform
Connects to IASME Consortium, Dun & Bradstreet lookup)
Connects to SCPS-MI</th><th>MODCloud ICE (AWS) with multiple data feeds, data processing, data storage using AWS service</th><th colspan="2">Hosted in MODCloud D2S using Java Script and Kubernetes</th></tr>
<tr><td colspan="6">Access</td></tr>
<tr><td></td><td>MOD Core Network (.r.mil.uk) – Full functionality.</td><td>Web based:
The Internet (gov.uk) – Limited functionality.
MOD Core Network (.r.mil.uk) – Full functionality.</td><td>MOD Core Network (.r.mil.uk) – Full functionality.
ODBC connectivity (for PowerBI / other data tools).
Custom website (for upload of files into data pipeline).</td><td colspan="2">Web based service accessed through Boundary Protection Service (BPS).</td></tr>
<tr><td colspan="6">Service Users</td></tr>
<tr><td rowspan="3">See applications</td><td rowspan="3">Delivery Team - 15000
TLB PMO - 150
CySAAS - 80
TLB Assessors - 20</td><td rowspan="3">Buyers - 8000
Suppliers - 20000
Risk and oversight users - 250
MOD CSM Process Admin - 4
Third party developer (possible) - 4</td><td rowspan="3">MOD Cyber Risk Dept Analysts - 50
MOD Cyber Risk Central Analysts - 5
Third party developer (possible) - 5</td><td>MOD Org Admins - 26</td><td></td></tr>
<tr><td colspan="2">Acc Management of service users out of scope</td></tr>
<tr><td>MOD Org Users - 0
System Owners - 3000
System Admin - 10000</td><td>Service Users - 200</td></tr>
</table>

The supplier is required to provide operational service management to the Authority across the MODFlow platform and applications integrating and using Authority owned and managed ITSM Tooling.

The supplier shall provide the Managed Service in the OFFICIAL and SECRET domains with a consistent End User experience across the OFFICIAL and SECRET domains.

The supplier shall provide core service management processes:

- o General Management o Service Management o Technical Management o Information and interoperability

The supplier shall provide variable service management processes: o

- Service enhancement

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Detailed Requirement

The **'Core'** element represents fixed output and activities that must be fulfilled across the duration of the contract. These activities are detailed in the following tables under General Management, Service Management, Technical Management and Information and Interoperability (refer to Annex A for further detail where specified).

The **'Variable**' element represents fixed levels of input for variable output enabling flexibility in how the "Authority" draws on the services from the supplier. The profile of "Days of Effort" usage will be planned and agreed as part of service enhancement scoping and delivery through management of the backlog

Task Number	Activities to be undertaken and completed by the Supplier	Key Deliverables	Required Delivery Date	Acceptance Criteria
1a	Provision of the Core Services of the contract not covered under a specific product (assumption is that this wont increase if more products are added in)	As per Statement of Requirement	Perpetual	As per Acceptance Criteria
1b	Additional work being done in first year, prior to OSM Integration, which will cease	As per Statement of Requirement	As agreed per deliverable	As per Acceptance Criteria
2a	Provision of the Core Service for Vigilant (O & S)	As per Statement of Requirement	Perpetual	As per Acceptance Criteria
2b	Provision of the Variable Service for Vigilant (O & S)	As per Statement of Requirement	As agreed per deliverable	As per Acceptance Criteria
3a	Provision of the Core Service for MODFLOW	As per Statement of Requirement	Perpetual	As per Acceptance Criteria
Task Number	**Activities to be undertaken and completed by the Supplier**	**Key Deliverables**	**Required Delivery Date**	**Acceptance Criteria**
3b	Provision of the Variable Service for MODFLOW	As per Statement of Requirement	As agreed per deliverable	As per Acceptance Criteria
4a	Provision of the Core Service for CAAT	As per Statement of Requirement	Perpetual	As per Acceptance Criteria
4b	Provision of the Variable Service for CAAT	As per Statement of Requirement	As agreed per deliverable	As per Acceptance Criteria

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

5a	Provision of the Core Service for SCPS-AT	As per Statement of Requirement	Perpetual	As per Acceptance Criteria
5b	Provision of the Variable Service for SCPS-AT	As per Statement of Requirement	As agreed per deliverable	As per Acceptance Criteria
6a	Provision of the Core Service for SCPS-MI	As per Statement of Requirement	Perpetual	As per Acceptance Criteria
6b	Provision of the Variable Service for SCPS-MI	As per Statement of Requirement	As agreed per deliverable	As per Acceptance Criteria

1.2. ***General Management***

General Management	**The supplier shall…**	**MODFLOW**	**CAAT**	**SCPS-AT**	**SCPS-MI**	**Vigilant**
Architecture Management	Maintain technical architectures in line with its sustainment needs and any agreed changes/enhancements	**Yes**				
	Review and update technical architectures when changed or at least annually to reflect planned changes to technology roadmaps, security plans	**Yes**				
Continual Improvement	Identify opportunities for improving services	**Yes**				
	Continually improve managed service provision	**Yes**				
Information Security Management ***(Refer to Annex A)***	Provide security management for Secure by Design	**Yes**				
	Provide Security Architecture Roles	**Yes**		**N/A**		
	Provide routine control assessments					
	Provide through life assurance					

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

General Management	The supplier shall…	MODFLOW	CAAT	SCPS-AT	SCPS-MI	Vigilant
	Support Authority assessments					
	Review security risk assessments					
Knowledge Management	Store and maintain the knowledge required to manage and operate the services in relevant Knowledge Management System(s)	**Yes**				
Measurement and Reporting	Implement processes to measure and report on metrics regarding the services under management	**Yes**				
Project Management	Assist the Authority in scoping enhancements/changes to the services and costing options	**Yes**				
Relationship Management	Manage day-to-day technical relationships with service orseganisations and suppliers where dependencies exist (e.g. MODCloud/CES, OSM, JCDU, MODCERT, Def Ind WARP, JDCU).	**Yes**				
Strategy Management	Interact with Authority suppliers, where delegated responsibility (e.g. to place service catalogue orders with MODCloud CES), however will not directly manage such suppliers on the Authority's behalf. The Supplier may bring on board its own suppliers with the agreement of the Authority and will be responsible for managing those suppliers in accordance with appropriate contractual Defence Conditions.	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

	Identify a role to manage the Supply Chain Risk Management requirements, addressing both the Service Providers obligations to MOD and managing to flow down of requirements to any sub-contractor agreements. The designated role shall review and update related documents and agreements annually or as part of a major system change endorsed by the CAB board or following the recommendations of an incident	**Yes**	**No**

1.3. ***Service Management***

Service Management	**The supplier shall…**	**MODFLOW**	**CAAT**	**SCPS-AT**	**SCPS-MI**	**Vigilant**
Availability Management/Service Continuity Management	Ensure that the services meet the availability requirements, refer to Annex A for full details.	**Yes**				
	Develop a business continuity plan (refer to Annex A)	**Yes**				
	Coordinate contingency plan development (refer to Annex A)	**Yes**				
	Manage the Through Life Management Plan (refer to Annex A)	**Yes**				
	Review the System Security Risk Management Frame Work Documents annually	**Yes**				
Planned Outages	Ensure planned outages are appropriately scheduled, communicated and overseen.	**Yes**				
Capacity and Performance Management	Monitor capacity and performance, tuning and configuring the services and infrastructure to meet the performance requirements within set authorisations.	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Change Enablement	Manage the delivery of all allocated service changes, providing governance to ensure that all changes follow the correct scheduling, approvals and testing activities in accordance with the Authority's security and service management policies, processes and guidance.	**Yes**	
	Identify and resource a role to manage the Change Control Governance Document	**Yes**	**No**
	Operate the Change Board review changes	**Yes**	
Incident Management	Provide a process for managing incidents for all managed services. Refer to Annex A for details.	**Yes**	
	Develop system level Incident Response Plan (Refer to Annex A)	**Yes**	
	Test effectiveness of the incident response capability for the system every 6 months	**Yes**	

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Service Management	The supplier shall…	MODFLOW	CAAT	SCPS-AT	SCPS-MI	Vigilant
IT Asset Management	Have an IT asset management process and maintain asset information for all assets within the managed services	**Yes**				**N/A**
Monitoring and Event Management	Systemically monitor the services and the service components for relevant events and report the events as required (refer to Annex A)	**Yes**				
Problem Management	Maintain a database of known/common problems and errors, identifying the root causes/errors and identifying the best approaches to mitigate the problems. Percentage of Problem Records exceeding a 3-month threshold of 50% Percentage of Problem Records exceeding a 4-month threshold of 30% Percentage of Problem Records exceeding a 5-month threshold of 10%	**Yes**				
Release Management	Working with the Authority, plan for and coordinate the release of the services and any associated upgrades/updates of services Schedule, co-ordinate the testing and verification and manage the deployment of Releases while minimising potential security and service issues.	**Yes**				
Service Catalogue Management	Develop a service catalogue which sets out the commoditised services and sub-services available.	**Yes**				
Service Configuration Management	Ensure the configuration of the services and service components remain documented and accurate (90% accuracy)	**Yes**				
	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using the Configuration Management Policy (90% accuracy)	**Yes**	**No**			

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Service Management		MODFLOW	CAAT	SCPS-AT	SCPS-MI	Vigilant
	The supplier shall… Identify, document, and seek approval for any deviations from established configuration settings for architecture elements based on MOD cloud policy and procedures; monitor and control changes to the configuration settings in accordance with the configuration control and change management processes (90% accuracy)	**Yes**	**No**			
	Identify and resource a role to manage the MODFlow Configuration Management Document.	**Yes**	**No**			
Service Desk	Operate a Service Desk at the OFFICIAL and SECRET tiers, which manages all Incidents and Requests. The service desk shall be hosted on Authority systems.	**Yes**				
Service Request Management	Design and implement processes for managing service requests which is effective and intuitive for the end-users. Refer to Annex A for details.	**Yes**				
	Initiate and manage new User accounts administration for all systems.	**Yes**				

1.4. ***Technical Management***

Technical Management	The supplier shall…	MODFLOW	CAAT	SCPS-AT	SCPS-MI	Vigilant

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Deployment Management	Be responsible for moving service components between environments (e.g. dev, test, live preprod / staging, live production) within agreed parameters and authorisations.	**Yes**	
Infrastructure and Platform Management	Monitor and manage the services' use of platforms and infrastructure.	**Yes**	
Software Development and Management	Address the reliability, maintenance and compliance of developed software within the services	**Yes**	
Patch Management	Update software to the latest versions as recommended by the manufacturers or MODCERT	**Yes**	
AV Update Management	Be responsible for updating antivirus and antimalware to the latest versions as recommended by the manufacturers or MODCERT (refer to Annex A)	**Yes**	**No**
Certificate and PKI Management	Be responsible for maintaining certificates used by the services which are service maintained	**Yes**	
License Management	Be responsible for ensuring software continues to be licensed for use and informing the Authority if there is any license issues well in advance	**Yes**	**No**
IT Health Checks	Support scoping of the ITHC, prepare for ITHC, provide access to ITHC suppliers, support ITHC suppliers during testing, respond to ITHC findings, propose remediations in a Remedial Action Plan for the Authority and remediate findings within its area of responsibility as agreed. The Contractor will contract for ITHC as per the individual service requirements.	**Yes**	

1.5. ***Information and Interoperability***

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Information and Interoperability	The supplier shall…	MODFLOW	CAAT	SCPS-AT	SCPS-MI	Vigilant
Service Management solution	Assume responsibility for existing Service Management operations and agree the full Service Management solution with the Authority.	**Yes**				
Service management solution security	Ensure the full Service Management solution meets MOD policy for security.	**Yes**				
Service Management solution implementation	Implement the full Service Management solution within 6 months from contract award.	**Yes**				
Service Management solution access	Ensure the full Service Management solution is accessible to the Authority	**Yes**				
Service management data	Ensure the data within the Service Management solution is accessible to the Authority	**Yes**				
Service Management interoperability	Ensure the Service Management functions can interoperate with the Authority's Operational Service Management (OSM) processes and tooling.	**Yes**				
Security Interoperability	Ensure the security functions are designed to integrate with relevant Security Operations Centres (SOC) within Defence.	**Yes**				
	Provide data from Security Information and Event Management tooling to SOCs where required.	**Yes**				

1.6. ***Service Enhancement***

Service Enhancement	The supplier shall…	MODFLOW	CAAT	SCPS-AT	SCPS-MI	Vigilant

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Enhancement scoping	Work with each Product/Service owner and appropriate suppliers/stakeholders to scope potential enhancements.	**Yes**
	Agree contractual variable Days of Effort utilisation with Product/Service owners for approved enhancements	**Yes**
Enhancement backlog	Maintain a backlog of enhancements and work with the Product/Service owner and appropriate suppliers/stakeholders to prioritise.	**Yes**
Service Validation and Testing	Undertake validation and testing for changes to existing services and for any new services introduced into the MSP	**Yes**

2. Outputs

Outputs	**The supplier shall…**	**MODFLOW**	**CAAT**	**SCPS-AT**	**SCPS-MI**	**Vigilant**
Operate Interim ITSM Tooling	The contractor will successfully take over and operate the interim service management tooling (ITSM) solution within 30 days	**Yes**				
	Ensure seamless continuity with no more that 1% downtime during the transition period	**Yes**				
	Achieve operational effectiveness of the ITSM solution evidenced by meeting or exceeding all established SLAs within 90 days of takeover	**Yes**				
ITSM Data Accessibility	Ensure that data within the service management tooling is fully accessible to the authority	**Yes**				
OSM Interoperability	Ensure the service management function operates with the authority's operational service management (OSM) processes, achieving full integration within 12 months of contract award.	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

	Ensure the service management tooling is interoperable with the authority operational service management tools within 12 months of contract award	**Yes**
Continual Improvements	The contractor shall identify opportunities for improvement to the services managed, providing a minimum of 2 actionable improvements proposals per quarter	**Yes**
Information Exchange Agreements	Review and update any information exchange agreements with external system annually.	**Yes**
Measurement and Reporting	Provide monthly reports and statistics that include but are not limited to: User satisfaction, Ticket resolution time, Service report compliance, Change requests, Admin access changes, Patches applied, Anti-virus changes, Licence usage, and Certificate changes.	**Yes**

Outputs	**The supplier shall…**	**MODFLOW**	**CAAT**	**SCPS-AT**	**SCPS-MI**	**Vigilant**
Change Enablement	Manage the change control governance and document within 30 days of contract commencement, measured by achieving 100% compliance with change control procedures as verified by quarterly audits, ensuring that all changes are documented, approved, and tracked according to the governance document.	**Yes**				
	Variable Costed tasks 2b, 3b, 4b, 5b, and 6b are for the flexible work to deliver technical change. This is assumed to require up to 1.0 FTE split over the five products, made from several competencies.	**Yes**				
	Ensure that all changes are communicated to stakeholders with a minimum of 48 hours' notice	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Service Catalogue Management	Document the service catalogue within 90 days of contract award.	**Yes**
Service Configuration Management	Conduct bi-annual reviews of configuration documentation with any discrepancies resolved within 10 business days.	**Yes**
Deployment Management	Be responsible for moving service components between environments and conducting the required testing within 10 working days of request.	**Yes**
Transition Plan	Draft a Transition Plan for review by the Authority and a jointly approved Transition Plan will be issued by the Authority prior to entering into the Contract.	**Yes**
Exit Plan	Provide an Exit Plan that shall include plans, programmes and explanatory documents for all services and activities covered by the Contract to be agreed with the Authority.	**Yes**
Management Plan Standards	The final Quality Plan shall be delivered to the quality Assurance Representative within 3 months of contract award. (A draft quality plan is required within the Tender submission)	**Yes**

3. Acceptance Criteria

Acceptance Criteria	**The supplier shall…**	**MODFLOW**	**CAAT**	**SCPS-AT**	**SCPS-MI**	**Vigilant**
Implement Service Management Tooling	Implement an ITSM solution within 90 days of Contract Award	**Yes**				
	Ensure the ITSM solution complies with Secure by Design Policy (JSP440 Leaflet 5c)	**Yes**				
ITSM Data Accessibility	Provide access to authorised users within 3 seconds for 95% of login attempts	**Yes**				
	Maintain compliance with all relevant accessibility standards as verified by bi-annual accessibility audits.	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Through Life Assurance	Shall maintain compliance with Secure by Design Policy (JSP440 Leaflet 5c) for all applications and platforms, including control assessment reports and SRO engagement.	**Yes**
Network Joining Rules	Shall maintain compliance with JSP604 for all applications and platforms	**Yes**
Support Authority Assessments	Support any audit of security controls, ensuring 100% availability and cooperation during audit activities.	**Yes**
Availability Management	Perform root cause analysis on any unplanned downtime exceeding 1% per month within 24 hours.	**Yes**
Planned Outages	Schedule all planned outages at least 7 days in advance and notice must be issued to affected stakeholders at least 48 hours in advance via email.	**Yes**
Capacity and Performance Management	Monitor capacity and initiate plans to increase capacity 90 days prior to capacity being breached.	**Yes**
Security Incident and Event Management	On direction of security officer to limit service availability within 1 working hour during service desk operating hours.	**Yes**
Problem Management	The authority shall be notified within 1 working day of a problem being identified	**Yes**

Acceptance Criteria		**MODFLOW**	**CAAT**	**SCPS-AT**	**SCPS-MI**	**Vigilant**
Service Configuration Management	**The supplier shall…** The contractor shall review and update the policy and processes annually or as part of a major system change endorsed by the MODFlow CAB board or following the recommendations of an incident investigation.	**Yes**				
Service Desk	Monday to Friday 09:00 to 17:00, excluding public holidays & weekends	**Yes**				
Service Request Management	Initiate and manage User account administration for all systems.	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Management Plan Standards	The Contractor shall manage quality in accordance with their approved QMP and be compliant with the following: I. The Primary Quality Assurance Standard Requirements: • AQAP 2110 Edition D Version 1 NATO Quality Assurance Requirements for Design, Development and Production. • CoC shall be provided in accordance with DEFCON 627. II. Developmental Software • NCSC Secure Development and Deployment Guidance • NIST SP 800-218 (Secure Software Development Framework v1.1) III. Concessions • Concessions shall be managed in accordance with Def Stan. 05-061 • Part 1, Issue 7 - Quality Assurance Procedural Requirements - Concessions. IV. Contractor Working Parties • Any contractor working parties shall be provided in accordance with Def Stan. 05-061 Part 4, Issue 4 - Quality Assurance Procedural Requirements - Contractor Working Parties. V. Avoidance of Counterfeit Materiel • Processes and controls for the avoidance of counterfeit materiel shall be established and applied in accordance with Def Stan. 05-135,	**Yes**
Acceptance Criteria	**The supplier shall…** Issue 2 – Avoidance of Counterfeit Materiel. VI. Informative Quality Assurance Standards • For guidance on the application and interpretation of AQAPs refer to the appropriate AQAP Standards Related Document (SRD). Where GQA is performed against this contract it will be in accordance with AQAP 2070 Edition B Version 4.	**MODFLOW** | **CAAT** | **SCPS-AT** | **SCPS-MI** | **Vigilant**

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

4. Key Performance Indicators (KPIs)

KPIs	The supplier shall…	MODFLOW	CAAT	SCPS-AT	SCPS-MI	Vigilant
Deliver Service Management	Ensure that service management functions for in-scope services are delivered with a minimum of 99% up time	**Yes**				
	Achieve a customer satisfaction rating of 4 or higher on a 5-point scale in quarterly surveys	**Yes**				
Deliver Service Enhancement	Resolving 90% of all service-related issues within the agreed service level (SLA) timeframe.	**Yes**				
	Ensure that service enhancement functions for in-scope services result in a 25% improvement in service efficiency as measured by KPIs within 6 months	**Yes**				
Implement Service Management Tooling	Maintain a feedback score of 4 or higher on a 5 point scale for the enhancements provided.	**Yes**				
ITSM Data Accessibility	Implement an ITSM that provides complete data access within 2 seconds for 90% of queries	**Yes**				
	Ensure data accuracy and integrity with an error rate of less than 0.5% as verified by quarterly audits.	**Yes**				
OSM Interoperability	Achieve 100% compatibility with all authority operational service management tools as verified by interoperability testing, enabling seamless data exchange with a success rate of 99% for automated transactions, and ensuring that any integration issues are resolved within 72 hours.	**Yes**				
	Perform interoperability testing with all authority operational service management tools with a success rate of 99% for automated transactions	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

	Ensure that any integration issues with all authority operations service management tools are resolved within 72 hours.	**Yes**

KPIs	**The supplier shall…**	**MODFLOW**	**CAAT**	**SCPS-AT**	**SCPS-MI**	**Vigilant**
	Provide the services in accordance with Defence Service Management Framework (SMF), ensuring 100% compliance with the Defence SMF standards and processes as verified by quarterly audits.	**Yes**				
SOC Integrations	Integrate with Defence relevant Security Operations Centres (SOCs) achieving full integration within 6 months with 100% of necessary data being transmitted and received.	**Yes**				
	Maintaining a 99% success rate of data transfer to SOCs as monitored by monthly performance assessments.	**Yes**				
Standards - SIAM Framework	Support the managed services in accordance with Defence SIAM framework, ensuring 100% compliance with SIAM processes and policies as verified by quarterly compliance audits	**Yes**				
Architectural Management	Maintain the technical architecture for each managed service in line with its sustainability needs and any agreed changes, ensuring that 100% of architectural updates align with established sustainability goals as confirmed by bi-annual sustainability audits and implementing agreed changes with 30 days of approval	**Yes**				
	Review and update the technical architecture at least annually to reflect planned changes to technology roadmaps and security plans, ensuring that 100% of updates incorporate both planned and actual changes in the cloud environment and security architecture	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

	Verify architectural changes by an annual audit, with all updates completed within 60 days of the review	**Yes**
	Ensure that any critical security updates are implemented within 30 days of identification	**Yes**
Continual Improvements	Implement 75% of accepted proposals with 120 days and achieve the anticipated benefits as validated by post implementation reviews.	**Yes**

KPIs	**The supplier shall…**	**MODFLOW**	**CAAT**	**SCPS-AT**	**SCPS-MI**	**Vigilant**
	Demonstrate a 5% annual improvement in system uptime and . Additionally, user satisfaction should increase by at least 0.1 points on a 5 point scale each year, as measured by quarterly user satisfaction surveys.	**Yes**				
	Demonstrate a reduction in incident response times by 5% annually	**Yes**				
	Demonstrate an increase by at least 0.1 points on a 5 point scale each year.	**Yes**				
Security Architecture	Maintain a processing accuracy rate of 95% for Security Architecture document(s) as verified by monthly audits.	**Yes**				
	Ensure that security architecture documents are reviewed and updated within agreed timeframes, with a compliance rate of 90% or higher.	**Yes**				
Support Authority Assessments	Address and resolve any identified non compliance issues found during a security audit within 30 days.	**Yes**				
	Providing all requested documentation and access within 5 business days of the request during security audits.	**Yes**				
Through Life Assurance	100% of quarterly assessments are reviewed and disseminated within 10 working days of completion.	**Yes**				

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

	Ensure identified risks are accurately document and communicated with a minimum of 90% accuracy as validated by internal audits.	**Yes**
	Update the technical risk assessment within 40 days of any significant changes, and ensuring the annual update is completed within the designated timeframe.	**Yes**
	Update information exchange agreements within 40 days of the review date and communicate agreed changes with external parties within 90 days of identification.	**Yes**
Change Enablement	Implement at least 90% of changes without incidents or rollbacks additionally and	**Yes**
KPIs	**The supplier shall…**	**MODFLOW** / **CAAT** / **SCPS-AT** / **SCPS-MI** / **Vigilant**
	Ensure that all changes are communicated to stakeholders with a minimum of 48 hours notice	**Yes**
	Conduct post-implementation reviews for 100% of changes to assess their impact and identify areas for improvident.	**Yes**
Problem Management	Ensure 50% of Problem Records do not exceed a 3-month threshold, ensure 30% of Problem Records do not exceed a 4-month threshold, and ensure 10% of Problem Records do not exceed a 5-month threshold.	**Yes**
Service Configuration Management	Achieve 100% documentation of all configurations and changes within 72 hours of implementation.	**Yes**
Service Configuration Management	Maintain all configuration records with at least 90% accuracy as verified by quarterly audits.	**Yes**
Service Request Management	Changes to admin/super user accounts will be administered within 2 business days of request receipt.	**Yes**

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Certificate and PKI Management	New certificate applications will be processed within 2 working days.	**Yes**

5. Security Clearance Requirements

All supplier staff deployed on the contract must hold current and valid Security Clearance at SC (as a minimum) or above.

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

6. Annex A General Management – Additional information

Information Security		Product
Security Architecture Roles Filled	The Service Provider shall identify and resource roles to manage the MODFlow Security Architecture Document	MODFLOW
Routine control assessment	The Service Provider shall assess the controls in the system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;	
Through life assurance	The Service Provider shall undertake ongoing through life assurance in accordance with MOD secure by design policy	
Support Authority assessments	The Service Provider shall support any authority initiated independent audit of security controls (CySASS assessor or other 2nd line audit)	
Review security risk assessments	The Service Provider shall review risk assessment results (risk register) Quarterly; Disseminate risk assessment results to the Security Working Group and Security Lead; and update the Technical Risk Assessment annually or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system. The designated role shall review and update the policy and processes annually or as part of a major system change endorsed by the MODFlow CAB or following the recommendations of an incident investigation. The Service Provider shall respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance. The Service Provider shall Prohibit the use of end user systems that are not assured for use with OFFICIAL SENSITIVE data.	

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Information Security		Product
	The service Provider shall permit authorized individuals to use an external system to access the system or to process, store, or transmit organizationcontrolled information only after: (a) Verification of the implementation of controls on the external system as specified in MODs security and privacy policies and security and privacy plans; or (b) Retention of MOD approved system connection or processing agreements with the organizational entity hosting the external system. The Service Provider shall review and update any information exchange agreements with external systems annually. The Service Provider shall identify and resource a role to manage the Security Assurance Plan.	

7. Service Management – Additional information

Availability Management	Product

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

a. The Service Provider shall develop a business continuity plan for the system that: 1. Identifies essential mission and business functions and associated business continuity requirements; 2. Considers recovery objectives, restoration priorities, and metrics; 3. Addresses business continuity roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of business continuity information; and 7. Is reviewed and approved by the MOD Authority; b. Distribute copies of the contingency plan to contingency personnel (identified by name and/or by role); c. Coordinate business continuity planning activities with incident handling activities; d. Review the business continuity plan for the system annually; e. Update the business continuity plan annually to address changes to the organization, system, or environment of operation or problems encountered during business continuity plan implementation, execution, or testing; f. Communicate business continuity plan changes to [contingency personnel (identified by name and/or by role); g. Incorporate lessons learned from business continuity plan testing, training, or actual business continuity activities into business continuity testing and training; and h. Protect the business continuity plan from unauthorized disclosure and modification.	MODFLOW
The Service Provider shall coordinate contingency plan development with MOD elements responsible for related plans and test the contingency plan for the system every 6 months to determine the effectiveness of the plan and the readiness to execute the plan: b. Review the contingency plan test results; and c. Initiate corrective actions, if needed. The Service Provider shall plan for the resumption of mission and business functions within no more than one week of business continuity plan activation and with no more than one day of lost data.	MODFLOW

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Availability Management	Product
The Service Provider shall provide business continuity training to system users consistent with assigned roles and responsibilities: 1. Within 1 Month of assuming a contingency role or responsibility; 2. When required by system changes; and 3. Annually thereafter; and b. Review and update business continuity training content annually and following a major change or incident. The Service Provider shall identify and resource roles to manage the Through Life Management Plan which includes: • risk assessment policy and procedures; • system maintenance policies	
The designated role shall review and update the policy and processes annually or as part of a major system change endorsed by the CAB board or following the recommendations of an incident investigation. The Service Provider shall review the System Security Risk Management Frame Work Documents annually, these include; • NIST Risk Management Framework Prepare Step Artefacts • Technical Risk Assessment • Risk Register • Security Control Tailoring Document • Data Privacy Impact Assessment Update the documents to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and Protect the plans from unauthorized disclosure and modification.	MODFLOW

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Incident Management	Product
a. Develop a system level incident response plan that: • Describes the structure and organization of the incident response capability; • Provides a high-level approach for how the system response fits into the overall MOD incident response; • Defines reportable incidents; • Provides metrics for measuring the incident response • Addresses the sharing of incident information; • Is reviewed and approved by the MOD Authority annually; and • Explicitly designates responsibility for incident response to defined personnel, or roles. b. Distribute copies of the incident response plan to incident response personnel (identified by name and/or by role); c. Update the incident response plan annually to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to incident response personnel (identified by name and/or by role); and e. Protect the incident response plan from unauthorized disclosure and modification. The Service Provider shall test the effectiveness of the incident response capability for the system [every 6 months], coordinating testing with MOD elements responsible for related plans. The Service Provider shall track, document and report incidents in accordance with the incident response plan.	MODFLOW

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

Monitoring and Event Management	Product
The Service Provider shall: Manage system event logging tools, Engage with the assigned authority security operating centre, Configure audit record generation to contain information requested by the authority SOC In the event of an audit logging process failure, Contact authority SOC Support the authority SOC with on-demand audit record access, system analysis, and after-the-fact investigations of incidents Review and update the event types selected for logging annually or as directed by the authority SOC. The Service Provider shall, , a. Monitor and scan for vulnerabilities in the system and hosted applications monthly as part of the patching cycle and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques available within Service Now and AWS. c. Analyse vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities in accordance with an assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with the assigned MOD SOC, d. Remediate legitimate vulnerabilities in accordance with an assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with the assigned MOD SOC,	MODFLOW

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

The Service provider shall update the system vulnerabilities to be scanned prior to a new scan or when new urgent vulnerabilities are identified and reported.	
Monitoring and Event Management	**Product**

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

The Service Provider shall support the authority SOC to monitor the system to detect attacks and indicators of potential attacks in accordance with the following monitoring objectives: Security Architecture Document - Monitoring Policy; The service provider shall manage internal monitoring capabilities within AWS and Service Now and adjust the level of system monitoring activity when there is a change in risk to operations and assets; g. The service provide3r shall provide system monitoring to the MOD SOC at an agreed frequency and on demand. The Service Provider shall alert the Security Admin and MOD SOC when agreed indications of compromise or potential compromise occur. The Service Provider shall receive system security alerts, advisories, and directives from MODCERT, MODCloud and Service Now on an ongoing basis and implement security directives in accordance with established time frames, or notify the Security Lead of the degree of noncompliance. The Service Provider shall generate internal security alerts, advisories, and directives as deemed necessary and disseminate them to impacted MODFlow Stakeholders]; and The Support Provider shall employ the integrity verification tools available in AWS and Service Now to detect unauthorized changes to the software, firmware, System Architecture or System configuration]; When unauthorized changes are detected the support provider shall log the event and alert the system security admin and MOD SOC.	

Service Request Management	**Product**

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

The Service Provider shall manage privileged user accounts, including: Authorising access to the system based on: Valid access authorisation; Intended system Role; Monitor accounts for compliance with account management requirements Review every Month the privileges assigned to [privileged users] to validate the need for such privileges, Review every 3 Months the activity status of standard Users. Reassign or remove privileges, if necessary, Work with TLBs to align account management processes with personnel termination and transfer processes. Disabling accounts of individuals within 8 working hours of MOD notification of a significant risk. The Service Provider shall be required to control access to roles with logging management permissions, to protect audit information from unauthorized access, modification, and deletion. The Service Provider shall establish and provide to individuals requiring privileged access to the system, the rules that describe their responsibilities and expected behaviour for information and system usage, security, and privacy (SyOPS); Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the SyOPS, before authorising access to information and the system; Review and update the SyOPS annually; and Require individuals who have acknowledged a previous version of the SyOPS to read and re-acknowledge when the rules are revised or updated.	CAAT

8. Annex B Technical Management – Additional information

AV Update Management	Product

DIPS Order Form / Statement of Requirements Template (Framework Schedule 6)

The Service Provider shall a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install routine security-relevant software updates within [one month] of the release of the updates; d. Install urgent security related software updates ,as identified by MODCERT, within the timescales agreed with the CAB, and e. Align flaw remediation with the configuration management process. The Service Provider shall update the system software asset register as part of system patches and updates.	MODFLOW

9. Annex C Service Levels

(Amendments to DIPS Call-Off Schedule 14)

1 Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	Definition
Critical Service Level Failure	has the meaning given to it in the Order Form;
KPI Failure	means a failure to meet a KPI;
Service Level Failure	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
Service Level Performance Measure	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
Service Level Threshold	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2 How the Service Levels work

2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A (Service Levels and KPIs) of this Schedule.

2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

2.4.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date; and

2.4.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards.

3 Critical Service Level Failure

On the occurrence of a Critical Service Level Failure the Buyer shall be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period **("Compensation for Critical Service Level Failure"**), provided that the operation of

this Paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

4 How the KPIs work

4.1 The Supplier shall at all times provide the Deliverables to meet or exceed the KPIs.

4.2 The Supplier acknowledges that failures to meet the KPIs shall entitle the Buyer to the rights set out in Part A (Service Levels and KPIs) of this Schedule.

Part A: Service Levels and KPIs

1 Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure or KPI; or

1.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent the failure to meet a KPI, a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process if there is a Critical Service Level Failure or the circumstances set out in paragraph 2.1 of this Schedule or paragraph 5.4 of Framework Schedule 4 (Framework management) apply; and/or

1.2.3 if a Critical Service Level Failure has occurred, exercise its right to compensation for Critical Service Level Failure (including the right to terminate for material Default).

2 Buyer redress for failure to provide Services at or above Service Levels

2.1 The Buyer may ask for a Rectification Plan if [any][insert number] of Service Level Failure[s] [has][have] occurred.

2.2 This Rectification Plan must clearly detail the improvements and associated timeframes within which the Supplier shall meet and achieve the Service Levels. The Rectification Plan must be provided in accordance with Clause 10.3 of the Core Terms and any failure to correct a Service Level Failure in line with an accepted Rectification Plan, or failure to provide a Rectification Plan within 10 days of the request may result in the Buyer exercising its right to terminate the Contract in accordance with Clause 10.4 of the Core Terms.

3 Buyer redress for failure to provide Services at or above KPIs

3.1 The Buyer may exercise the remedies set out in paragraph 5.4 of Framework Schedule 4 (Framework management) in the event of a KPI Failure.

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)

Annex A to Part A: Services Levels Table

Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	**Buyer redress for Failure to provide Services at or above Service Level**
Accurate and timely billing of Buyer	Accuracy /Timelines	at least 98%, Monday to Friday 09:00 to 17:00, excluding public holidays & weekends	[98%]	Subject to Call-Off Schedule 10 (Rectification Plan) and right to withhold payment until rectified
Access to Supplier support	Availability	at least 98%, Monday to Friday 09:00 to 17:00, excluding public holidays & weekends	[98%]	Subject to Call-Off Schedule 10 (Rectification Plan) and Critical Service Level Failure
Key Service Performance Indicators	As per "KPI" section in "20240708CRP MSP SoR detailed requirement s v1-OSC"	As per specific KPI, including accepted Proof of Innocence where incidents lay outside of the service scope	As per specific KPI	Subject to Call-Off Schedule 10 (Rectification Plan) and Critical Service Level Failure

The applicable KPIs are set out in Framework Schedule 4.

Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)
Part B: Performance Monitoring

1 Performance Monitoring and Performance Review

1.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels and KPIs will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

1.2 The Supplier shall provide the Buyer with performance monitoring reports **("Performance Monitoring Reports"**) in accordance with the process and timescales agreed pursuant to Paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

1.2.1 for each Service Level and KPI, the actual performance achieved over the Service Level for the relevant Service Period;

1.2.2 a summary of all failures to achieve Service Levels and KPIs that occurred during that Service Period;

1.2.3 details of any Critical Service Level Failures;

1.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence; and

1.2.5 such other details as the Buyer may reasonably require from time to time.

1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports **("Performance Review Meetings"**) on a Monthly basis, or as otherwise agreed between the Parties. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

1.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location, format and time (within normal business hours) as the Buyer shall reasonably require;

1.3.2 be attended by the Supplier's Authorised Representative and the Buyer's Authorised Representative; and

1.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Authorised Representative and any other recipients agreed at the relevant meeting.

1.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Authorised Representative and the Buyer's Authorised Representative at each meeting.

1.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier for any specified Service Period.

2 Satisfaction Surveys

2.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the

Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.