

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.

1a. Identification

Call-Off Lot	Lot 1 - Solution, Enterprise and Technical Architecture, Data, Innovation, Technical Assurance and Knowledge & Information Management				
Call-Off Reference	RM6249/DIPS (1) 045	Version Number	1.0	Date	25/06/2024
Business Case Reference	Original FBC Number	20240424_CC_MOD Enablement Programme Continuation			
	Amendment FBC Number	N/A			
Project / equipment for which Services are in support	Secret Cloud	Urgent Capability Requirement (UCR)		N/A	
Call-Off Contract title:	PS438 MOD Cloud Enablement Programme Continuation				
Call-Off Contract description:	The Community Cloud project seeks to deliver a hyperscale-like cloud service, enhancing ways of working and increasing interoperability with partners, other government departments requiring both continuity of resource and significant digital expertise to accelerate the execution of an upcoming Invitation to Negotiate process. This contract will be placed in support of the ITN process, approvals campaign, and the supporting evidence required to progress through these complex activities.				

1b. Contact details

Government Directorate / Organisation Title	Core Enabling Services	Name of Supplier	<i>KPMG LLP</i>
Name of Requirement Holder's Authorised Representative		Name of Supplier's Authorised Representative	

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

Post title		Post title	
Requirement Holder's Address	MOD Corsham, Mustang Bldg, Wiltshire, SN13 9NR	Supplier Address	66 Queen Square Bristol UK, BS1 4BE
Postcode		Postcode	
Telephone		Telephone	
Email		Email	
Unit Identification Number (UIN)	D2428A	Value Added Tax (VAT) Code	
Resource Accounting Code (RAC)	NPB004		
Name of Requirement Holder's Project Lead			
Requirement Holder's Secondary Contact Name		Supplier Secondary Contact Name	
Requirement Holder's Secondary Contact Role		Supplier Secondary Contact Role	
Requirement Holder's Secondary Contact Email		Supplier Secondary Contact Email	

Date that the Statement of Requirements was issued

27/06/2024

Deadline for Requirement Holder's receipt of Supplier's Call-Off Tender

N/A

Background/justification for Call-Off Contract
This is short-term DIPS direct award to continue to deliver Secret Community Cloud until 31 December 2024. Any further requirement will be competed via DIPS, pending two sets of internal approvals which will define what the ongoing requirements will be from 2025.
Description of Services to be provided under the Call-Off Contract
See Appendix 3 - SOW
Activities required to be undertaken under the Call-Off Contract
See Appendix 3 - SOW
Outputs to be provided under the Call-Off Contract

See Appendix 3 - SOW

Acceptance/rejection criteria / provisions

See Appendix 3 - SOW

1c. Statement of Requirements (SOR) (This section 1c. to be completed in full OR a complete SOR to be attached in Appendix 3 of this document)

Unique Order Number (defined by delivery team)	N/A		
SOR version issue number	2.0	SOR dated	27/06/2024
SOR title	20240627-SOR_MCEP_CY24_Support-V2		

Material KPIs / Critical Service Level Failure

N/A

The following Material KPIs shall apply to this Call-Off Contract in accordance with Framework Schedule 4 (Framework Management):

Material KPIs

N/A

The following shall constitute a Critical Service Level Failure for the purposes of this Call-Off Contract in accordance with Call-Off Schedule 14 (Service Levels):

Critical Service Level Failure

N/A

The applicable Service Levels are as specified in Annex A to Part A of Call-Off Schedule 14 (Service Levels).

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

- MODNet account and MOD virtual desktop
- Site pass (as required, Corsham)

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:

- No specific Quality Management System requirements are defined. This does not relieve the Supplier of providing conforming products under this contract. CoC shall be provided in accordance with DEFCON 627
- No Deliverable Quality Plan is required reference DEFCON 602B
- Concessions shall be managed in accordance with Def Stan. 05-061 Part 1, Issue 7 - Quality Assurance Procedural Requirements – Concessions
- 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

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.

Reporting & Meetings

- Monthly Contract Review
- Fortnightly progress report, submitted to the Authority Project Lead and the CES 1*
- Fortnightly Steering Group with Defence Digital Senior Leadership Team • Other meetings as required by the Authority

Timescales (Prior to Further Competition enter anticipated dates. Following Further Competition update with actual dates)

Call-Off Start Date	05 July 2024
Call-Off Initial Period	6 Months
Call-Off Expiry Date	31 December 2024
Call-Off Optional Extension Period	3 Months
Minimum notice period prior to a Call-Off Optional Extension Period	4 Weeks

SOR approved by (Name in capital letters)		Telephone	
Directorate / Division		Email	
Organisation Role / Position		Date	27/06/2024
Approver's signature			

OFFICIAL-SENSITIVE - COMMERCIAL

Original FBC Number (when known)	Amendment FBC Number (if applicable)
20240424_CC_MOD Enablement Programme_Continuation	N/A

1d. Key Deliverables Template

Full details are contained within the Statement of Requirement (SOR) - See Appendix 3

OFFICIAL-SENSITIVE - COMMERCIAL

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 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 2 (Staff Transfer), Part D only. ○ 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 9 (Security)
 - Call-Off Schedule 10 (Exit Management) ○ Call-Off Schedule 13 (Implementation Plan and Testing) ○ Call-Off Schedule 17 (MOD Terms) ○ Call-Off Schedule 25 (Ethical Walls Agreement) ○ Call-Off Schedule 26 (Cyber)
- 5 Core Terms (DIPS version)
- 6 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.

2a. Strategy for procurement and evaluation

Further competition	<input type="checkbox"/>	Competitive award criteria to be used for undertaking evaluation of proposal(s)	Direct Award		
Direct award	Error! Bookmark not defined.				
		Weighting (Technical)	N/A	Weighting (Price)	N/A

2b. General Conditions

Additional general DEFCON/conditions and DEFFORMs applicable to providing the Deliverables, are to be listed here:

Additional Conditions:

•



2c. Call-Off Special Terms

The following Special Terms are incorporated into this Call-Off Contract:

To support the development and handover of any future modelling artefacts, the below applies:

- 1) The model(s) developed as part of this Call-Off Contract are subject to the following, to be confirmed during the initial specification:
 - Only key products, to be agreed with you, will be modelled in detail. Others will be treated in aggregate;
 - Limited to a maximum of 5 modelled use-cases;
 - The model(s) will not include any automated links to existing business reporting or other systems; and
 - The model(s) will be in UK GBP only.
- 2) To assist the Buyer in the development of the model(s), the Supplier will:
 - Work with the Buyer to prepare an initial specification for the model(s) based on Buyer's objectives and requirements for the model(s). This initial specification will describe the structure of the model(s), its key inputs, calculations and outputs, and set out the proposed sensitivities and scenarios. The Supplier will request your confirmation of this before proceeding with development of the model(s);
 - Design and assist the Buyer to develop the model(s) based on the initial specification and data;
 - Provide interim versions of the model(s) to discuss with the Buyer;
 - Deliver a draft version of the completed model(s) for Buyer's user acceptance testing; and
 - Handover a final version of the completed model(s).
- 3) The Buyer agrees to be responsible for the following with respect to the model(s):
 - Specifying the requirements of the model(s) and how it is to be used by the Buyer, in connection with the Services;
 - The assumptions and input data to be used in developing and running the model(s);
 - The Buyer satisfying itself that the model(s) has been constructed in such a way that its use will meet the Buyer's objectives in all material respects;
 - Performing user acceptance testing when provided with drafts of the model(s);
 - The uses to which the model(s) and output data are put by Buyer, in connection with the Services;
 - Decisions the Buyer may make with respect to the Services based on the use of the model(s);
 - Any modifications to the model(s) after its release to the Buyer and any uses or decisions made following any such modifications;
 - Maintenance of the model(s) after its delivery to the Buyer.

Following completion of the development of the model in accordance with the model specification, and user acceptance testing of the model, The Supplier will hand over the Model to the Buyer and issue a letter substantially in the form of a "Transmittal Letter". Unless the Supplier hears from the Buyer to the contrary in writing within 5 Working Days ("the Transitional Period") of receipt of the model, the Supplier will treat and accept receipt of the model by the Buyer as demonstration and evidence of agreement that the Supplier has discharged their responsibilities in relation to the development of the model and in particular, that from the date of receipt of the model the Buyer will be solely responsible for the maintenance of the model. This will not affect the Buyer's ability to raise any comments or concerns about aspects of the Supplier's work or its quality after receipt of the model but it will remove the Buyer's ability to assert that the Supplier have not carried out the model development tasks in accordance with the model specification assigned to them under this letter or that the Supplier has any responsibility for maintenance of the model after its release.

If after the Transitional Period the Buyer has any additional requirements that were not in the scope of work originally agreed, the Supplier will be happy to discuss any further assistance that they may be able to provide and the terms and remuneration for such assistance.

2d. Call-Off Charges

Capped Time and Materials (CTM)	<input type="checkbox"/>
Incremental Fixed Price Time and Materials (T&M)	<input type="checkbox"/>
Fixed Price	<input type="checkbox"/>
A combination of two or more of the above Charging methods	<input checked="" type="checkbox"/>
T&S is applicable	<input checked="" type="checkbox"/>

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, the applicable rate card(s) shall be incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy) and the Supplier shall charge the Requirement Holder a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the Deliverables.

Reimbursable Expenses

Travel and subsistence will be limited to essential requirements in the UK up to a maximum limit of £12,240.00 ex VAT. Travel to and from duty station is at the supplier's own cost. The supplier requires approval from the Authority prior to travel commencing.

2e. Payment Method

CP&F payment against deliverables as per section 2F
PO Number TBA

Requirement Holder's Invoice Address

Strategic Command, Defence Digital, Core Enabling Services MOD
Corsham, Mustang Bldg, Wiltshire, SN13 9NR

Requirement Holder's Authorised Representative

Strategic Command, Defence Digital, Core Enabling Services
MOD Corsham, Mustang Bldg, Wiltshire, SN13 9NR

2f. Milestone Payments Schedule (MPS) (expand table as appropriate)

Milestone / Stage Payment number	Key Deliverable	Appendix 3 Deliverable Milestone & Acceptance Criteria Mapping	Deliverable Description	Payment Due Date	%	Milestone Payment value £ (ex VAT)
----------------------------------	-----------------	--	-------------------------	------------------	---	------------------------------------

**** These payments relate to activity associated with the T&M collaborative scope which will be prioritised, progressed and invoiced alongside the above. These activities will be tracked and signed off both through the agreed weekly reporting and the monthly cadence of Product Owner meetings in Secret Cloud to ensure agreed acceptance criteria are met. Payment schedule dates may adjust based on prioritisation of activity by the authority but aim to align with fixed outcome invoicing dates.**

		Total Contract Value	£609,070
--	--	----------------------	----------

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

Security Aspects Letter to be issued and executed alongside this Order Form. See Appendix 6.

2j. Progress Reports and meetings

Progress Report Frequency	Weekly	Progress Meeting Frequency	Fortnightly Steering Group & Monthly Contract Review
---------------------------	--------	----------------------------	--

2k. Quality Assurance Conditions

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

Allied Quality Assurance Publications (AQAP) 2110 – North Atlantic Treaty Organization (NATO) Quality Assurance Requirements for Design, Development and Production.

N/A ☒

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

Y ☒

AQAP 2105:2 – NATO Requirements for Deliverable Quality Plans

N/A ☒

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

N/A ☒

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)

N/A ☒

Relevant MAA Regulatory Publications (See attachment for details)

N/A ☒

Additional Quality Requirements (See attachment for details)

N/A ☒

Planned maintenance schedule requirement

N/A

N/A ☒

2l. Key Staff

KPMG LLP
66 Queen Square
Bristol UK, BS1 4BE

M: [REDACTED]

E:

2m. Key Subcontractor(s)

N/A

2n. Commercially Sensitive Information

Supplier's Commercially Sensitive Information:

- Attached proposal and pricing information
- Deliverables developed will be done with the authorities branding and templates.
- Deliverables provided with MOD branding are not to be attributed to KPMG

2o. Cyber Essentials

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 CallOff Schedule 26 (Cyber).

☒ **Error! Bookmark not defined.**

2p. Implementation Plan

Not applicable

**3. Charges**

Estimated Contract Value (excluding VAT) for Call-Off Contract

**4. Additional Insurances**

Not applicable

5. Guarantee

Not applicable

6. Social Value Commitment

Not applicable

7. Requirement Holder Commercial Officer Authorisation

Order Form approved by (Name in capital letters)		Telephone	
Directorate / Division		Email	
Organisation Role / Position		Date	05/07/2024
Approver's signature			

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

DEFFORM 111
(Edn 10/22)**Appendix 1 - Addresses and Other Information****1. Commercial Officer Name:**

Address: Defence Digital,
Floorplate B2, Building 405, MOD Corsham,
Westwells Road, Corsham, SN13 9NR

Email: [REDACTED]

**2. Project Manager, Equipment Support
Manager or PT**

Leader (from whom technical information is available)

Name: [REDACTED]

Address: Strategic Command, Defence Digital, Core Enabling
Services
MOD Corsham, Mustang Bldg, Wiltshire, SN13 9NR

Email: [REDACTED]

**3. Packaging Design Authority Organisation & point of
contact:**

(Where no address is shown please contact the Project Team
in Box 2)

**4. (a) Supply / Support Management Branch or Order
Manager:**

Branch/Name:



(b) U.I.N.

5. Drawings/Specifications are available from**6. Intentionally Blank****1. Quality Assurance Representative:**

Commercial staff are reminded that all Quality Assurance
requirements should be listed under the General Contract
Conditions.

AQAPS and **DEF STANs** are available from UK Defence
Standardization, for access to the documents and details of the
helpdesk visit <http://dstan.gateway.isg-r.r.mil.uk/index.html>
[intranet] or <https://www.dstan.mod.uk/> [extranet, registration

8. Public Accounting Authority

1. Returns under DEFCON 694 (or SC equivalent) should be
sent to DBS Finance ADMT – Assets In Industry 1, Level 4
Piccadilly Gate, Store Street, Manchester, M1 2WD
☎ 44 (0) 161 233 5397

2. For all other enquiries contact DES Fin FA-AMET Policy,
Level 4 Piccadilly Gate, Store Street, Manchester, M1 2WD
☎ 44 (0) 161 233 5394

9. Consignment Instructions

The items are to be consigned as follows:

10. Transport. The appropriate Ministry of Defence
Transport Offices are:

A. DSCOM. DE&S, DSCOM, MoD Abbey Wood, Cedar 3c,
Mail Point 3351, BRISTOL BS34 8JH

Air Freight Centre

IMPORTS ☎ 030 679 81113 / 81114 Fax 0117 913 8943

EXPORTS ☎ 030 679 81113 / 81114 Fax 0117 913 8943

Surface Freight Centre

IMPORTS ☎ 030 679 81129 / 81133 / 81138 Fax
0117 913 8946

EXPORTS ☎ 030 679 81129 / 81133 / 81138 Fax 0117
913 8946 **B. JSCS**

JSCS Helpdesk No. 01869 256052 (select option 2, then
option 3)

JSCS Fax No. 01869 256837

Users requiring an account to use the MOD Freight Collection
Service should contact [UKStratCom-
DefSpRAMP@mod.gov.uk](mailto:UKStratCom-DefSpRAMP@mod.gov.uk) in the first instance.

11. The Invoice Paying Authority

Ministry of Defence
DBS Finance

☎ 0151-242-2000

Walker House, Exchange Flags Fax: 0151-242-2809
Liverpool, L2 3YL **Website is:**
<https://www.gov.uk/government/organisations/ministry-ofdefence/about/procurement>

Leidos-FormsPublications@teamleidos.mod.uk

*** NOTE**

1. Many **DEFCONs** and **DEFFORMs** can be obtained from the MOD Internet Site:
<https://www.kid.mod.uk/maincontent/business/commercial/index.htm>

2. If the required forms or documentation are not available on the MOD Internet site requests should be submitted through the Commercial Officer named in Section 1.

12. **Forms and Documentation are available through *:**
Ministry of Defence, Forms and Pubs Commodity Management
PO Box 2, Building C16, C Site
Lower Arncott
Bicester, OX25 1LP (Tel. 01869 256197 Fax: 01869 256824)
Applications via fax or email:
needed].


OFFICIAL-SENSITIVE COMMERCIAL

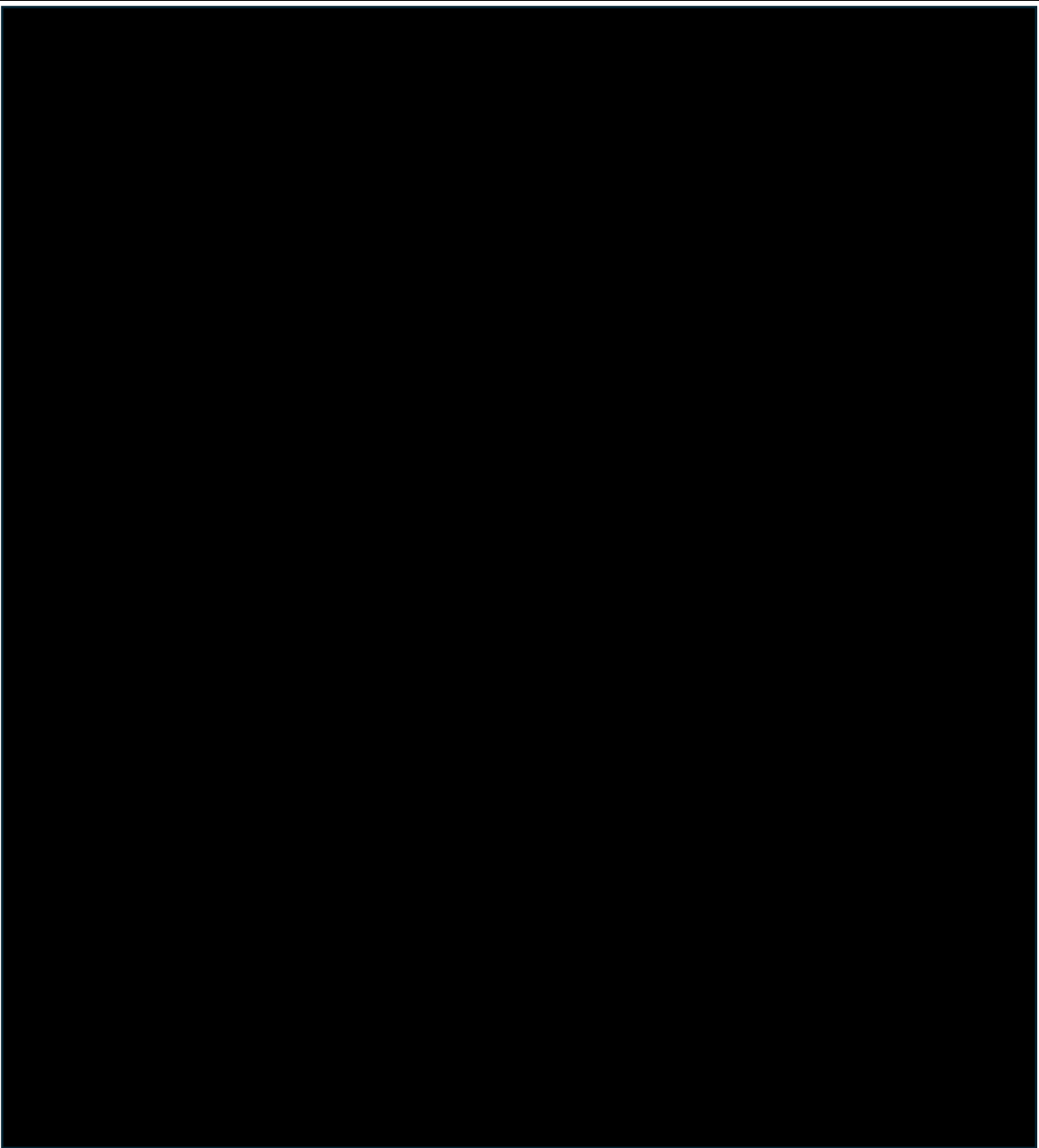
Appendix 2 – Supplier’s Quotation - Charges Summary



Materials	
Other (Please provide details below) Description	Cost
.....	(excl. VAT)

Appendix 3

Unique Tasking Number XXXXXX	Issue Number & Date Version 2.0 (27 June 2024)	DIPS Ref: Lot 1: RM6249/DIPS (1) 045
Task Title: MOD Enhancement Programme		
Contract Start Date: 01 July 2024 Contract End Date: 31 Dec 2024		Extension Option: 3 Months – 01 Jan 25 to 31 Mar 25
1. Brief Description of Task and Background The Community Cloud project seeks to deliver a hyperscale-like cloud service, enhancing ways of working and increasing interoperability with partners, other government departments requiring both continuity of resource and significant digital expertise to accelerate the execution of an upcoming Invitation to Negotiate process. This contract will be placed in support of the ITN process, approvals campaign, and the supporting evidence required to progress through these complex activities.		
2. Activities to be Undertaken/Deliverables 		



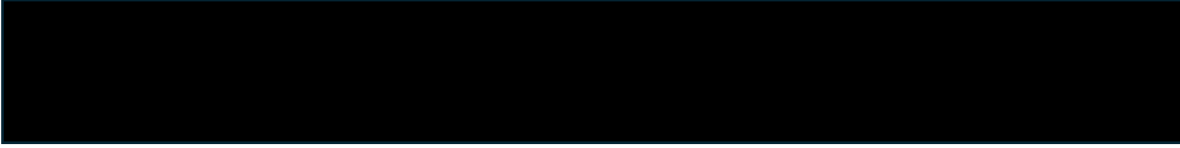
3. Reporting & Meetings

1. Monthly Contract Review
2. Fortnightly progress report, submitted to the Authority Project Lead and the CES 1*
3. Fortnightly Steering Group with Defence Digital Senior Leadership Team
4. Other meetings as required by the Authority

4. Performance Criteria

1. In line with best practice, performance reviews should be conducted at key stages throughout the contract as set out in **Section 5** of this Statement of Requirement.

4. Project Deliverables & Acceptance Criteria



6. Location and T&S

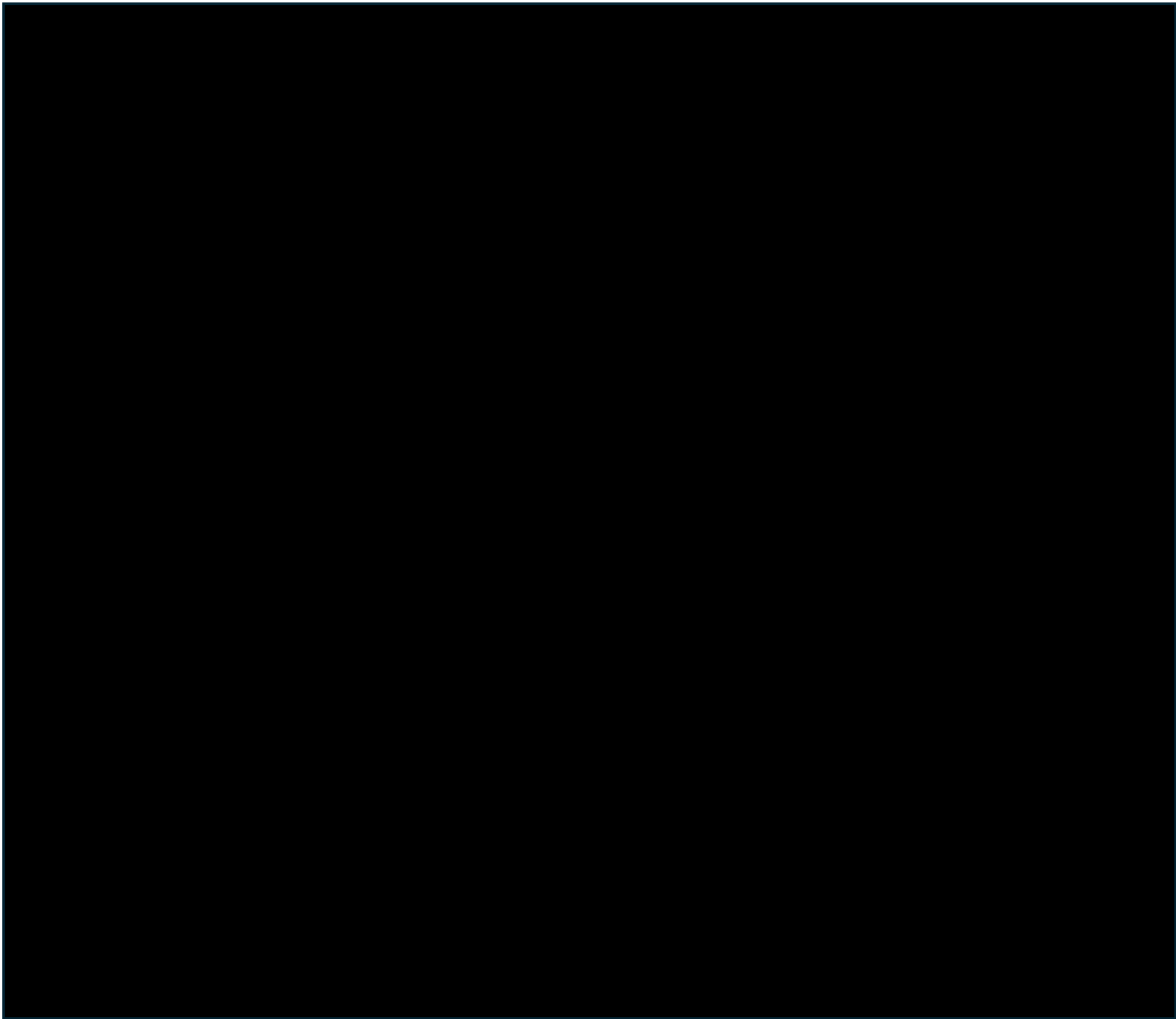
1. The supplier will be required to complete the majority of this work remotely from their own premises but should be willing to travel to MOD Corsham (duty station) as and when required by the Authority. All personnel must be SC cleared.
2. Travel and subsistence will be limited to essential requirements in the UK up to a maximum limit of £[REDACTED] ex VAT. Travel to and from duty station is at the supplier's own cost. The supplier requires approval from the Authority prior to travel commencing.

7. Government Furnished Assets (GFA) (*List all GFA applicable to the task in accordance with DEFCON 611 (Edn 02/16) & 694 (Edn 03/16)*)

The individuals will require MOD owned facilities and equipment for daily working including mobile devices as a matter of necessity. Specifically:

1. MODNet account and MOD virtual desktop
2. Office space (as required in Corsham)
3. Site pass (as required, Corsham)
4. Support to enable flexible working

8. Dependencies



Appendix 5 Confidentiality Undertaking

Employee: [REDACTED]

Name of Employer: KPMG

MOD Contract/Task No: PS438

Title: [REDACTED]

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

OFFICIAL-SENSITIVE -

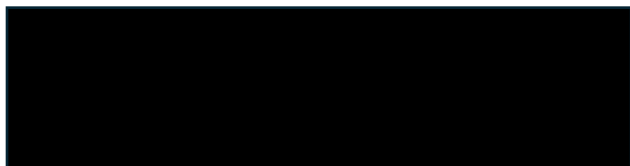
COMMERCIAL

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 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.



Date: 5th JULY 2024

Appendix 6 Security Aspects Letter



**Strategic
Command**

Name:

Title: Core Enabling Services Security Aspects Letter - SCC

1. Strategic Command

Mustang Building, MOD Corsham, Westwells
Road, CORSHAM, SN13 9NR

++

Military Network: 96770 7493
Telephone: 0306770 7493
Email:

Chief Information Security Officer

Jan 2024

SECRET COMMUNITY CLOUD - SECURITY ASPECTS LETTER FOR MOD

Date of Issue: 27/06/2024

For the attention of: [REDACTED]

**ITT/CONTRACT NUMBER & TITLE: PS438 MOD Cloud Enablement Programme
Continuation**

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

2. Aspects that constitute 'SECRET Matter' for the purpose of the DEFCON 659A Security Clause and OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Grading Guide outlines the minimum measures required to safeguard the assets and information.

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

4. Will you please confirm that:

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

b. The definition is fully understood.

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

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

5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.
6. Classified Information associated with this Contract must not be published or communicated to anyone without the approval of the MOD Contracting Authority.
7. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer in accordance with DEFCON 76.
8. Contact details for the MOD Project Security Officer (PSyO) (responsible for the coordination of effective security measures throughout the Project/Programme) are included below:

Yours
faithfully

ANNEX A
Security Grading Guide
Dated Jan 24

Annex A to the Security Aspects Letter is an extract of the Security Grading Guide for SECRET Cloud. The following appendixes cover the security aspects, security classification of any physical assets and the security clearances.

Document Amendment Version History

Changes to this document should be addressed to the project Security Lead. Such changes will need agreement from ISS App Services Assistant Head for Project EMPORIUM.

Version	Date	Detail	By
0.1	03/01/24	Initial Draft	
1.0	15/01/24	Final review	

Annual Document Review History

Revision date	Reviewer

References

Ref	Ref No	Title
1	Version 3	DIO BIM Security Guidance Note
2	JSP 440 Part 2 V6.02	Leaflet 9 Classification Policy – Dec 2018
3	JSP 440 Part 2 V6.02	Leaflet 10 Information Asset Security
4	JSP 440 Part 2 V6.01	Leaflet 12 Communications Security – Oct 2018
5	DEFCON 531	Disclosure of Information
6	DEFCON 532A	Protection of Personal Information
7	DEFCON 532B	Protection of Personal Information
8	DEFCON 659A	Security Measures
	GSC V1.1	Government Security Classification May 18
10	DEFSTAN 05-138	Cyber Security for Defence Suppliers

Glossary

Name	Definition
------	------------

OFFICIAL	The majority of information that is created or processed by the Public sector. This includes routine business operation and services, some of which could have damaging consequences if lost, stolen or disclosed inappropriately, but are not subject to a heightened risk profile. This includes the information relating to the routine operations of Defence.
Reportable OFFICIAL	Large quantities of OFFICIAL information, either by aggregation or association.
Security Lead	Security Advisor for SCC
SENSITIVE	Information which in the wrong hands could cause significant harm to the work or reputation of Defence or the Government more widely. Useful test – could its loss lead to significant criticism of MoD at the national level?
SECRET	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable Threat Actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious crime.
LIMDIS	The Handling Instruction 'Limited Distribution' (LIMDIS) is used in MOD to provide a commonly understood system for ensuring that particularly sensitive information is seen only by those with a need to know.
UK EYES DISCRETION	Departments and agencies may exercise their discretion to allow non-UK national's access to an asset marked UK EYES DISCRETION in exceptional circumstances, subject to the mandatory requirements for access.
UK EYES ONLY	UK EYES ONLY must be used to designate classified assets that are of particular sensitivity to UK national interests. Information identified as UKEO must not be sent to foreign governments, overseas contractors, international organisations or released to any foreign nationals (either overseas or in the UK) without the originator's specific consent.
Commercial-in-Confidence	Sensitive information that an authority or business shares with another party in confidence. Therefore, whom it is shared with the information is obligated to not disclose or use that information without consent.
Aggregation	The marking of an individual Information Asset may be less than that which should be attributed to a set of multiple such assets, similar or dissimilar. When multiple instances of the same type of assets when taken together accrue a higher sensitivity.

Acronym	Description
BPSS	Baseline Personal Security Standard
BOM	Bill Of Materials

CTO	Chief Technical Officer
DV	Developed Vetting
FAQ	Frequently Asked Questions
HDD	Hard Drive
HLD	High Level Design
IOC	Interim Operating Capability
LLD	Low Level Design
NCSC	National Cyber Security Centre
RMADS	Risk Management Accreditation Document Set
SAC	Security Assurance Coordinator
SC	Security Check
SCC	SECRET Community Cloud
SCG	Security Classification Guide
SDA	System Design Authority
SM	Service Manager
SOC	Security Operating Centre
SPC	Sensitive Post Check
SRD	System Requirement Document
URD	User Requirements Document

1. Introduction

1. This Security Classification Guide (SCG) is to be issued under cover of this SAL for all contractor involvement in project delivery of the SECRET Community Cloud (SCC).
2. The scope of the SCG includes the project (the artefacts, project staff, physical environments, and document deliverables) and the Community Cloud capability that are the ultimate project outputs.
3. The SCG requirements placed on specific aspects for confidentiality reasons are stated at Appendix A.
4. The SCG requirements placed on specific Physical Assets for confidentiality reasons are stated in Appendix B.
5. The security Clearance requirements for the project team, technical support and peripheral personnel are stated in Appendix C.
6. Note – that as this Guide will also be issued and used internally within the MoD, the Appendices contain some aspects and roles which are not relevant to the contractor.
7. This Guide is intended to be a living document with additions (and corrections) applied as required to support the project. The process for such updates will be managed through the Security Lead for the project in line with the contractors change process.
8. When using this document, readers should read the entire guidance rather than go directly to a specific section, as information elsewhere may directly impact the classification of a specific item.

2. HMG Security Classifications

9. There are three Security Classifications as implemented on 1 Apr 14:

OFFICIAL
SECRET
TOP SECRET

10. Assets which are classified as OFFICIAL but are Security Marked as SENSITIVE are subject to strict handling rules for this project in accordance with MOD Policy.

3. Handling Instruction – OFFICIAL and OFFICIALSENSITIVE

11. The following advice has been issued by HMG and for the protection and handling of OFFICIAL and OFFICIAL-SENSITIVE information:

- a. Physical documents or printed emails must be locked in a secure container when leaving your place of work.
- b. Physical documents must be disposed of by HMG approved means.
- c. Email of OFFICIAL-SENSITIVE information for this project must only be sent within
MoD and to other Departments across secure systems (including MoDnet and the Government Secure Intranet) or by following information detailed in MOD Policy, or with the information owner's permission. OFFICIAL-SENSITIVE can be transmitted over the internet to a third party provided that the conditions described in MOD Policy for Information Asset Security.
- d. Working with MoD approved ICT (MODNET) providing there is a business need, in
certain strict conditions, OFFICIAL-SENSITIVE aspects may be physically taken and worked on at non-MoD locations but not read or worked on in public or otherwise in sight of unauthorised persons.
- e. OFFICIAL-SENSITIVE discussions may take place on all types of phone, but not with, or within earshot of, unauthorised persons (those who are not approved to work on or to be involved with this project).
- f. OFFICIAL-SENSITIVE information can be sent across OFFICIAL-SENSITIVE accredited Authority systems.
- g. OFFICIAL-SENSITIVE Information is to be handled with greater care and steps taken to reinforce the need to know, note there is special rules for information exchanged internationally.

4. Handling Instruction – SECRET

12. All SECRET information must be very well protected following advice has been issued by HMG and for the protection and handling of SECRET information:

- a. **ICT infrastructure (including Cloud)** – must be physically or cryptographically isolated from less trusted domains.
- b. **Special Handling** – is to be implemented with enforcement of the Need to Know.
- c. **Document handling** – Register and file documents in line with HMG policies.
- d. **Storage** - must follow the Defence in Depth methodology using CPNI approved security furniture.
- e. **Moving assets by hand** – follow MoD process for the movement of SECRET assets.
- f. **Electronic Information at Rest** – is to be protected by physical security appropriate for SECRET assets. Where data is at rest on non-physically secure devices it will be encrypted with High Grade protection.
- g. **Electronic Information in Transit** – will only be exchanged via appropriately secured mechanisms. This must involve use of appropriately accredited shared services or High-Grade encryption approved by NCSC for use at SECRET.
- h. **ICT Services/Cloud Services** – must be assured as per Secure by Design.
- i. **Removable Media** – Content must be appropriately encrypted using High Grade Encryption.
- j. **Telephony** – Must only be via secure assured/approved telephony and VTC.
- k. **Disposal / Destruction** – Must be via MoD approved processes.

5. **Mandatory Conditions to be included in all Contracts.**

13. It is important that the correct contractual security clauses are included in the tender/contract. This includes clauses which relate to the appropriate protection of nonprotectively marked information which nevertheless must be protected appropriately such as Personal Data.

14. All MoD Contracts must as a minimum, include the following mandatory conditions:

- a. DEFCON 531 (Disclosure of Information)
- b. DEFCON 532A (Protection of Personal Information (Where Personal Data is **not** being processed on behalf of the Authority)) or DEFCON 532B (Protection of Personal Data (Where Personal Data **is** being processed on behalf of the Authority)).
- c. DEFCON 76 (Contractors at Government Establishments)
- d. DEFCON 659A (Security Measures)
- e. DEFSTAN 05-138

- i. CSM Risk Assessment
- ii. Supplier Assurance questionnaire
- iii. Defence Cyber Protection Partnership (DCPP)

6. Classification for Aspects

The classification of Aspects detailed below refer to the UK Gov specific elements and does not place a requirement to classify pre-existing or generic IP and assets. The following classification of Aspects is for the SCC Build and Operate phases.

OPERATE		
ASPECT		CLASSIFICATION
A.1 Existence of the Project	A.1.1 In Service Date	OFFICIAL
	A.1.2 Highest classification of information to be stored forwarded and processed.	SECRET-UK EYES ONLY
A.2 Project/System Name i.e.	A.2.1 Out of context of the system data Classification or system use, i.e. not associated with the system's purpose of user community	OFFICIAL
	A.2.2 In context	SECRET
	A.2.3 Operational Concept of SCC use-case	Up to SECRET – to be determined with the project before classification is decided.
	A.2.4 Association with similar projects	SECRET-UK EYES ONLY
	A.2.5 Details of specific usecase capabilities	SECRET – UK EYES ONLY
A.3 Project/System Cover Name	A.3.1 To be used for out of context reference to the Project or System.	N/A
A.4 Detailed meaning of codeword	A.4.1 Link to operational capability or locations or users	N/A

A.5 Personal Data	A.5.1 Personal data is to be handled according to relevant Data protection laws.	OFFICIAL
A.6 High-Level Architecture summary/Description of the project/system		SECRET (seek confirmation before publishing from the Security Lead to understand the differences between Build & Operate)
A.7 Design Documentation	A.7.1 System Design Overview	SECRET
	A.7.2 High Level Design (with no IPs or Aspects within it which are of a higher classification that will comprise SCC)	OFFICIAL-SENSITIVE
	A.7.3 High Level Design of the whole SCC capability (Individual document)	SECRET
	A.7.4 Low Level Design Artefacts (relating to a single Sub-System or HLD)	SECRET-UK EYES ONLY
	A.7.5 Full complete set of HLDs or LLD artefacts	SECRET-UK EYES ONLY
	A.7.6 As long as it does not contravene any other Aspects within this guide which are of a higher classification, individual elements of the configuration design, when used or handled in isolation from the HLD and LLD.	Discussion with the Security lead to determine the classification from build to operate considering data storage.
	A.7.7 General Project Documentation to enable the administration and management of the project – Not to include site locations, or any classified subjects that will bring above the OFFICIAL classification.	OFFICIAL
A.8 Complete set of Design Documentation	A.8.1 (SDO, HLD, LLDs) Hardware and software, logical and Physical Diagrams	SECRET-UK EYES ONLY
	A.8.2 Internal cutaway and exploded views; Circuit diagrams of important units; Technical specification of hardware, details of	SECRET-UK EYES ONLY

	processors, capacity of magnetic storage media	
	A.8.3 Technical specifications, Drawings, sketches and photographs if they in no way indicate operational user, users, user locations and do not include detail on any security enforcing function	OFFICIAL-SENSITIVE
	A.8.4 Technical Specifications, Drawings sketches and photographs if they do indicate operational use, users, user locations or detail any security enforcing function	SECRET UK EYES ONLY
	A.8.5 Final Security design of any selected use-case	SECRET UK EYES ONLY
A.9 Network IP Addresses – Allocated to systems¹	A.9.1 A single IP address with no associated indication of what it is being used for, or the Classification of the system or network on which it is being used ²	OFFICIAL-SENSITIVE
	A.9.2 A single or range of IP addresses, together with information that identified them as being used on a SECRET system or network either directly or by use of system or project names	SECRET, up to SECRET-UK EYES ONLY
	A.9.3 A single or number of IP addresses and the name or device for which it is being used on.	SECRET, up to SECRET-UK EYES ONLY
	A.9.4 The Full IP Range	SECRET, up to SECRET-UK EYES ONLY
	A.9.5 Obfuscated IP address, single (e.g. x.x.1.1	OFFICIAL
	A.9.6 Aggregation of more than 1 different system/service IP address	SECRET-UK EYES ONLY
	A.9a Fully Qualified Domain Names	
	A.9a.1 FQDN by their nature always provide the context of the capability	SECRET UK EYES ONLY

A.9b Hostnames	A.9b.1 Hostnames without capability context as a Secret Cloud	OFFICIAL-SENSITIVE
	A.9b.2 Hostnames with capability context of the System	SECRET
A.10 User Requirements Documents (URD)	A.10.1 Complete document, linked to system capability	SECRET-UK EYES ONLY
	A.10.2 Selected extracts referring to non-specialist capability (i.e., implementation of COTS products)	OFFICIAL-SENSITIVE

A.11 Detailed Technical Requirements (SRD)	A.11.1 Complete document, linked to system capability	SECRET
	A.11.2 Selected extracts referring to non-specialist capability (i.e., implementation of COTS products)	OFFICIAL-SENSITIVE
A.12 Secure by Design Artifacts		SECRET
A.13 File Type Control Policy (inc dirty word list)		SECRET UK EYES ONLY
A.14 Management Documentation and Plans (except financial information)	A14.1 Very high-level programme status information with no detail of purpose or role of system – ideally as a small part of a wider reporting.	Up to OFFICIAL-SENSITIVE
	A14.2 Not including any other information otherwise described herein	OFFICIAL
	A14.3 Names of developers/manufacturers/maintainers	Up to OFFICIAL-SENSITIVE COMMERCIAL
	A.14.4 Including information otherwise described herein, or which by aggregation may warrant a higher marking	To be agreed.
A.15 Management Documentation and Plans with Financial and costing information	A.15.1 Very high-level financial information with no detail of purpose or role of system – ideally as a small part of wider reporting.	OFFICIAL
	A.15.2 Not including any other documentation otherwise described herein	OFFICIAL-SENSITIVE (COMMERCIAL)

	A15.3 Including information otherwise described herein, or which by aggregation may warrant a higher marking.	Reportable OFFICIAL-SENSITIVE (if large amount through aggregation) SECRET This should be risk managed where a decision on what the aggregation classification should be.
A.16 Hardware Assets All carry the same security classification as that of the Cloud they are part of or have been used on.	A.16.1 Hardware inventory (inc versions) with no detail of purpose, nature of role of system (i.e. BOM)	OFFICIAL-SENSITIVE
	A.16.2 Once deployed (installed but without operational data)	SECRET
	A.16.3 Once deployed (installed but with operational data)	SECRET
A.16a Software Assets	A.16a.1 Base software inventory (excluding versions) with no detail of purpose nature or role of system (i.e. BOM)	OFFICIAL-SENSITIVE
	A.16a.2 Base Software inventory including versions	SECRET
	A.16a.3 Software inventory without sufficient detail (version/patch state) to enable inference of vulnerabilities	OFFICIAL-SENSITIVE
	A.16a.4 Detailed Software inventory (with versions, numbers, patch state etc)	SECRET
	A.16a.5 Programme specifications and code; Protection of validated software during development; Protection of non-validated software during development.	SECRET
	A.16a.6 Features of operating system other than the above.	SECRET
	A.16a.7 Physical protection of training software	SECRET
	A.16a.8 Deployed-in service software	SECRET
A.17 Complete System Installation and Configuration Documentation individual documents as agreed		SECRET-UK EYES ONLY

A.18 Complete Network Installation and Configuration Documentation individual documents as agreed		SECRET-UK EYES ONLY
A.19 Locations	A.19.1 Identification of system installation (Site) by Site ID	OFFICIAL-SENSITIVE
	A.19.2 Identification of System Installation site ID and Installation site name, building name and room number	SECRET
	A.19.2 Identification of system installation at UK site by site or building name, or unit or establishment title	SECRET
	A.19.3 Identification of system installation at (non-sensitive) overseas sites, by site or building name, or unit or establishment title	N/A
	A.19.4 Identification of system installation at sensitive sites by site or building name or unit or establishment title	SECRET
	A.19.5 Physical location of Data Centre and Disaster Resilience Centre (DC/DR)	SECRET
	A.19.6 Data Centres ³	SECRET
A.20 Users of systems based at specific sites (e.g. anonymous user lists) This is for the protection of the organisational structure		OFFICIAL-SENSITIVE
A.21 Detailed Identification of users of system based at a specific site, with full details of user's names, roles etc. This is for the protection of the individuals		SECRET
A.22 Factory Acceptance Testing	A.22.1 Without inference of specific system codename; architecture or purpose	OFFICIAL-SENSITIVE
	A.22.2 Allowing inference of system architecture and	SECRET
	purpose or documenting system configuration and or failures.	
	A.22.3 All System Test Plans & Procedures. As testing progresses to IOC this increases.	SECRET
A.23 System Acceptance Test Data (i.e. Dummy data	A.23.1 Without inference of system architecture and purpose	OFFICIAL

generated for test purposes only)	A.23.2 Allowing inference of system architecture and purpose	SECRET
A.24 System Acceptance Test Reporting	A.24.1 CTAS reports, Pen Test Reports, Functional testing and Security test data which identifies and details system defects, vulnerabilities.	SECRET
	A.24.2 Other system test results and reports from Functional and User testing and trials	SECRET
	A.24.3 Statistical reporting of testing progress for Management Information	OFFICIAL-SENSITIVE
A.25 System Acceptance Test Reporting: Individual functional or security defect associated with potential vulnerabilities but without detailed explanation of vulnerability and/or exploitation.		SECRET (Unless approved otherwise by Security Lead)
A.26 Site Acceptance Testing		SECRET
A.27 Operational Data (live data or used for test purposes) Including video images		SECRET
A.28 Passwords and PINs: System passwords (inc all user accounts, service accounts, Network devices, BIOS passwords, Secondary logon passwords). Password algorithms and user profiles	A.28.1 OS Development Instance/Environment	OFFICIAL-SENSITIVE
	A.28.2 Secret Development Instance/Environment	SECRET
	A.28.3 Reference Instance/Environment	SECRET
	A.28.4 Production Instance/Environment	SECRET
A.29 Cryptographic material		SECRET or as otherwise marked
A.30 Service Management	A.30.1 SM Overview	OFFICIAL
	A.30.2 SM Processes (exc User Account Management)	OFFICIAL
	A.30.3 User Account Management Process	SECRET
	A.30.4 SM Work Instructions	SECRET
	A.30.5 All material containing SOC related operational, procedural or technical information.	SECRET-UK EYES ONLY
A.31 Training Information	A.31.1 Basic User Guidance (pre-logon training for general systems users).	(seek confirmation before publishing)

	A.31.2 FAQs	OFFICIAL
	A.31.3 Training material	OFFICIAL
	A.31.4 COTS software application training material which does not disclose the design or specific use of the application on the system	OFFICIAL
A.32 Applications	A.32.1 Details of a single app or suite of apps (with version)	OFFICIAL
	A.32.2 Details of a single app and version in context to SCC	SECRET
	A.32.3 List of applications, but with no detail of number of users, organisation, versions	OFFICIAL
	A.32.4 Detailed list of Apps (inc versions, numbers of users and their organisations)	SECRET
	A.32.5 Proposed tactical field application	SECRET
A.33 Test and Trials Documentation	A.33.1 Strategy	OFFICIAL-SENSITIVE
	A.33.2 Plans	OFFICIAL-SENSITIVE
	A.33.3 Test Scripts	SECRET
	A.33.4 Trials Scenarios	SECRET
	A.33.5 Test and Trials Results (identifying vulnerability)	See serials A.22-26
	A.33.6 Test and Trials Results (not identifying a vulnerability)	See serials A.22-26
A.34 Live System Diagnostic Information (e.g. Logs from COTS packages) Sanitisation to a lower Classification of Diagnostics for return to Vendors will need agreement from the Security Lead		SECRET
A.35 Pre-Prod, System Test Diagnostic Information (e.g. Logs from COTS packages) Sanitisation to a lower Classification of Diagnostics for return to vendors will need agreement from the Security Lead.		SECRET
A.36 IT Health Check/Vulnerability Assessment or Penetration Test. This includes the Response/Remedial Action Plan and rectification activities.		SECRET-UK EYES ONLY
A.37 <ul style="list-style-type: none"> • System Concept of Employment • System Concept of Use • System Concept of Operation 		SECRET
A.38 Cloud Environments	A.38.1 Development testing with no association to MoD including all test and dev accounts	Commercial-in-Confidence

	A.38.2 Design and development with association to MoD, no Personal or classified information, including all test and design accounts	SECRET
	A.38.3 Environment Operational	SECRET

A.39 Equipment	A.39.1 Design equipment for application design and cloud environments Only MoD equipment to be used or MoD approved equipment	SECRET
A.40 Databases	A.40.1 Design of Data base with no information held	the context is to be determined between the authority and contractor.
	A.40.2 Data base with Live information	SECRET
A.41 Software Factory including Hardened Containers	A.41.1 CI/CD Orchestrator	OFFICIAL
	A.41.2 Develop	OFFICIAL
	A.41.3 Build	OFFICIAL-SENSITIVE
	A.41.4 Test	SECRET
	A.41.5 Release	SECRET
A.42 Repositories less Public Repositories	A.42.1 All repositories	SECRET
A.43 Public Repositories	A.43.1 Public Repositories (COTS, vendor or Open-Source Communities)	OFFICIAL if a relationship to MOD
A.44 Virtual Machines	A.44.1 All Virtual Machines	Seek confirmation before publishing
A.45 Security Tooling	A.45.1 All Security Tooling	Seek confirmation before publishing
A.46 Financial and costing information – General	A.46.1 High level financial information with no specific detail of use-case capabilities – ideally as a small part of wider reporting	OFFICIAL

	A.46.2 Costing Elements (individual elements) when separated from project, no context of capability. This will allow contractors to engage with sub-contractors and supply chain on a single element of the costing of the project with the need for cumbersome audit and protective security arrangements.	OFFICIAL
	A.46.3 Total project costs	OFFICIAL-SENSITIVE - COMMERCIAL
A.47 Timescales	A.47.1 Timelines are broad, and consideration may be given to increasing the classification when linked to threat assessments Political decision timescales may be classified as SECRET	OFFICIAL-SENSITIVE
A.48 Key User Requirements (KUR's) system requirements, CONUSE, and detailed objectives	A.48.1 Initial generation of documents will have low classification at OFFICIALSENSITIVE and excludes metrics/volumetrics. All	Up to UK SECRET UKEO – Consultation with Security Lead.
	aspects relating to metrics/Volumetrics and specific capabilities shall be up to UK SECRET UKEO.	
A.49 Requirements	A.49.1 All Authority requirements that are sent via from the Authority.	OFFICIAL-SENSITIVE - COMMERCIAL
	A.49.2 Replies to requirements are to be sent in line with this SGG.	UPTO UK SECRET UKEO – it is advised to confirm with the Authority Security Lead prior.
A.50 Cloud Hardening	A.50.1 All security hardening of SCC is to be treated as the highest classification of the Cloud offering	Up to SECRET UKEO

Table 1 Classification of Aspects

All of the items in the Table 1 that are marked OFFICIAL and higher are also subject to NEED-TO-KNOW: they should only be made available to those who have a demonstrable requirement to see that information. For all items marked SECRET or above application of the need-to-know principal shall be supported with formal recording and reporting of who has access and why.”

7. Security Classification of Physical Assets

Detailed below are the physical assets and what they are classified during the various phases (Design, Build and Operate). The CES disposal process should be followed where equipment is scheduled for end of life. Other arrangements maybe granted if the supplier needs to dispose of single items such as HDD, this should be discussed with the Authority Security Lead.

ID	Component	DESIGN	BUILD	Operate	Reuse/ Decommissioning /Disposal ⁴
B.1	Thick Client unencrypted Hard Disk Drive (HDD) Including Images	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.2	Thick Client encrypted HDD Including images	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.3	Thick client UAD (laptop/ desktop) Ex HDD)	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.4	Thin Client UAD	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.5	Monitor	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL- SENSITIV E	Dispose as OFFICIAL; if 'burn in' exists, dispose of according the highest Classification asset(s) handled
B.6	Keyboard & Mouse	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL	Dispose or re-use as OFFICIAL

B.7	Inkjet Printers (with no internal HDD)	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL- SENSITIV E	Dispose memory components as Highest classification of the system non-memory components as OFFICIAL
B.8	Inkjet Printer HDD	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.9	Inkjet Printer Cartridge	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL	Dispose as OFFICIAL

OFFICIAL-SENSITIVE - COMMERCIAL

B.10	Laser Printer (inc Drum etc)	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.11	Red Routers	SECRET	SECRET	SECRET	SECRET
B.12	Black Router	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL	Dispose as OFFICIAL
B.13	Red Switches	SECRET	SECRET	SECRET	Dispose memory components as SECRET non-memory components as OFFICIAL
B.14	Black Switches	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL	Dispose as OFFICIAL
B.15	Dumb Power Supply Units	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL	reuse as OFFICIAL
B.16	Managed UPS	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL- SENSITIV E	Dispose as OFFICIAL SENSITIVE
B.17	Unmanaged UPS	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL	Dispose as OFFICIAL
B.18	Server and SAN hard Drives	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.19	Server and SAN (no disks)	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.20	Non-powered network equipment (fibre taps, fly leads, etc)	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL ⁵	Dispose or re-use as OFFICIAL
B.21	Media converters	Commercial -in- Confidence	Commercial -in- Confidence	OFFICIAL- SENSITIV E	Dispose as or reuse at OFFICIAL
B.22	Scanners/ Digi-senders (With no internal hard drive)	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.23	Scanners/ digi-senders (with internal hard drive)	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.24	Dev, Test & Reference and Pre-Prod environments (System High)	Commercial -in- Confidence	Commercial -in- Confidence	As above for component s	As above for components

OFFICIAL-SENSITIVE - COMMERCIAL

B.25	Dynamic/ Static RAM	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.26	Non-Volatile Memory	Commercial -in- Confidence	Commercial -in- Confidence	SECRET	SECRET
B.27	Optical Media. Blue ray CD/DVD	Commercial -in- Confidence	Commercial -in- Confidence	Treat as per the classificatio n of information held	SECRET
B.28	Flash memory	Commercial -in- Confidence	Commercial -in- Confidence	Treat as per the classificatio n of information held	SECRET
B.29	Paper	Commercial -in- Confidence	Commercial -in- Confidence	Treat as per the classificatio n of information held	OFFICIAL – SHRED SUKEO approved crosscut shredder or incinerate
B.30	Garrison	Commercial -in- Confidence	Commercial -in- Confidence up to any SECRET Configs	SECRET	SECRET
B.31	Firewall	Commercial -in- Confidence	Commercial -in- Confidence up to any SECRET Configs	SECRET	SECRET

8. Handling

1. OFFICIAL is aimed at ensuring storage to protect against tampering, obfuscation of enduser to the non-MoD supply chain, and that proper disposal routes are followed as mandated by HMG requirements. SECRET is to be stored and protected at a much higher level where attacks may be bespoke in nature and tailored to specifically attack the target infrastructure. Vulnerable elements of the supply chain may be targeted to facilitate a further compromise of information. Disposal routes for SECRET is to be strictly followed and all communication of SECRET information via MoD assured products and devices.

2. OFFICIAL-SENSITIVE is aimed at physical protection and integrity without formal accountable tracking (PDR MoD Form 102); as well as the physical protection of, and limited access to, the component. SECRET information is to be fully accounted and tracked (PDR MoD Form 102 or alike system approved by MoD).

3. The above table should be read fully before a decision is made over the classification of an individual item.

9. Disposal

4. Advice must be obtained from the authority project Security Lead before any project assets are reused, decommissioned, disposed of, or sent for repair, as they shall require security sanitisation as mandated by HMG policy.
5. Discussion with the authority project Security Lead to explore options before any decision to dispose/reuse. Components for decommissioning or disposal that have forwarded, stored and processed SUKEO data or higher, shall require overwriting with approved software, then sent for degaussing or incineration by a NCSC approved facility.
6. Components for decommissioning or disposal that have forwarded stored and processed OFFICIAL-SENSITIVE data shall require overwriting with approved software or shall require memory to be flushed; reset or powered/depowered for a specific time period.
7. Components for reuse shall only be reused at the same classification and within other parts of the MOD with consultation with CES.
8. At the end of a contract a contractor/Crown servant is to ensure that all system accounts are removed to restrict further access to the system/incidence.
9. It should be noted that the destruction of individual Hard Drives can be carried out by the Supplier following NCSC and NPSA guidance on the destruction of Classified media as well as accounting for the end of life as per MODF102/PDR.

10. Role Security Clearances

In all areas of Design, Build and Operate the clearances are the same. It is to be noted that all security clearances are to be checked and confirmed during onboarding where particular attention is to be paid on any security conditions of individuals.

Role or Position		Clearances, Checks, Nationality and Indoctrinations
C.1 Security Leads		Minimum SC
C.2 Security Officer for Contractor		Minimum SC
C.3 Technical Architect, SDA, Chief Eng, CTO		Minimum SC
C.4 CyDR Assessors		Minimum SC
C.5 System Management and administration	C.5.1 Any Supplier or Contractor that requires Privileged Access and/or Administrative Access to enable system/platform level changes, e.g., domain administrator, application administrator, etc. The principle of least privilege must be applied.	Minimum DV
	C.5.2 Authority personnel that require Privileged Access and/or Administrative Access to enable system/platform	Minimum SC

	level changes, e.g., domain administrator, application administrator, etc. The principle of least privilege must be applied.	
	C.5.3 System Manager and Administration as per C.5.1	Minimum DV
C.6 Crypto Material (Live and Pre-Prod)	C.6.1 Crypto Custodian (Live)	Minimum DV + UK Nationality only
	C.6.2 Crypto Custodian (PreProd)	Minimum DV + UK Nationality only
	C.6.3 Crypto Holder	Minimum SC
C.7 Design and Development	C.7.1 Limited access to a single HLD or LLD Design artefact for a specific purpose.	Minimum SC
	C.7.2 Regular access to HLD or LLD Design artefact.	Minimum DV
C.8 Service Design, Service Management Processes, Work Instructions		Minimum SC
C.9 Help Desk Staff	C.9.1 Support staff providing 2 nd /3 rd line technical support for applications, where no protectively marked information or design aspects are required to be disclosed (managed via 1 st line)	Minimum SC
	C.9.2 Remote support staff providing 3 rd line telephone technical support for network infrastructure.	Minimum SC or equivalent national clearance
	C.9.3 All other support staff who do not have direct administration rights over the system	Minimum BPSS or equivalent.
C.10 Development of Training material		Minimum SC
C.11 Supporting Non-functional Aspects: ARM, Safety Case, ILS (with no direct access to designs or close daily contact with wider aspects the project). 'Need-To-Know' Applies.		Minimum SC
C.12 Software applications technical consultants with limited access to systems details and no access to the live system or data. 'Need-To-Know' Applies		Minimum SC
C.13 Physical installation and build staff (power, HVAC, cabling etc – with no access to live system or data) – not data centres. 'Need-To-Know' Applies		Minimum SC
C.14 Network installation and maintenance staff (with access to live system or data) 'Need-To-Know' Applies		Minimum SC

C.15 Non-project staff with physical unescorted access to live system terminals in offices, staff attached to other projects, cleaners etc ONLY If there is no risk of observing information or them being left alone in the facility. 'Need-To-Know' Applies		Minimum SC
C.16 Migration Staff: Involved in detailed migration planning, applications and user needs etc. 'Need-To-Know' Applies		Minimum SC
C.17 Migration Staff: Managing migration as part of a site's wider IT management. e.g. Site SCIDAs, BU-POCs, TLB Leads. 'Need-To-Know' Applies		Minimum SC
C.18 Migration Staff: Conducting migration activities on the live environment.		Minimum SC
C.19 System Implementation Team: Data Centres build out, site installation inc network and comms		Minimum SC
C.20 Testers	No access to live system and data (e.g. facilities support)	Minimum SC
C.21 Project Management staff – with regular access/discussions of technical and security aspects of the solution		Minimum DV
C.22 Project, Finance, Commercial staff with limited contact and information on the wider aspects of the solution.		Minimum BPSS
C.23 In Country Senior Management and Line Managers of project staff with awareness of system name – but with no awareness of the project scope or purpose, and no direct daily engagement on programme or technical aspects.		Contractor screening
C.24 Senior Management and Line Managers of project staff with awareness of project and purpose, but no direct daily engagement on programme or technical aspects of solution.		BPSS or Contractor screening
C.25 Attendees of wider programme meetings. E.g. ASOG, CIWG, TS CCD, JRB 'Need-To-Know' Applies		Minimum SC
C.26 Attendees of Specific meetings where specific aspects are likely to be discussed e.g. Change Control Board 'NeedTo-Know' Applies		Minimum SC
C.27 Attendees of Technical and Security meeting where detailed discussion of how the system will be deployed and used occur e.g. SWG, Security Surgery.		Minimum SC
C.28 User access to system and controlled access to data (e.g. programme staff)		Minimum SC

Table 3 Role of Security Clearances

1. All project staff are bound by the guidance in Annex A, and the handling requirements of such 'Secret Materials' under JSP 440, The Defence Manual of Security and associated supplements. In some instances (such as meetings and presentations), both material marking and personnel clearance need to be considered in concert.