

Order Schedule 1 - Transparency Reports

1. The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (<https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles>)). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.
2. Without prejudice to the Supplier's reporting requirements set out in the DPS Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.
3. If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.
4. The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Performance	Service Levels and Balance Scorecard in accordance with Order Schedule 14	Presentation – Performance review	Quarterly
Order Contract Charges	Contract Prices and any incentivisation mechanisms in the Contract	Invoice	Monthly
Key Subcontractors	List of Key-Subcontractors Supply chain governance	Stand-ups & Presentation	Monthly & Quarterly
Technical	As detailed within the monthly Statement of Work	Stand-up	Weekly, and provide information within Quarterly Performance Review Meetings
Performance and underperformance management	In accordance with Order Schedule 14	Stand-up, email, Face to Face	Weekly, and provide information within Quarterly Performance Review Meetings
Resource plans	Supplier is to provide suitably qualified experienced resource to deliver the outputs, if resource becomes unavailable, the supplier must provide replacement SQEP resource within 48 hours (to be further agreed with contract manager)	Email notification to Authority of any unavailability to be further discussed and agreed with contract manager	As & When required

Order Schedule 2 - Staff Transfer

1. Definitions

1.1 In this Order Schedule 2, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Employee Liability" all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following:

- a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;
- b) unfair, wrongful or constructive dismissal compensation;
- c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;
- d) compensation for less favourable treatment of part-time workers or fixed term employees;
- e) outstanding debts and unlawful deduction of wages including any PAYE and National Insurance Contributions in relation to payments made by the Buyer or the Replacement Supplier to a Transferring Supplier Employee which would have been payable by the Supplier or the Sub-contractor if such payment should have been made prior to the Service Transfer Date and also including any payments arising in respect of pensions;
- f) claims whether in tort, contract or statute or otherwise;

any investigation by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;

"Former Supplier" a supplier supplying the Deliverables to the Buyer before the Relevant Transfer Date that are the same as or substantially similar to the Deliverables (or any part of the Deliverables) and shall include any Sub-contractor of such supplier (or any Sub-contractor of any such Sub-contractor);

"Partial Termination" the partial termination of the relevant Contract to the extent that it relates to the provision of any part of the Services as

further provided for in Clause 10.4 (When CCS or the Buyer can end this contract) or 10.6 (When the Supplier can end the contract);

"Relevant Transfer"	a transfer of employment to which the Employment Regulations applies;
"Relevant Transfer Date"	in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place, and for the purposes of Part D: Pensions, shall include the Commencement Date, where appropriate;
"Supplier's Final Supplier Personnel List"	a list provided by the Supplier of all Supplier Personnel whose will transfer under the Employment Regulations on the Service Transfer Date;
"Supplier's Provisional Supplier Personnel List"	a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier;
"Staffing Information"	<p>in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Laws), but including in an anonymised format:</p> <ul style="list-style-type: none">a) their ages, dates of commencement of employment or engagement, gender and place of work;b) details of whether they are employed, self- employed contractors or consultants, agency workers or otherwise;c) the identity of the employer or relevant contracting Party;d) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments;e) their wages, salaries, bonuses and profit-sharing arrangements as applicable;f) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;g) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);

- h) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;
- i) copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and
- j) any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations;

"Term"	the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract;
"Transferring Buyer Employees"	those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date;
"Transferring Former Supplier Employees"	in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date.

2. Interpretation

- 2.1 Where a provision in this Schedule imposes any obligation on the Supplier including (without limit) to comply with a requirement or provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Sub-contractors shall comply with such obligation and provide such indemnity, undertaking or warranty to CCS, the Buyer, Former Supplier, Replacement Supplier or Replacement Sub-contractor, as the case may be and where the Sub-contractor fails to satisfy any claims under such indemnities the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.

3. Which parts of this Schedule apply

Only the following parts of this Schedule shall apply to this Order Contract:

- Part C (No Staff Transfer On Start Date)
- Part D (Pensions)
 - - Annex D1 (CSPS)
- Part E (Staff Transfer on Exit)

Part C: No Staff Transfer on the Start Date

1. What happens if there is a staff transfer

1.1 The Buyer and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.

1.2 Subject to Paragraphs 1.3, 1.4 and 1.5, if any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Sub-contractor pursuant to the Employment Regulations then:

1.2.1 the Supplier will, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing;

1.2.2 the Buyer may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;

1.2.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;

1.2.4 if after the period referred to in Paragraph 1.2.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Supplier's compliance with Paragraphs 1.2.1 to 1.2.4:

1.2.5 the Buyer will indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in Paragraph 1.2; and

1.2.6 the Buyer will procure that the Former Supplier indemnifies the Supplier and/or any Sub-contractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 1.2.

1.3 The indemnities in Paragraph 1.2 shall not apply to any claim:

1.3.1 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees in relation to any alleged act or omission of the Supplier and/or Sub-contractor; or

1.3.2 any claim that the termination of employment was unfair because the Supplier and/or any Sub-contractor neglected to follow a fair dismissal procedure

1.4 The indemnities in Paragraph 1.2 shall not apply to any termination of employment occurring later than 3 Months from the Commencement Date.

1.5 If the Supplier and/or the Sub-contractor does not comply with

1.6 Paragraph 1.2, all Employee Liabilities in relation to such employees shall remain with the Supplier and/or the Sub-contractor and the Supplier shall (i) comply with the provisions of Part D: Pensions of this Schedule, and (ii) indemnify the Buyer and any

Former Supplier against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Sub-contractor.

2. Limits on the Former Supplier's obligations

- 2.1 Where in this Part C the Buyer accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

Part D: Pensions

1. Definitions

1.1 In this Part D, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions), and shall be deemed to include the definitions set out in the Annexes:

- "Actuary"** a Fellow of the Institute and Faculty of Actuaries;
- "Admission Agreement"** means either or both of the CSPS Admission Agreement (as defined in Annex D1: CSPS) or the LGPS Admission Agreement) as defined in Annex D3: LGPS), as the context requires;
- "Broadly Comparable"**
- a) in respect of a pension scheme, a status satisfying the condition that there are no identifiable employees who will suffer material detriment overall in terms of future accrual of pension benefits as assessed in accordance with Annex A of New Fair Deal and demonstrated by the issue by the Government Actuary's Department of a broad comparability certificate; and
 - b) in respect of benefits provided for or in respect of a member under a pension scheme, benefits that are consistent with that pension scheme's certificate of broad comparability issued by the Government Actuary's Department,
- and "Broad Comparability" shall be construed accordingly;
- "CSPS"** the schemes as defined in Annex D1 to this Part D;
- "Fair Deal Employees"** those:
- a) Transferring Buyer Employees; and/or
 - b) Transferring Former Supplier Employees; and/or
 - c) employees who are not Transferring Buyer Employees or Transferring Former Supplier Employees but to whom the Employment Regulations apply on the Relevant Transfer Date to transfer their employment to the Supplier or a Sub-contractor, and whose employment is not terminated in accordance with the provisions of Paragraphs 2.3.4 of Parts A or B or Paragraph 1.2.4 of Part C;
 - d) where the Former Supplier becomes the Supplier those employees;
- who at the Commencement Date or Relevant Transfer Date (as appropriate) are or become entitled to New Fair Deal protection in respect of any of the Statutory Schemes as notified by the Buyer;
- "Fair Deal Schemes"** means the relevant Statutory Scheme or a Broadly Comparable pension scheme;

- "Fund Actuary"** means Fund Actuary as defined in Annex D3 to this Part D;
- "LGPS"** the schemes as defined in Annex D3 to this Part D;
- "NHSPS"** the schemes as defined in Annex D2 to this Part D;
- "New Fair Deal"** the revised Fair Deal position set out in the HM Treasury guidance: "Fair Deal for Staff Pensions: Staff Transfer from Central Government" issued in October 2013 including:
- a) any amendments to that document immediately prior to the Relevant Transfer Date; and
 - b) any similar pension protection in accordance with the subsequent Annex D1-D3 inclusive as notified to the Supplier by the CCS or Buyer;
- "Statutory Schemes"** means the CSPS, NHSPS or LGPS.

2. Supplier obligations to participate in the pension schemes

- 2.1 In respect of all or any Fair Deal Employees each of Annex D1: CSPS, Annex D2: NHSPS and/or Annex D3: LGPS shall apply, as appropriate.
- 2.2 The Supplier undertakes to do all such things and execute any documents (including any relevant Admission Agreement and/or Direction Letter, if necessary) as may be required to enable the Supplier to participate in the appropriate Statutory Scheme in respect of the Fair Deal Employees and shall bear its own costs in such regard.
- 2.3 The Supplier undertakes:
- 2.3.1 to pay to the Statutory Schemes all such amounts as are due under the relevant Admission Agreement and/or Direction Letter or otherwise and shall deduct and pay to the Statutory Schemes such employee contributions as are required; and
 - 2.3.2 to be fully responsible for all other costs, contributions, payments and other amounts relating to its participation in the Statutory Schemes, including for the avoidance of doubt any exit payments and the costs of providing any bond, indemnity or guarantee required in relation to such participation.

3. Supplier obligation to provide information

- 3.1 The Supplier undertakes to the Buyer:
- 3.1.1 to provide all information which the Buyer may reasonably request concerning matters referred to in this Part D as expeditiously as possible; and
 - 3.1.2 not to issue any announcements to any Fair Deal Employee prior to the Relevant Transfer Date concerning the matters stated in this Part D without the consent in writing of the Buyer (such consent not to be unreasonably withheld or delayed).

4. Indemnities the Supplier must give

- 4.1 The Supplier undertakes to the Buyer to indemnify and keep indemnified CCS, NHS Pensions the Buyer and/or any Replacement Supplier and/or any Replacement Sub-contractor on demand from and against all and any Losses whatsoever arising out of or in connection with any liability towards all and any Fair Deal Employees arising in respect of service on or after the Relevant Transfer Date which arise from any breach by the Supplier of this Part D, and/or the CSPA Admission Agreement and/or the Direction Letter and/or the LGPS Admission Agreement or relates to the payment of benefits under and/or participation in an occupational pension scheme (within the meaning provided for in section 1 of the Pension Schemes Act 1993) or the Fair Deal Schemes.
- 4.2 The Supplier hereby indemnifies the CCS, NHS Pensions, the Buyer and/or any Replacement Supplier and/or Replacement Sub-contractor from and against all Losses suffered or incurred by it or them which arise from claims by Fair Deal Employees of the Supplier and/or of any Sub-contractor or by any trade unions, elected employee representatives or staff associations in respect of all or any such Fair Deal Employees which Losses:
- 4.2.1 relate to pension rights in respect of periods of employment on and after the Relevant Transfer Date until the date of termination or expiry of this Contract; or
 - 4.2.2 arise out of the failure of the Supplier and/or any relevant Sub-contractor to comply with the provisions of this Part D before the date of termination or expiry of this Contract.
- 4.3 The indemnities in this Part D and its Annexes:
- 4.3.1 shall survive termination of this Contract; and
 - 4.3.2 shall not be affected by the caps on liability contained in Clause 11 (How much you can be held responsible for).

5. What happens if there is a dispute

- 5.1 The Dispute Resolution Procedure will not apply to this Part D and any dispute between the CCS and/or the Buyer and/or the Supplier or between their respective actuaries or the Fund Actuary about any of the actuarial matters referred to in this Part D and its Annexes shall in the absence of agreement between the CCS and/or the Buyer and/or the Supplier be referred to an independent Actuary:
- 5.1.1 who will act as an expert and not as an arbitrator;
 - 5.1.2 whose decision will be final and binding on the CCS and/or the Buyer and/or the Supplier; and
 - 5.1.3 whose expenses shall be borne equally by the CCS and/or the Buyer and/or the Supplier unless the independent Actuary shall otherwise direct.

6. Other people's rights

- 6.1 The Parties agree Clause 19 (Other people's rights in this contract) does not apply and that the CRTPA applies to this Part D to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation owed to him or her or it by the Supplier under this Part D, in his or her or its own right under section 1(1) of the CRTPA.

6.2 Further, the Supplier must ensure that the CRTPA will apply to any Sub- Contract to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation owed to them by the Sub-contractor in his or her or its own right under section 1(1) of the CRTPA.

7. What happens if there is a breach of this Part D

7.1 The Supplier agrees to notify the Buyer should it breach any obligations it has under this Part D and agrees that the Buyer shall be entitled to terminate its Contract for material Default in the event that the Supplier:

7.1.1 commits an irremediable breach of any provision or obligation it has under this Part D; or

7.1.2 commits a breach of any provision or obligation it has under this Part D which, where capable of remedy, it fails to remedy within a reasonable time and in any event within 28 days of the date of a notice from the Buyer giving particulars of the breach and requiring the Supplier to remedy it.

8. Transferring New Fair Deal Employees

8.1 Save on expiry or termination of this Contract, if the employment of any Fair Deal Employee transfers to another employer (by way of a transfer under the Employment Regulations) the Supplier shall and shall procure that any relevant Sub-Contractor shall:

8.1.1 consult with and inform those Fair Deal Employees of the pension provisions relating to that transfer; and

8.1.2 procure that the employer to which the Fair Deal Employees are transferred (the "New Employer") complies with the provisions of this Part D and its Annexes provided that references to the "Supplier" will become references to the New Employer, references to "Relevant Transfer Date" will become references to the date of the transfer to the New Employer and references to "Fair Deal Employees" will become references to the Fair Deal Employees so transferred to the New Employer.

9. What happens to pensions if this Contract ends

9.1 The provisions of Part E: Staff Transfer On Exit (Mandatory) apply in relation to pension issues on expiry or termination of this Contract.

10. Broadly Comparable Pension Schemes

10.1 If either:

10.1.1 the terms of any of Paragraphs 2.2 of Annex D1: CSPS, 5.2 of Annex D2: NHSPS and or 4 of Annex D3: LGPS apply; and/or

10.1.2 the Buyer agrees, having considered the exceptional cases provided for in New Fair Deal, (such agreement not to be unreasonably withheld) that the Supplier (and/or its Sub- contractors, if any) need not continue to provide the Fair Deal Employees, who continue to qualify for Fair Deal Protection, with access to the appropriate Statutory Scheme;

the Supplier must (and must, where relevant, procure that each of its Sub- contractors will) ensure that, with effect from the Relevant Transfer Date or if later cessation of participation in the Statutory Scheme until the day before the Service Transfer Date, the relevant Fair Deal Employees will be eligible for membership of a pension scheme

under which the benefits are Broadly Comparable to those provided under the relevant Statutory Scheme, and then on such terms as may be decided by the Buyer.

- 10.2 Where the Supplier has set up a Broadly Comparable pension scheme or schemes pursuant to the provisions of Paragraph 10.1, the Supplier shall (and shall procure that any of its Sub-contractors shall):
- 10.2.1 supply to the Buyer details of its (or its Sub-contractor's) Broadly Comparable pension scheme and provide a full copy of the valid certificate of broad comparability covering all relevant Fair Deal Employees, as soon as it is able to do so and in any event no later than 28 days before the Relevant Transfer Date;
 - 10.2.2 fully fund any such Broadly Comparable pension scheme in accordance with the funding requirements set by that Broadly Comparable pension scheme's Actuary or by the Government Actuary's Department for the period ending on the Service Transfer Date;
 - 10.2.3 instruct any such Broadly Comparable pension scheme's Actuary to, and to provide all such co-operation and assistance in respect of any such Broadly Comparable pension scheme as the Replacement Supplier and/or CCS and/or NHS Pension and/or CSPS and/or the relevant Administering Authority and/or the Buyer may reasonably require, to enable the Replacement Supplier to participate in the appropriate Statutory Scheme in respect of any Fair Deal Employee that remain eligible for New Fair Deal protection following a Service Transfer;
 - 10.2.4 provide a replacement Broadly Comparable pension scheme with immediate effect for those Fair Deal Employees who are still employed by the Supplier and/or relevant Sub-contractor and are still eligible for New Fair Deal protection in the event that the Supplier and/or Sub-contractor's Broadly Comparable pension scheme is terminated;
 - 10.2.5 allow and make all necessary arrangements to effect, in respect of any Fair Deal Employee that remains eligible for New Fair Deal protection, following a Service Transfer, the bulk transfer of past service from any such Broadly Comparable pension scheme into the relevant Statutory Scheme and as is relevant on a day for day service basis and to give effect to any transfer of accrued rights required as part of participation under New Fair Deal. For the avoidance of doubt, should the amount offered by the Broadly Comparable pension scheme be less than the amount required by the appropriate Statutory Scheme to fund day for day service ("**Shortfall**"), the Supplier or the Sub- contractor (as agreed between them) must pay the Statutory Scheme, as required, provided that in the absence of any agreement between the Supplier and any Sub-contractor, the Shortfall shall be paid by the Supplier; and
 - 10.2.6 indemnify CCS and/or the Buyer and/or NHS Pension and/or CSPS and/or the relevant Administering Authority and/or on demand for any failure to pay the Shortfall as required under Paragraph 10.2.5 above.

Annex D1: Civil Service Pensions Schemes (CSPS)

1. Definitions

1.1 In this Annex D1: CSPS to Part D: Pensions, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"CSPS Admission Agreement" an admission agreement in the form available on the Civil Service Pensions website immediately prior to the Relevant Transfer Date to be entered into for the CSPS in respect of the Services;

"CSPS Eligible Employee" any Fair Deal Employee who at the relevant time is an eligible employee as defined in the CSPS Admission Agreement;

"CSPS" the Principal Civil Service Pension Scheme available to Civil Servants and employees of bodies under Schedule 1 of the Superannuation Act 1972 (and eligible employees of other bodies admitted to participate under a determination under section 25 of the Public Service Pensions Act 2013), as governed by rules adopted by Parliament; the Partnership Pension Account and its:

- a) Ill health Benefits Arrangements and
- b) Death Benefits Arrangements; the Civil Service Additional Voluntary Contribution Scheme; [Delete after 30 September 2018: the Designated Stakeholder Pension Scheme which is scheduled to close to new members in September 2018] and "alpha" introduced under The Public Service (Civil Servants and Others) Pensions Regulations 2014.

2. Access to equivalent pension schemes after transfer

2.1 The Supplier shall procure that the Fair Deal Employees, shall be either admitted into, or offered continued membership of, the relevant section of the CSPS that they currently contribute to, or were eligible to join immediately prior to the Relevant Transfer Date or became eligible to join on the Relevant Transfer Date and the Supplier shall procure that the Fair Deal Employees continue to accrue benefits in accordance with the provisions governing the relevant section of the CSPS for service from (and including) the Relevant Transfer Date.

2.2 The Supplier undertakes that should it cease to participate in the CSPS for whatever reason at a time when it has CSPS Eligible Employees, that it will, at no extra cost to the Buyer, provide to any Fair Deal Employee who immediately prior to such cessation of participation remained a CSPS Eligible Employee with access to a pension scheme which is Broadly Comparable to the CSPS on the date the CSPS Eligible Employees ceased to participate in the CSPS.

Part E: Staff Transfer on Exit

1. Obligations before a Staff Transfer

1.1 The Supplier agrees that within 20 Working Days of the earliest of:

1.1.1 receipt of a notification from the Buyer of a Service Transfer or intended Service Transfer;

1.1.2 receipt of the giving of notice of early termination or any Partial Termination of the relevant Contract;

1.1.3 the date which is 12 Months before the end of the Term; and

1.1.4 receipt of a written request of the Buyer at any time (provided that the Buyer shall only be entitled to make one such request in any 6 Month period),

it shall provide in a suitably anonymised format so as to comply with the Data Protection Laws, the Supplier's Provisional Supplier Personnel List, together with the Staffing Information in relation to the Supplier's Provisional Supplier Personnel List and it shall provide an updated Supplier's Provisional Supplier Personnel List at such intervals as are reasonably requested by the Buyer.

1.2 At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Buyer or at the direction of the Buyer to any Replacement Supplier and/or any Replacement Sub-contractor (i) the Supplier's Final Supplier Personnel List, which shall identify the basis upon which they are Transferring Supplier Employees and (ii) the Staffing Information in relation to the Supplier's Final Supplier Personnel List (insofar as such information has not previously been provided).

1.3 The Buyer shall be permitted to use and disclose information provided by the Supplier under Paragraphs 1.1 and 1.2 for the purpose of informing any prospective Replacement Supplier and/or Replacement Sub-contractor.

1.4 The Supplier warrants, for the benefit of The Buyer, any Replacement Supplier, and any Replacement Sub-contractor that all information provided pursuant to Paragraphs 1.1 and 1.2 shall be true and accurate in all material respects at the time of providing the information.

1.5 From the date of the earliest event referred to in Paragraph 1.1, 1.1.2 and 1.1.1, the Supplier agrees that it shall not assign any person to the provision of the Services who is not listed on the Supplier's Provisional Supplier Personnel List and shall, unless otherwise instructed by the Buyer (acting reasonably):

not replace or re-deploy any Supplier Personnel listed on the Supplier Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and expertise and is employed on the same terms and conditions of employment as the person he/she replaces not make, promise, propose, permit or implement any material changes to the terms and conditions of (i) employment and/or (ii) pensions, retirement and death benefits (including not to make pensionable any category of earnings which were not previously pensionable or reduce the pension contributions payable) of the Supplier Personnel (including any payments connected with the termination of employment);

1.5.1 not increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Personnel save for fulfilling assignments and projects previously scheduled and agreed;

- 1.5.2 not introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Supplier's Provisional Supplier Personnel List;
- 1.5.3 not increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant part of the Services);
- 1.5.4 not terminate or give notice to terminate the employment or contracts of any persons on the Supplier's Provisional Supplier Personnel List save by due disciplinary process;
- 1.5.5 not dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Buyer and/or the Replacement Supplier and/or Replacement Sub-contractor;
- 1.5.6 give the Buyer and/or the Replacement Supplier and/or Replacement Sub-contractor reasonable access to Supplier Personnel and/or their consultation representatives to inform them of the intended transfer and consult any measures envisaged by the Buyer, Replacement Supplier and/or Replacement Sub-contractor in respect of persons expected to be Transferring Supplier Employees;
- 1.5.7 co-operate with the Buyer and the Replacement Supplier to ensure an effective consultation process and smooth transfer in respect of Transferring Supplier Employees in line with good employee relations and the effective continuity of the Services, and to allow for participation in any pension arrangements to be put in place to comply with New Fair Deal;
- 1.5.8 promptly notify the Buyer or, at the direction of the Buyer, any Replacement Supplier and any Replacement Sub-contractor of any notice to terminate employment given by the Supplier or received from any persons listed on the Supplier's Provisional Supplier Personnel List regardless of when such notice takes effect;
- 1.5.9 not for a period of 12 Months from the Service Transfer Date re-employ or re-engage or entice any employees, suppliers or Sub-contractors whose employment or engagement is transferred to the Buyer and/or the Replacement Supplier (unless otherwise instructed by the Buyer (acting reasonably));
- 1.5.10 not to adversely affect pension rights accrued by all and any Fair Deal Employees in the period ending on the Service Transfer Date;
- 1.5.11 fully fund any Broadly Comparable pension schemes set up by the Supplier;
- 1.5.12 maintain such documents and information as will be reasonably required to manage the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Sub-contractor in the provision of the Services on the expiry or termination of this Contract (including without limitation identification of the Fair Deal Employees);
- 1.5.13 promptly provide to the Buyer such documents and information mentioned in Paragraph 3.1.1 of Part D: Pensions which the Buyer may reasonably request in advance of the expiry or termination of this Contract; and
- 1.5.14 fully co-operate (and procure that the trustees of any Broadly Comparable pension scheme shall fully co-operate) with the reasonable requests of the Supplier relating to any administrative tasks necessary to deal with the pension aspects of any onward transfer of any person engaged or employed

by the Supplier or any Sub-contractor in the provision of the Services on the expiry or termination of this Contract.

- 1.6 On or around each anniversary of the Effective Date and up to four times during the last 12 Months of the Term, the Buyer may make written requests to the Supplier for information relating to the manner in which the Services are organised. Within 20 Working Days of receipt of a written request the Supplier shall provide such information as the Buyer may reasonably require which shall include:
 - 1.6.1 the numbers of employees engaged in providing the Services;
 - 1.6.2 the percentage of time spent by each employee engaged in providing the Services;
 - 1.6.3 the extent to which each employee qualifies for membership of any of the Fair Deal Schemes (as defined in Part D: Pensions); and
 - 1.6.4 a description of the nature of the work undertaken by each employee by location.
- 1.7 The Supplier shall provide all reasonable cooperation and assistance to the Buyer, any Replacement Supplier and/or any Replacement Sub-contractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within 5 Working Days following the Service Transfer Date, the Supplier shall provide to the Buyer or, at the direction of the Buyer, to any Replacement Supplier and/or any Replacement Sub-contractor (as appropriate), in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:
 - 1.7.1 the most recent month's copy pay slip data;
 - 1.7.2 details of cumulative pay for tax and pension purposes;
 - 1.7.3 details of cumulative tax paid;
 - 1.7.4 tax code;
 - 1.7.5 details of any voluntary deductions from pay; and
 - 1.7.6 bank/building society account details for payroll purposes.

2. Staff Transfer when the contract ends

- 2.1 A change in the identity of the supplier of the Services (or part of the Services), howsoever arising, may constitute a Relevant Transfer to which the Employment Regulations will apply. The Buyer and the Supplier agree that where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Sub-contractor (as the case may be) and each such Transferring Supplier Employee.
- 2.2 The Supplier shall comply with all its obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (and including) the Service Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and

pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Fair Deal Schemes (as defined in Part D: Pensions).

- 2.3 Subject to Paragraph 2.4, the Supplier shall indemnify the Buyer and/or the Replacement Supplier and/or any Replacement Sub-contractor against any Employee Liabilities arising from or as a result of any act or omission of the Supplier or any Sub-contractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date.
- 2.4 The indemnity in Paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Replacement Supplier and/or any Replacement Sub-contractor whether occurring or having its origin before, on or after the Service Transfer Date.
- 2.5 Subject to Paragraphs 2.6 and 2.7, if any employee of the Supplier who is not identified in the Supplier's Final Transferring Supplier Employee List claims, or it is determined in relation to any employees of the Supplier, that his/her contract of employment has been transferred from the Supplier to the Replacement Supplier and/or Replacement Sub-contractor pursuant to the Employment Regulations then.
- 2.5.1 the Replacement Supplier and/or Replacement Sub- contractor will, within 5 Working Days of becoming aware of that fact, notify the Buyer and the Supplier in writing;
- 2.5.2 the Supplier may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Replacement Supplier and/or Replacement Sub-contractor;
- 2.5.3 if such offer of employment is accepted, the Replacement Supplier and/or Replacement Sub-contractor shall immediately release the person from its employment;
- 2.5.4 if after the period referred to in Paragraph 2.5.2 no such offer has been made, or such offer has been made but not accepted, the Replacement Supplier and/or Replacement Sub-contractor may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Replacement Supplier's and/or Replacement Sub- contractor's compliance with Paragraphs 2.5.1 to 2.5.4 the Supplier will indemnify the Replacement Supplier and/or Replacement Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Supplier's employees referred to in Paragraph 2.5.

- 2.6 The indemnity in Paragraph 2.5 shall not apply to:
- 2.6.1 any claim for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief, or equal pay or compensation for less favourable treatment of part-time workers or fixed- term employees, arising as a result of any alleged act or omission of the Replacement Supplier and/or Replacement Sub-contractor, or
- 2.6.2 any claim that the termination of employment was unfair because the Replacement Supplier and/or Replacement Sub-contractor neglected to follow a fair dismissal procedure.

- 2.7 The indemnity in Paragraph 2.5 shall not apply to any termination of employment occurring later than 3 Months from the Service Transfer Date.
- 2.8 If at any point the Replacement Supplier and/or Replacement Sub-contract accepts the employment of any such person as is described in Paragraph 2.5, such person shall be treated as a Transferring Supplier Employee and Paragraph 2.5 shall cease to apply to such person.
- 2.9 The Supplier shall promptly provide the Buyer and any Replacement Supplier and/or Replacement Sub-contractor, in writing such information as is necessary to enable the Buyer, the Replacement Supplier and/or Replacement Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Replacement Supplier and/or Replacement Sub-contractor, shall promptly provide to the Supplier and each Sub-contractor in writing such information as is necessary to enable the Supplier and each Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.
- 2.10 Subject to Paragraph 2.9, the Buyer shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Sub-contractor and its Sub-contractors against any Employee Liabilities arising from or as a result of any act or omission, whether occurring before, on or after the Service Transfer Date, of the Replacement Supplier and/or Replacement Sub-contractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee.
- 2.11 The indemnity in Paragraph 2.10 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier and/or any Sub-contractor (as applicable) whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier and/or any Sub- contractor (as applicable) to comply with its obligations under the Employment Regulations, or to the extent the Employee Liabilities arise out of the termination of employment of any person who is not identified in the Supplier's Final Supplier Personnel List in accordance with Paragraph 2.5 (and subject to the limitations set out in Paragraphs 2.6 and 2.7 above).

Order Schedule 3 – INTENTIONALLY BLANK

Order Schedule 4 - Order Tender

SUPPLIER'S TENDER RESPONSE REDACTED

Order Schedule 5 - Pricing Details

SUPPLIER'S PRICING REDACTED

PRICING PROPOSAL FOR:
701246374 (DInfoCom/0149) - Provision of ADS Security Architecture Compliance as a Service

Charging Method: Capped Time and Materials (CTM)

Table 1 - TRANSITION PERIOD (01 Jul 2021 -31 Jul 2021)							
Cyber Security Services 3 (RM3764.3)	Roles providing including minimum SFIA Level	Day Rate	T&S (If applicable) (See Para 7 of Special Notice to Suppliers)	Total	No. of resources	Total Days	Total cost Ex VAT
Cyber Security Services 3 (RM3764.3)	Security Assurance (SFIA 3)	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
Cyber Security Services 3 (RM3764.3)	Security Assurance (SFIA 4)	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
Sub Total							REDACTED

Table 2 - twenty-four (24) months, 01 Aug 2021 - 31 Jul 2023 (T&S Not Applicable)				
Cyber Security Services 3 (RM3764.3)	Roles providing including minimum SFIA Level	Day Rate	No. of resources	Total cost Ex VAT NOT TO EXCEED
Cyber Security Services 3 (RM3764.3)	Security Assurance (SFIA 3)	REDACTED	REDACTED	REDACTED
Cyber Security Services 3 (RM3764.3)	Security Assurance (SFIA 4)	REDACTED	REDACTED	

Table 3 - OPTION PERIOD (twelve (12) months, 01 Aug 2023 - 31 Jul 2024) (T&S Not Applicable)				
Cyber Security Services 3 (RM3764.3)	Roles providing including minimum SFIA Level	Day Rate	No. of resources	Total cost Ex VAT NOT TO EXCEED
Cyber Security Services 3 (RM3764.3)	Security Assurance (SFIA 3)	REDACTED	REDACTED	REDACTED
Cyber Security Services 3 (RM3764.3)	Security Assurance (SFIA 4)	REDACTED	REDACTED	

ADDITIONAL ROLES TO SUPPORT AD-HOC TASKS AS AND WHEN REQUIRED IN ACCORDANCE WITH ORDER SCHEDULE 5		
DURATION OF CONTRACT (T&S is in accordance with Appendix 1 to Order Schedule 5)		
Cyber Security Services 3 (RM3764.3)	Roles providing (including SFIA Level) (Add more rows if required)	Day rate
Cyber Security Services 3 (RM3764.3)	SFIA 3	REDACTED
Cyber Security Services 3 (RM3764.3)	SFIA 4	REDACTED
Cyber Security Services 3 (RM3764.3)	SFIA 5	REDACTED

Annex 1: Expenses Policy

UK Rail Travel

Standard Class must be selected

Accommodation

Service Mess

If your business travel has taken you onto a base and you need overnight accommodation, it may be that staying in the Service Mess is more cost efficient than a hotel; and should be considered. All military personnel should refer to **JSP 752** Pt 2 Chapter 3 for occasions in which any other form of accommodation may be considered. For civilian staff, the availability and suitability criteria for Mess accommodation is being further developed and will be included in policy guidance shortly.

Hotel

All hotel bookings must be made using the **GBT Online Portal**.

Civilian staff must comply with the approvals processes (Chapter 2). Service Personnel must have both line management and budgetary written or verbal authority before making subsistence arrangements and should note that Night Subsistence (NS) is paid for an overnight absence where there is no suitable Service accommodation provision.

All staff must consult the MOD **capped hotel rates** for spend limits in each location. The Booking Service website will raise a warning if you select a hotel exceeding the capped rate. To proceed with such a booking, you must have line manager written approval of Band D/ OF2/OR7 or above (or locally delegated budget management staff).

Exceptional circumstances where you might exceed a cap rate include: the only hotel available; an overall saving; concern as a 'lone traveller'.

Travel & Subsistence

Spend taxpayers' money responsibly.

If in doubt about what to claim, seek advice from your line manager, budget manager, or from Unit HR/Admin Staff and/ or DBS – it is best to check before you commit to expenditure. Details for military personnel is in **JSP 752**, and for civilian staff in the **Policy Rules and Guidance**.

You cannot claim for alcohol purchased whilst undertaking business travel, either as part of a meal or consumed in isolation.

Subsistence cost limits: You can claim for actual receipted expenditure, within the subsistence limits detailed below, (**not** at a flat rate). You must obtain and retain itemised receipts for all claims. If you do not have a receipt you will need auditable line manager approval, e.g. by email, before you claim, and you must keep the approval.

Over 5 hours **£5.00**

Over 10 hours **£10.00**

Over 12 hours **£15.00**

Evening Meal **£22.50** (overnight stay)

Breakfast* **£10.00**

* when not included in the hotel/B&B rate

Motor Mileage Allowance (MMA) – UK

There are a number of different rates which are related to UK vehicle travel:

- Motor Mileage Allowance (up to 10,000 miles) 30p per mile
- Motor Mileage Allowance (over 10,000 miles) 25p per mile
- Motorcycle 24p per mile
- Pedal cycle 15p per mile
- Passenger Supplement 3p per mile for first passenger; 2p per mile for second and additional passengers
- Equipment Supplement 2p per mile (taxable)
- Excess Fares Allowance 30p per mile

Home to Duty Liability

The Home To Duty Liability (HTDL) is the travel cost incurred getting to/from your normal place of work. This should be deducted from expenses incurred when undertaking business travel to/from the home and a business location. This deduction does not apply to travel between business locations.

Using a Private Vehicle is probably the easiest application. If you normally drive to work and use your vehicle for business travel, then your Motor Mileage Allowance claim should have a deduction commensurate with the normal mileage to work. So, if you normally travel 10 miles to/from your normal place of work (total 20 miles) and drive 30 miles to/from a business location (total 60 miles), the claim should be reduced by 20 miles. This results in a net MMA claim of 40 miles. The deduction only applies to travel to/from the home and business location; not between your normal work place and business location(s).

Order Schedule 6 - ICT Services

1. Definitions

1.1 In this Order Schedule 6, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Buyer Software"	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
"Buyer System"	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Order Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
"Commercial off the shelf Software" or "COTS Software"	non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms;
"Defect"	any of the following: <ol style="list-style-type: none">any error, damage or defect in the manufacturing of a Deliverable; orany error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; orany failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Order Contract; orany failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Order Contract;
"ICT Environment"	the Buyer System and the Supplier System;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Order Contract, including any COTS Software;
"New Release"	an item produced primarily to extend, alter or

	improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"Open Source Software"	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or c) where any part of the Supplier System is situated;
"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Order Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 8.1 of this Schedule;
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
"Supplier System"	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

2.1 This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT services which are part of the Deliverables.

3. Buyer due diligence requirements

3.1 The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

3.1.1 suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;

3.1.2 operating processes and procedures and the working methods of the Buyer;

3.1.3 ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

3.1.4 existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

3.2 The Supplier confirms that it has advised the Buyer in writing of:

3.2.1 each aspect, if any, of the Operating Environment that is not suitable for the provision of the Deliverables;

3.2.2 the actions needed to remedy each such unsuitable aspect; and

3.2.3 a timetable for and the costs of those actions.

4. Software warranty

4.1 The Supplier represents and warrants that:

4.1.1 it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub- Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Order Contract including the receipt of the Deliverables by the Buyer;

4.1.2 all components of the Specially Written Software shall:

(a) be free from material design and programming errors;

(b) perform in all material respects in accordance with the relevant specifications and Documentation; and

(c) not infringe any IPR.

5. Provision of ICT Services

5.1 The Supplier shall:

5.1.1 ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with any interface requirements of the Buyer specified in this Order Contract and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

- 5.1.2 ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
- 5.1.3 ensure that the Supplier System will be free of all encumbrances;
- 5.1.4 ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Order Contract;
- 5.1.5 minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

- 6.1 The Supplier shall, where specified by the Buyer as part of their Order Procedure, and in accordance with agreed timescales, develop quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").
- 6.2 The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.
- 6.3 Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
- 6.4 The Supplier shall ensure that the Supplier Personnel shall at all times during the Order Contract Period:
 - 6.4.1 be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Order Contract;
 - 6.4.2 apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and
 - 6.4.3 obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

- 7.1 The Supplier shall allow any auditor access to the Supplier premises to:
 - 7.1.1 inspect the ICT Environment and the wider service delivery environment (or any part of them);
 - 7.1.2 review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
 - 7.1.3 review the Supplier's quality management systems including all relevant Quality Plans.

8. Intellectual Property Rights in ICT

8.1 Assignments granted by the Supplier: Specially Written Software

8.1.1 The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

- (a) the Documentation, Source Code and the Object Code of the Specially Written Software; and
- (b) all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

8.1.2 The Supplier shall:

- (a) inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
- (b) deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and
- (c) without prejudice to paragraph 8.1.2(c), provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

8.1.3 The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

8.2 Licences for non-COTS IPR from the Supplier and third parties to the Buyer

8.2.1 Unless the Buyer gives its Approval the Supplier must not use any:

- (a) of its own Existing IPR that is not COTS Software;
- (b) third party software that is not COTS Software

8.2.2 Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a

Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Order Contract Period and after expiry of the Order Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

- 8.2.3 Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 8.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:
- (a) notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and
 - (b) only use such third party IPR as referred to at paragraph
 - (c) 8.2.3(a) if the Buyer Approves the terms of the licence from the relevant third party.
- 8.2.4 Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 8.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.
- 8.2.5 The Supplier may terminate a licence granted under paragraph 8.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.
- 8.3 Licenses for COTS Software by the Supplier and third parties to the Buyer
- 8.3.1 The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 8.3.2 Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 8.3.3 Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 8.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 8.3.4 The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:
- (a) will no longer be maintained or supported by the developer; or
 - (b) will no longer be made commercially available.
- 8.4 Buyer's right to assign/novate licences

- 8.4.1 The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 8.2 (to:
- (a) a Central Government Body; or
 - (b) to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.
- 8.4.2 If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 8.2.
- 8.5 Licence granted by the Buyer
- 8.5.1 The Buyer grants to the Supplier a licence to use the Specially Written Software:
- (a) during the Order Contract Period for the purpose of fulfilling its obligations under the Order Contract, and
 - (b) after the Contract period on the terms set out in the Open Government Licence.
- 8.5.2 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub- licences to Sub-Contractors provided that any relevant Sub- Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).
- 8.6 Open Source Publication
- 8.6.1 Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 8.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:
- (a) suitable for publication by the Buyer as Open Source; and
 - (b) based on Open Standards (where applicable),
- and the Buyer may, at its sole discretion, publish the same as Open Source.
- 8.6.2 The Supplier hereby warrants that the Specially Written Software and the New IPR:
- (a) are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;
 - (b) have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;
 - (c) do not contain any material which would bring the Buyer into disrepute;

- (d) can be published as Open Source without breaching the rights of any third party;
- (e) will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and
- (f) do not contain any Malicious Software.

8.6.3 Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

- (a) as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and
- (b) include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9. Supplier-Furnished Terms

9.1 Software Licence Terms:

- 9.1.1 Terms for licensing of non-COTS third party software in accordance with Paragraph 8.2.3 are detailed in Annex A of this Order Schedule 6.
- 9.1.2 Terms for licensing of COTS software in accordance with Paragraph 8.3 are detailed in Annex B of this Order Schedule 6.

Annex A: Non-COTS Third Party Software Licensing Terms – N/A

Annex B: COTS Licensing Terms – N/A

Order Schedule 7 - Key Supplier Staff

1. The Annex 1 to this Schedule lists the key roles (“**Key Roles**”) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
2. The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
3. The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
4. The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
 - 4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 4.2 the person concerned resigns, retires or dies or is on maternity or long- term sick leave; or
 - 4.3 the person’s employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
5. The Supplier shall:
 - 5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
 - 5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
 - 5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff’s employment contract, this will mean at least 3 Months’ notice;
 - 5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and
 - 5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.
6. The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Annex 1: Key Roles

Key Role	Key Staff	Contact Details
Architecture Compliance Service – senior representative	REDACTED	REDACTED
Architecture Compliance Service – consultant	REDACTED	REDACTED
Architecture Compliance Service – consultant	REDACTED	REDACTED
Actica Project Director	REDACTED	REDACTED

Order Schedule 8 - Business Continuity and Disaster Recovery

1. Definitions

1.1 In this Order Schedule 8, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"BCDR Plan"	has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	has the meaning given to it in Paragraph 6.2 of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

2.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan ("**BCDR Plan**"), which shall detail the processes and arrangements that the Supplier shall follow to:

2.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

2.2.2 the recovery of the Deliverables in the event of a Disaster

2.3 The BCDR Plan shall be divided into three sections:

2.3.1 Section 1 which shall set out general principles applicable to the BCDR Plan;

2.3.2 Section 2 which shall relate to business continuity ("**Business Continuity Plan**"); and

2.3.3 Section 3 which shall relate to disaster recovery ("**Disaster Recovery Plan**").

2.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are

unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3. General Principles of the BCDR Plan (Section 1)

3.1 Section 1 of the BCDR Plan shall:

- 3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
- 3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;
- 3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;
- 3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;
- 3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;
- 3.1.6 contain a risk analysis, including:
 - (a) failure or disruption scenarios and assessments of likely frequency of occurrence;
 - (b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
 - (c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
 - (d) a business impact analysis of different anticipated failures or disruptions;
- 3.1.7 provide for documentation of processes, including business processes, and procedures;
- 3.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;
- 3.1.9 identify the procedures for reverting to "normal service"; set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;
- 3.1.10 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and
- 3.1.11 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

3.2 The BCDR Plan shall be designed so as to ensure that:

- 3.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;
 - 3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;
 - 3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and
 - 3.2.4 it details a process for the management of disaster recovery testing.
- 3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.
- 3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service Levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4. Business Continuity (Section 2)

- 4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:
- 4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and
 - 4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.
- 4.2 The Business Continuity Plan shall:
- 4.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;
 - 4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;
 - 4.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and
 - 4.2.4 set out the circumstances which the Business Continuity Plan is
 - 4.2.5 invoked.

5. Disaster Recovery (Section 3)

- 5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

- 5.2.1 loss of access to the Buyer Premises;
- 5.2.2 loss of utilities to the Buyer Premises;
- 5.2.3 loss of the Supplier's helpdesk or CAFM system;
- 5.2.4 loss of a Subcontractor;
- 5.2.5 emergency notification and escalation process;
- 5.2.6 contact lists;
- 5.2.7 staff training and awareness;
- 5.2.8 BCDR Plan testing;
- 5.2.9 post implementation review process;
- 5.2.10 any applicable Performance Indicators with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;
- 5.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
- 5.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and testing and management arrangements.

6. Review and changing the BCDR Plan

- 6.1 The Supplier shall review the BCDR Plan:
 - 6.1.1 on a regular basis and as a minimum once every six (6) Months;
 - 6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph Error! Reference source not found.; and
 - 6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.
- 6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.
- 6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report ("**Review Report**") setting out

the Supplier's proposals ("**Supplier's Proposals**") for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

- 6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

7. Testing the BCDR Plan

- 7.1 The Supplier shall test the BCDR Plan:
- 7.1.1 regularly and in any event not less than once in every Contract Year;
 - 7.1.2 in the event of any major reconfiguration of the Deliverables;
 - 7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).
- 7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.
- 7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.
- 7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.
- 7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:
- 7.5.1 the outcome of the test;
 - 7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and
 - 7.5.3 the Supplier's proposals for remedying any such failures.
- 7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8. Invoking the BCDR Plan

- 8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such

invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

9. Circumstances beyond your control

- 9.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

Order Schedule 9 – Security

Part A: Short Form Security Requirements – N/A

Part B: Long Form Security Requirements

1. Definitions

1.1 In this Part B to Order Schedule 9 the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	means the occurrence of: <ul style="list-style-type: none">a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/orb) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
"ISMS"	the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
"Security Tests"	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

2.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

- 2.3.1 Maj Steve Gibbs, Steven.Gibbs794@mod.gov.uk.
 - 2.3.2 Paul Allen, Director, paul.allen@actica.co.uk
 - 2.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.
 - 2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.
 - 2.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.
 - 2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.
 - 2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.
- 3. Information Security Management System (ISMS)**
- 3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.5.
 - 3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.
 - 3.3 The Buyer acknowledges that;
 - 3.3.1 If the Buyer has not stipulated during an Order Procedure that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and
 - 3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.
 - 3.4 The ISMS shall:
 - 3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;
 - 3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;
 - 3.4.3 at all times provide a level of security which:

- (a) is in accordance with the Law and this Contract;
 - (b) complies with the Baseline Security Requirements;
 - (c) as a minimum demonstrates Good Industry Practice;
 - (d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
 - (e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework(Tiers1-4) (<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>)
 - (f) takes account of guidance issued by the Centre for Protection of National Infrastructure <https://www.cpni.gov.uk/>
 - (g) complies with HMG Information Assurance Maturity Model and Assurance Framework (<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>);
 - (h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
 - (i) addresses issues of incompatibility with the Supplier's own organisational security policies; and
 - (j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;
- 3.4.4 document the security incident management processes and incident response plans;
- 3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and
- 3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).
- 3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
- 3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.
- 3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and

maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

- 3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

- 4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4.3 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

- 4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3(d), the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

- 4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);
 - 4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;
 - 4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;
 - 4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and
 - 4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.
- 4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non- approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.
- 4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.
- 5. Amendment of the ISMS and Security Management Plan**
- 5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:
- 5.1.1 emerging changes in Good Industry Practice;
 - 5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
 - 5.1.3 any new perceived or changed security threats;
 - 5.1.4 where required in accordance with paragraph 3.4.3(d), any changes to the Security Policy;
 - 5.1.5 any new perceived or changed security threats; and
 - 5.1.6 any reasonable change in requirement requested by the Buyer.

- 5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:
- 5.2.1 suggested improvements to the effectiveness of the ISMS;
 - 5.2.2 updates to the risk assessments;
 - 5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
 - 5.2.4 suggested improvements in measuring the effectiveness of controls.
- 5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.
- 5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

- 6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
- 6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.
- 6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.
- 6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to

make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

- 6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

- 7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3.

- 7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

- 7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

- 8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

- 8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

- (a) minimise the extent of actual or potential harm caused by any Breach of Security;
- (b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;
- (c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the

Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

- (d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
- (e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and
- (f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST <http://nvd.nist.gov/cvss.cfm>); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had

- followed and continues to follow the security patch test plan agreed with the Buyer; or
- 9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.
- 9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:
- 9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or
- 9.4.2 is agreed with the Buyer in writing.
- 9.5 The Supplier shall:
- 9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;
- 9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
- 9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;
- 9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.4.5;
- 9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;
- 9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;
- 9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and
- 9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.
- 9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.
- 9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1: Baseline security requirements

1. Handling Classified information

- 1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

- 2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

- 2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (<https://www.ncsc.gov.uk/guidance/end-user-device-security>). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

- 3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

- 3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

- 3.3 The Supplier shall:

- 3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;
- 3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
- 3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
- 3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

- 4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has

been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA.

- 4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

- 5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.
- 5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (<https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

- 6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
- 6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.
- 6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
- 6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
- 6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

- 7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

- 8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to

facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

- 8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.
- 8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
- 8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
- 8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2: Security Management Plan

JSP 440, The Defence Manual of Security, Resilience and Business Continuity.

JSP 604, Defence Manual for Information and Communications Technology (ICT).

JSP 740, Acceptable Use Policy (AUP) for Information and Communications Technology (ICT).

UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

REDACTED

Cyber Implementation Plan

Contract Title:	Provision of Security Architecture Compliance as a Service (SACaaS)
MOD Contract Number:	701246374 (DInfoCom/0149)
CSM Risk Acceptance Reference:	RAR-ABSG3NZU
CSM Cyber Risk Level:	High
Name of Supplier (to be shared with the MOD only):	Actica Consulting
Current Level of Supplier Compliance:	Cyber Essentials Plus (REDACTED)
Reasons why Supplier is unable to achieve full compliance:	Not applicable
Measures planned to achieve compliance/ mitigate the risk with associated dates:	Not applicable
Anticipated date of compliance/mitigations will be in place:	Not applicable
Current Cyber Essential Plus Certification No:	REDACTED
Expiry Date:	29 January 2022
Renewal certification to be issued to the Authority:	Annually until expiration of the Contract
Name:	Matthew Gibson
Position:	Director
Date:	01 June 2021

Order Schedule 10 - Exit Management

1. Within 20 (twenty) working days of the Start Date the Supplier must provide for the Buyer's Approval an exit plan which ensures continuity of service and which the Supplier will follow at the end of the Order Contract. The Buyer shall not unreasonably withhold Approval of the draft provided that the Supplier shall incorporate the Buyer's reasonable requirements in it
2. The Supplier must ensure that the exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its Replacement Supplier at the expiry or if the Order Contract ends before the scheduled expiry.
3. The exit plan should set out full details of timescales, activities and roles and responsibilities of the Parties for:
 - 3.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier;
 - 3.2 the strategy for export and migration of Buyer data from any relevant Supplier system to the Buyer or a Replacement Supplier, including conversion to open standards or other standards required by the Buyer;
 - 3.3 the transfer of New IPR items to the Buyer or a Replacement Supplier;
 - 3.4 the testing and assurance strategy for exported Buyer data;
 - 3.5 if relevant, TUPE-related activity to comply with the TUPE regulations;
 - 3.6 any other activities and information which are reasonably required to ensure continuity of service during the exit period and an orderly transition to the Buyer or a Replacement Supplier.

Order Schedule 11 – INTENTIONALLY BLANK

Order Schedule 12 – INTENTIONALLY BLANK

Order Schedule 13 – Implementation Plan and Testing – N/A

Order Schedule 14 - Service Levels

1. Definitions

1.1 In this Order Schedule 14, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Critical Service Failure" Means a failure to meet a Service Level Threshold in respect of a Service Level

"Service Credits" any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;

"Service Credit Cap" has the meaning given to it in the Order Form;

"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. What happens if you don't meet the Service Levels

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 of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.

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 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2 the Service Level Failure:

- (a) exceeds the relevant Service Level Threshold;
- (b) has arisen due to a Prohibited Act or wilful Default by the Supplier;
- (c) results in the corruption or loss of any Government Data; and/or

(d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

2.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

3. Critical Service Level Failure

3.1 On the occurrence of a Critical Service Level Failure:

3.1.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.1.2 the Buyer shall (subject to the Service Credit Cap) 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.

Part A: Service Levels and Service Credits

1. Service Levels

1.1 If the level of performance of the Supplier:

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

1.1.2 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:

- (a) require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
- (b) instruct the Supplier to comply with the Rectification Plan Process;
- (c) if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
- (d) 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. Service Credits

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

Annex A to Part A: Services Levels and Service Credits Table

Service Level Performance Criteria	Key Indicator	Service Level Performance Measure	Service Level Threshold	Service Credit for each Service Period
Provision of two resources This measures the availability of the contracted resource as per Order Schedule 20 - Order Specification	Availability of resource to supply service	99% of contracted days (where contracted SAC resources are agreed to be working for SAC) are fulfilled as per SoW.	95%	1% Service Credit gained for each 0.5 percentage under the specified Service Level Performance Measure

The Service Credits shall be calculated on the basis of the following formula:

Formula:

$$\begin{aligned}
 &x\% \text{ (Service Level Performance Measure)} - \\
 &x\% \text{ (actual Service Level performance)}
 \end{aligned}
 =
 \begin{aligned}
 &x\% \text{ of the Charges payable to the Buyer} \\
 &\text{as Service Credits to be deducted from} \\
 &\text{the next Invoice payable by the Buyer}
 \end{aligned}$$

Worked example:

$$\begin{aligned}
 &98\% \text{ (e.g. Service Level} \\
 &\text{Performance Measure requirement for} \\
 &\text{accurate and timely billing Service Level)} - \\
 &75\% \text{ (e.g. actual performance achieved} \\
 &\text{against this Service Level in a Service} \\
 &\text{Period)}
 \end{aligned}
 =
 \begin{aligned}
 &23\% \text{ of the Charges payable to the} \\
 &\text{Buyer as Service Credits to be} \\
 &\text{deducted from the next Invoice payable} \\
 &\text{by the Buyer}
 \end{aligned}$$

In relation to **Delivery of Monthly outputs against Statement of Work** a Critical Service Level Failure shall include a delay in producing **the required monthly tasks** ordered by the Customer in excess of **that month** more than once in any **three (3) month** period.

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 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, 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 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;
 - 1.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
 - 1.2.6 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. 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 and time (within normal business hours) as the Buyer shall reasonably require;
 - 1.3.2 be attended by the Supplier's Representative and the Buyer's 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 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 Representative and the Buyer's 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 and the calculations of the amount of Service Credits 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.

Order Schedule 15 - Order Contract Management

1. Definitions

1.1 In this Order Schedule 15, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Operational Board"	the board established in accordance with paragraph 5.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be the delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Contract Risk Management

4.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Order Contract.

4.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

- 4.2.1 the identification and management of risks;
 - 4.2.2 the identification and management of issues; and
 - 4.2.3 monitoring and controlling project plans.
- 4.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 4.4 The Supplier will maintain a risk register of the risks relating to the Order Contract which the Buyer and the Supplier have identified.

5. Role of the Operational Board

- 5.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.
- 5.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.
- 5.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.
- 5.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.
- 5.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

- **Weekly:** Stand-Ups. **Attendance:** Delivery Team Leader and Supplier
- **Monthly:** Review of delivered statement of Work – **Attendance:** Delivery Team Leader and Supplier
- **Quarterly:** Performance Review Meetings – **Attendance:** Finance, Commercial, Delivery Team Leader and Supplier

Order Schedule 16 – INTENTIONALLY BLANK

Order Schedule 17 - MOD Terms

1. Definitions

1.1 In this Order Schedule 17, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"MOD Terms and Conditions" the terms and conditions listed in this Schedule;

"MOD Site" shall include any of Her Majesty's Ships or Vessels and Service Stations;

"Officer in charge" shall include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Officers superintending Government Establishments;

2. Access to MOD sites

2.1 The Buyer shall issue passes for those representatives of the Supplier who are approved for admission to the MOD Site and a representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Buyer and shall be surrendered on demand or on completion of the supply of the Deliverables.

2.2 The Supplier's representatives when employed within the boundaries of a MOD Site, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force for the time being for the conduct of staff at that MOD Site. When on board ship, compliance shall be with the Ship's Regulations as interpreted by the Officer in charge. Details of such rules, regulations and requirements shall be provided, on request, by the Officer in charge.

2.3 The Supplier shall be responsible for the living accommodation and maintenance of its representatives while they are employed at a MOD Site. Sleeping accommodation and messing facilities, if required, may be provided by the Buyer wherever possible, at the discretion of the Officer in charge, at a cost fixed in accordance with current Ministry of Defence regulations. At MOD Sites overseas, accommodation and messing facilities, if required, shall be provided wherever possible. The status to be accorded to the Supplier's staff for messing purposes shall be at the discretion of the Officer in charge who shall, wherever possible give his decision before the commencement of this Contract where so asked by the Supplier. When sleeping accommodation and messing facilities are not available, a certificate to this effect may be required by the Buyer and shall be obtained by the Supplier from the Officer in charge. Such certificate shall be presented to the Buyer with other evidence relating to the costs of this Contract.

2.4 Where the Supplier's representatives are required by this Contract to join or visit a Site overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided for them free of charge by the Ministry of Defence whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Supplier shall make such arrangements through the Technical Branch named for this purpose in the Buyer Contract Details. When such transport is not available within a reasonable time, or in circumstances where the Supplier wishes its representatives to accompany material for installation which it is to arrange to be delivered, the Supplier shall make its own transport arrangements. The Buyer shall reimburse the Supplier's reasonable costs for such transport of its representatives on presentation of evidence supporting the use of alternative transport and of the costs involved. Transport of the Supplier's representatives locally overseas which is

necessary for the purpose of this Contract shall be provided wherever possible by the Ministry of Defence, or by the Officer in charge and, where so provided, shall be free of charge.

- 2.5 Out-patient medical treatment given to the Supplier's representatives by a Service Medical Officer or other Government Medical Officer at a Site overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Site and transportation of the Supplier's representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Supplier at rates fixed in accordance with current Ministry of Defence regulations.
- 2.6 Accidents to the Supplier's representatives which ordinarily require to be reported in accordance with Health and Safety at Work etc. Act 1974, shall be reported to the Officer in charge so that the Inspector of Factories may be informed.
- 2.7 No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the Supplier's representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current Ministry of Defence rates.
- 2.8 The Supplier shall, wherever possible, arrange for funds to be provided to its representatives overseas through normal banking channels (e.g. by travellers' cheques). If banking or other suitable facilities are not available, the Buyer shall, upon request by the Supplier and subject to any limitation required by the Supplier, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made at the Site to which the Supplier's representatives are attached. All such advances made by the Buyer shall be recovered from the Supplier

3. DEFCONS and DEFFORMS

- 3.1 The DEFCONS and DEFFORMS listed in Annex 1 to this Schedule are incorporated into this Contract.
- 3.2 In the event of a conflict between any DEFCONS and DEFFORMS listed in the Order Form and the other terms in an Order Contract, the DEFCONS and DEFFORMS shall prevail.

Annex 1: DEFCONS & DEFFORMS

The full text of Defence Conditions (DEFCONS) and Defence Forms (DEFFORMS) are available electronically via <https://www.gov.uk/acquisition-operating-framework>.

The following MOD DEFCONS and DEFFORMs form part of this contract:

DEFCONS

DEFCON No	Version	Description
DEFCON 5J	18/11/16	Unique Identifiers
DEFCON 76	12/06	Contractors Personnel at Government Establishments
DEFCON 129J	18/11/16	The Use of Electronic Business Delivery Form
DEFCON 513	11/16	Value Added Tax
DEFCON 514	08/15	Material Breach
DEFCON 515	02/17	Bankruptcy and Insolvency
DEFCON 516	04/12	Equality
DEFCON 518	02/17	Transfer
DEFCON 520	05/18	Corrupt Gifts and Payments of Commission
DEFCON 522	11/17	Payment and Recovery of Sums Due
DEFCON 526	08/02	Notices
DEFCON 527	09/97	Waiver
DEFCON 528	09/97	Law (English)
DEFCON 531	11/14	Disclosure of Information
DEFCON 532B & Deform 532	04/20	Protection of Personal Data (Where Personal Data is being processed on behalf of the Authority)
DEFCON 534	06/17	Subcontracting and Prompt Payment
DEFCON 537	06/02	Rights of Third Parties
DEFCON 539	08/13	Transparency
DEFCON 550	02/14	Child Labour and Employment Law
DEFCON 566	10/20	Change of Control of Contractor
DEFCON 602B	12/06	Quality Assurance (without Quality Plan)
DEFCON 604	06/14	Progress Reports
DEFCON 611	02/16	Issued Property
DEFCON 625	10/98	Co-operation on Expiry of Contract
DEFCON 632	08/12	Third Party Intellectual Property – Rights and Restrictions

DEFCON 642	06/14	Progress Meetings
DEFCON 658	10/17	Cyber Note: Further to DEFCON 658 the Cyber Risk Profile of the Contract is High as defined in DEF-STAN 05-138
DEFCON 659A	02/17	Security Measures
DEFCON 660	12/15	Official Sensitive Security Requirements
DEFCON 694	07/18	Accounting For Property Of The Authority

DEFFORMs (Ministry of Defence Forms)

DEFFORM No	Version	Description

Order Schedule 18 - Background Checks

1. When you should use this Schedule

- 1.1 This Schedule should be used where Supplier Staff must be vetted before working on the Contract.

2. Definitions

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

“Relevant Conviction” means any conviction listed in Annex 1 to this Schedule.

3. Relevant Convictions

- 3.1 The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

- 3.2 Notwithstanding Paragraph 3.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

3.2.1 carry out a check with the records held by the Department for Education (DfE);

3.2.2 conduct thorough questioning regarding any Relevant Convictions; and

3.2.3 ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub- Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1: Relevant Convictions

Any conviction passed in a Court of Law.

Order Schedule 19 - Scottish Law – N/A

Order Schedule 20 - Order Specification

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Order Contract.

1. OUTCOME

- 1.1 The Army Digital Services (ADS) 'Security Architecture Compliance as a Service' (SACaaS) will provide a cost effective, flexible and scalable security architecture, compliance and information assurance service that can meet the demands of the ADS Programme. Working alongside the existing in-house team, this "as a Service" will provide the capability to fulfil the service support wrapper outputs and allow veering and hauling to react quickly to changing requirements.

2. PURPOSE

- 2.1 The MoD may be referred to as "the Authority" hereafter.
- 2.2 The purpose of this document is to define the Security Architecture Compliance as a Service (SACaaS) services required by ADS. This is inclusive of, but not limited to:
 - 2.2.1 Ensure all ADS services are coherent with MoD Policy.
 - 2.2.2 Risk Management and Audit capabilities.
 - 2.2.3 Accreditation work relating to hosting environments and hosted applications.
 - 2.2.4 Compliance and information assurance in line with Defence Security and Compliance policy and practices

3. SOR COMPOSITION

- 3.1 This document is split into three schedules:
 - 3.1.1 Schedule 1 - Background to the ADS Organisation.
 - 3.1.2 Schedule 2 - The Services required.
 - 3.1.3 Schedule 3 - The Service levels required.

4. HARDWARE AND SOFTWARE INFRASTRUCTURE PROCUREMENT

- 4.1 The Authority will be responsible for procurement of all the IT assets and equipment required to support this requirement.

5. INTELLECTUAL PROPERTY RIGHTS (IPR)

- 5.1 The selected Supplier shall not retain IPR relating to any services delivered during the terms of the contract.

6. LICENCING AND SUPPORT AGREEMENTS

- 6.1 The Authority will retain the overall responsibility for ensuring that all system software utilised by the Service Supplier on behalf of the Authority is fully licenced with the provider.

7. EXIT PLAN

- 7.1 The Authority and the Supplier will agree an exit plan during the Call-Off Contract period to enable the Supplier Deliverables to be transferred to the Authority ensuring that the Authority has all the documentation required to support and continuously develop the Service with Authority resource or any third party as the Authority requires. The Supplier will update this plan whenever there are material changes to the Services. A Statement of Work (SoW) may be agreed between the Authority and the Supplier to specifically cover the exit plan.

8. DURATION

- 8.1 The duration of the overall requirement is for a twenty-four (24) month period, from 01 Aug 2021 until 31 Jul 2023, with a twelve (12) month option period.

SCHEDULE 1 – BACKGROUND TO THE ADS ORGANISATION

9. OVERVIEW

- 9.1 This following section is designed to provide information, for context, on the structure, organisation, processes and remit of the Authority. It is therefore broader than the specific needs of this contract which are detailing in the following schedules.
- 9.2 ADS provides hosting and through life application-based information services to the Army and wider Defence; predominantly through web applications accessible either on the intranet or on Defence infrastructure. It comprises of a core of 100+ personnel across military, Civil Servants (CS) and core Technical Support staff which includes elements from 605 Signal Troop (10 Signal Regiment) that directly support ADS. This figure increases when new products are in delivery.
- 9.3 ADS provides hosting capability across three security domains in the form of Official, Official-Sensitive and Secret. The official domain is provided by the Joint Server Farm (JSF) capability and is currently provided under a G-Cloud contract. In the Official-Sensitive and Secret environments, ADS provides the hosting platform (hardware and software) in the form of a private cloud; known as the Army Hosting Environment (AHE). The landscape of ADS hosting capability is as detailed on Page 6, Figure 1. In addition to these hosting capabilities, some aspects of the pipeline for delivery onto both the JSF and AHE are in Microsoft Azure, enabling remote access to the product teams.

10. THE ARMY HOSTING ENVIRONMENT (AHE)

- 10.1 The AHE is a 'private cloud' located on MOD premises that currently supports 70+ business applications across multiple security classifications. In the Official-Sensitive and Secret environments, this is connected to the military WAN. ADS provides the hosting platform in the form of a fully Software Defined Data Centre (SDDC) (using VMware technology) to enable applications to be accessed from a web browser on Defence Information Infrastructure (DII) at Secret and MODNET at Official-Sensitive.
- 10.2 The applications hosted on AHE support a wide range of functions across HR, logistics, intelligence, finance, command and control. These include a number of applications that have been developed by ADS on behalf of the Field Army, the more significant ones of which include:
- 10.2.1 CHURCHILL - an event scheduling application;
 - 10.2.2 OPUS - a single tasking mechanism;
 - 10.2.3 MUSTER - a personnel deployability tool;
 - 10.2.4 MARSHAL - an equipment availability tool;
 - 10.2.5 Reserve Attendance and Pay Service - a Reserve Army management system;
 - 10.2.6 TARGET - an individual training management system; and
 - 10.2.7 MyMUSTER - a system which reports on individual readiness to soldiers.
- 10.3 More broadly there are currently 70+ live application services on the Official-Sensitive, of which 25+ are Oracle APEX, 8 are .Net, 2 utilising Software AG technology and the remainder are Commercial Off the Shelf (COTS). The COTS products include Microsoft Customer Relationship Management (CRM) Dynamics, SharePoint and Remedy which are configured

to meet the requirements of the users. Other COTS products are used in the form of ResourceLink to pay civilian employees in the Army.

- 10.4 The Army also has a significant Management Information (MI) and Business Information (BI) capability in the form of the Army Data Warehouse (ADW) utilising Oracle Business Intelligence Enterprise Edition (OBIEE) and Statistical Analysis Software (SAS) ~~VYA~~ to provide reporting and analytics across the Army. On Secret, there are 6 application services. This is anticipated to grow due to the lack of Secret hosting facilities across Defence.
- 10.5 Application users range from a handful for some of the more specialist applications to tens of thousands for those widely used across the Army and pan Defence, including the RAF, Navy and Defence Equipment & Support (DE&S).
- 10.6 ADS is now moving to an Application Programming Interface (API) first strategy based on services from the system of records mediated through an API Gateway. As applications are being improved or delivered the opportunity is being taken to break down existing applications into their component parts and delivered as business services.
- 10.7 ADS are also looking into the use of public cloud to include VMC on AWS with a view to deliver a Hybrid Cloud allowing centralised management and interoperability between applications and services that bridge security domains.

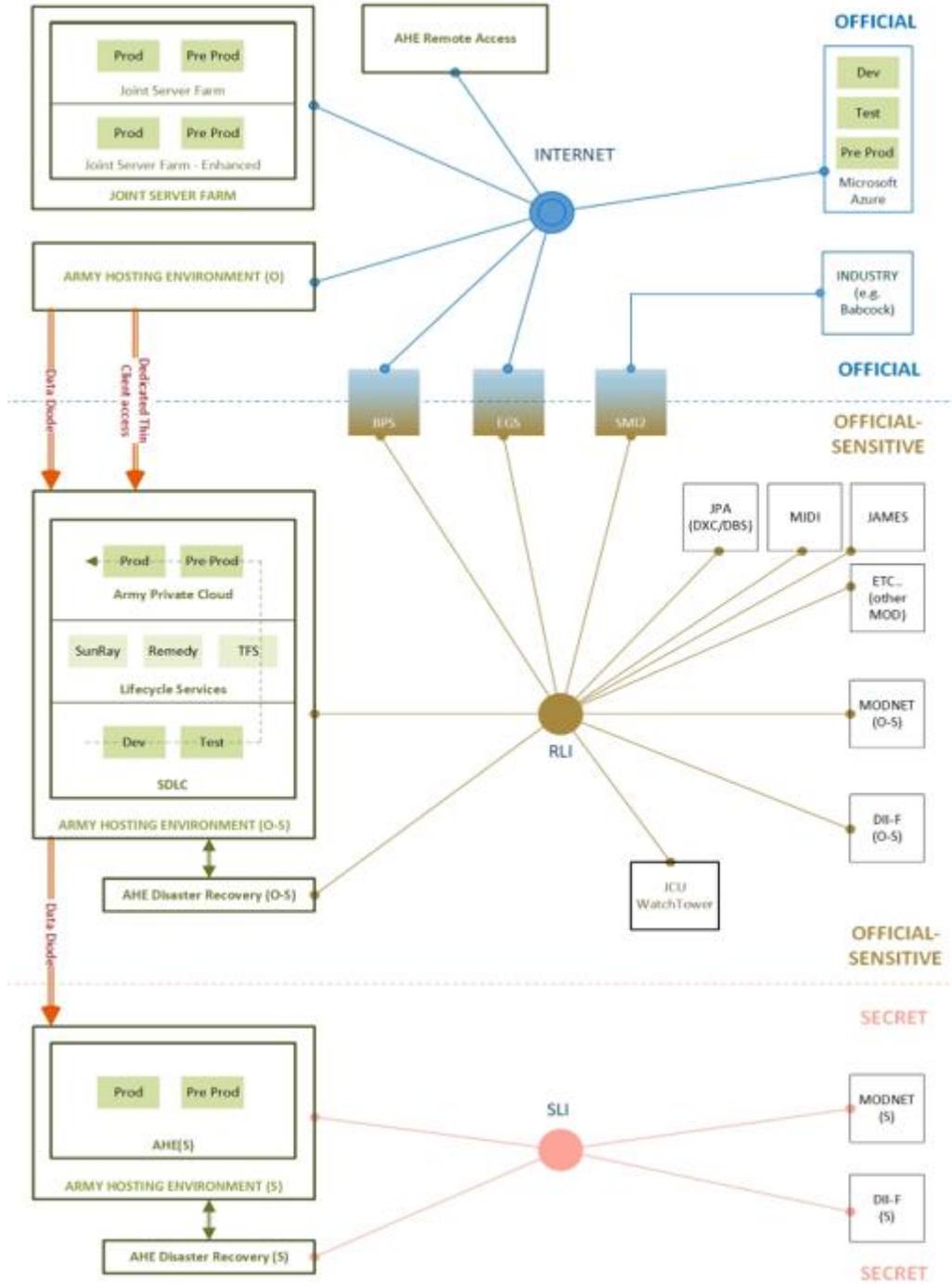


Figure 1 – AHE Landscape

11. THE JOINT SERVER FARM (JSF)

- 11.1 The JSF is a 'public cloud' currently hosted by Rackspace and is contracted as Infrastructure as a Service (IaaS). The JSF provides the hosting capability for the Defence Gateway (DGW) that support 300,000 registered users across regulars, reserves, families, veterans and contractors. Application users access the DGW applications from all standard internet-based devices (personal laptops, tablets, phones, etc.) but can also access them from the military WAN via the MOD Border Protection Service (BPS). It also provides Defence with a platform to host other capabilities, these include Defence Learning Environment and Westminster (Cadet information system) amongst the 19 partners.
- 11.2 The DGW provides an official capability that is accessed via Single Sign On (SSO) behind which there are currently 26 services of which 7 are ADS delivered. These are predominantly web services with a handful of native mobile applications. The web services provided range from COTS, in the form of web e-mail, SharePoint (used as a Content Management System) and Jive (known as Defence Connect). The bespoke developed services include, a portal page (consolidating access to all the services), MoDBox (an MoD variant of DropBox) and Reserve Attendance & Pay Service (RAPS) and My Admin (provides pay statements). The remainder of the services/application are third party provided utilising Platform as a Service (PaaS) and the DGW SSO.

12. OPERATING MODEL

- 12.1 ADS has invested significant time and effort to adopt Agile and then start to mature as a DevSecOps organisation. A pipeline approach has been established for deploying onto both the AHE and the JSF, utilising the same technologies for the majority.
- 12.2 The product teams are utilising Continuous Integration (CI) and Continuous Deployment (CD) with SCRUM as the agile framework. The in-service team have adopted Kanban. A Significant and on-going investment has been made to automate testing.
- 12.3 The Service Operations and Management teams utilise ITIL for change, incident, problem, knowledge and asset management. Remedy is used as the main IT Service Management Tool. The change and incident processes are used to capture the requirement but are then fed into the DevSecOps ways of working.
- 12.4 The Service landscape on AHE is as detailed below in Figure 2.

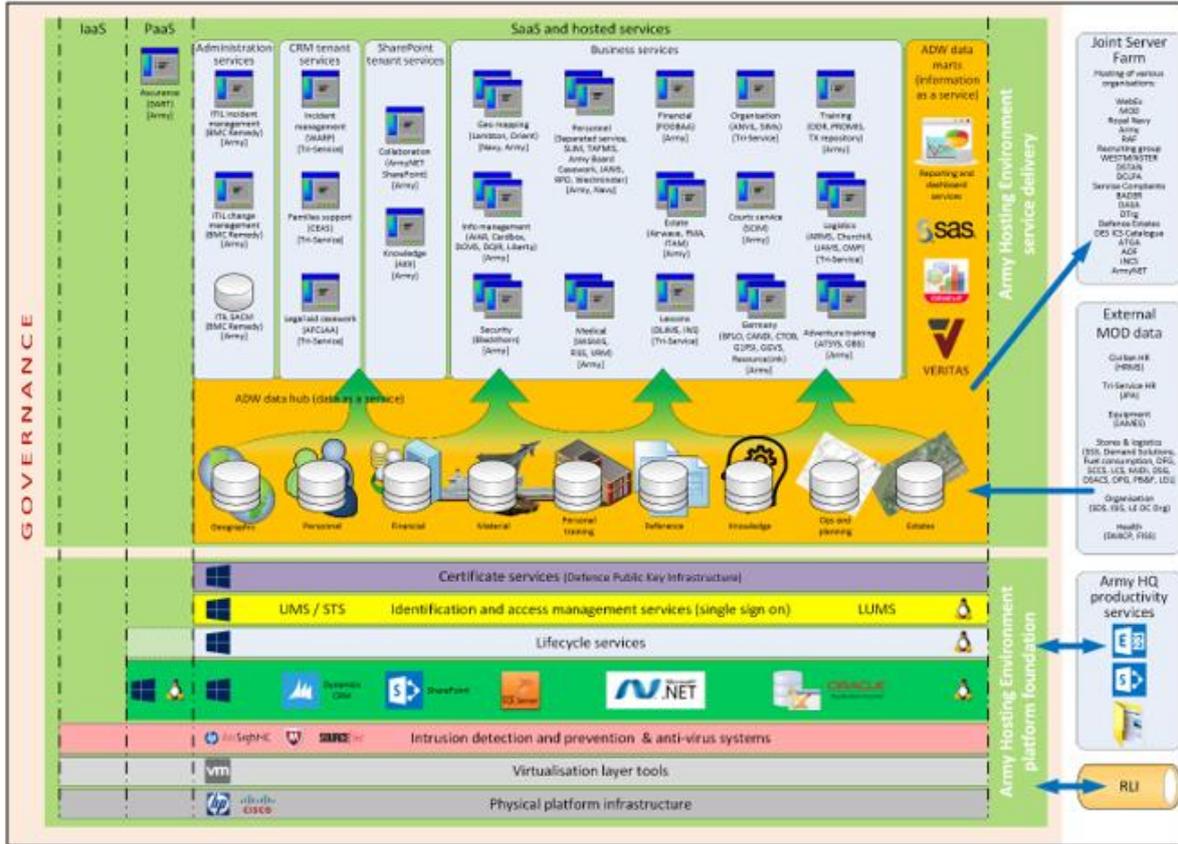


Figure 2 – Service landscape on AHE

13. ADS ORGANISATION, ROLES AND RESPONSIBILITIES

13.1 The structure of ADS and 605 Signal Troop is detailed in the diagram below and in the following paragraphs:



- 13.1.1 **Product Teams.** These are based predominantly on a 4-6 resource team, comprising of 2-4 developers, 1-2 testers, and a Business Analyst (BA) as their primary skills but all are multi-disciplined. These teams use SCRUM as their main framework for delivering software.
- 13.1.2 **In-Service Development Team.** These consist of 3 Oracle APEX and 2 .Net Developers with 3 testers matrix managed to enable the Service Managers to make changes to the services they support. These work on bug fixes and minor changes to live services. As the code base is changed the automated scripts are updated. Kanban is the agile framework used to process work. The Service Development Team also provide 3rd line support for the resolution of incidents and problems with application services. ADS has the ability to provide remote Dev/Test for this team utilising Azure. The main Dev/Test is on AHE v2 with automated release on to production.
- 13.1.3 **Test.** ADS has shifted left with testers imbedded in the product and in-service management teams. These testers are responsible for the automation of the functionality and regression testing. As part of the CI pipeline, after Dev/Test the next phase is System Integration Testing (SIT), where the software is tested on as close to production environment as possible; on SIT integration and exploratory testing are conducted; as well as the assurance of the automation tests. The technical assurance is provided by a senior tester.
- 13.1.4 **Army Data Warehouse (ADW).** The ADW is the single repository for the consolidation of Army and Defence data, which is then used to enable

reporting on Army activities. The ADW is also the hub for integration of other ADS applications and services ensuring use authoritative data.

- 13.1.5 **Defence Gateway Team.** This is a small DevSecOps team that does everything from supporting the infrastructure, to developing new services and maintaining them on the Defence Gateway (internet – official). Services include MoDBox (drop box equivalent), SharePoint, e-mail, Defence Connect (Jive) and applications to support activities such as Reserve Pay. The team has normally undertaken its own testing but has recently had a tester embedded to follow the same operating model as the rest of ADS with a pipeline of environments and automated testing. At present a single tester has been dedicated to this team. The DGW team utilise Azure for their Dev Test and Pre-production with production currently being delivered via Rackspace.
- 13.1.6 **Enterprise Administration.** A team of predominantly military (from 605 Troop) and civil servants with some Technical Support contractors. This team supports the AHE v2 for the Official Sensitive and Secret Environments. Responsibilities include support and maintenance of the storage, network, compute, hardware VMware tech stack (including virtualised network), VMs, OS and monitoring the health of applications/services. For all technical matters they are supported and guided by the TDO.
- 13.1.7 **Service Desk.** A team of civil servants and military that provide the first line of support for applications. This Service Management as a Service requirement will work alongside this in-house capability.
- 13.1.8 **Service Management.** A team of civil servants and military that ensure that applications continue to satisfy the evolving needs of the business and to support their Business-as-Usual. This Service Management as a Service requirement will work alongside this in-house capability.
- 13.1.9 **Application Support Team (AST).** This a team of mainly Civil Servants with technical support contractors. The main role of the team has been the transition of services onto Pre-Production and Production and provide second line support for application incidents and problems. The transition of services is now being automated utilising Microsoft Release Manager.
- 13.1.10 **Technical Design Office (TDO).** This is the main technical hub of the organisation, with the technical expertise for all the technologies employed by ADS. They are responsible for deploying new infrastructure services, handing over knowledge to the relative teams and providing 3rd and 4th line support for these services, predominately infrastructure and main core services for the data centres.
- 13.1.11 **Delivery Managers.** The delivery of new or small to medium sized services within ADS is the responsibility of Delivery Managers; this could be anything from an infrastructure change to a small product/service.

- 13.1.12 **Compliance Team.** Provides in-house advice to ensure ADS adheres to security and policies as laid out in Joint Service Publication (JSP) 440 and 604, ISO 27001 and security architecture.
- 13.1.13 **Configuration Team.** Responsible for the configuration control of hardware, software and documentation.
- 13.1.14 **Security Operations Centre.** Responsible for the protective monitoring of the AHE (O & S).
- 13.1.15 **Army Data Analytics.** The Army Data Analytics Team offer a range of analytical services to enable the business to gain insight and benefit from enterprise data. Dashboards display data visualisations of the current and historical status of metrics and key performance indicators for the enterprise.

SCHEDULE 2 – SERVICES REQUIRED

14. OVERVIEW OF REQUIREMENT

- 14.1 ADS is currently providing security architecture, compliance and information assurances, for ADS hosting infrastructures and applications in those environments.
- 14.2 Working alongside the existing in-house team, this "as a Service" will provide the capability to fulfil the Service Support wrapper outputs and allow veering and hauling to react quickly to changing requirements. These will require liaison with the FAST project teams, Application Support team (AST), Operational Support team (OST), Defence Gateway team, Technical Design Office (TDO), Security Operating Centre (SOC) and Service Managers.
- 14.3 Outputs will include but are not limited to; contributing to the renewal documentation required for compliance of ADS applications and environments, ensure coherence with MOD policy and Government guidance, policy and legislation regarding information assurance.
- 14.4 The service needs to be undertaken by technical outputs who hold MOD Security Clearance (SC) as a minimum, with a strong technical background and a very good understanding of Defence Security and Compliance policy and practices.

15. DELIVERABLES

- 15.1 The high-level deliverables for the service are outcomes associated with:
 - 15.1.1 **Application Onboarding.** To assist application owners through onboarding and accreditation processes, in line with JSP440, JSP604 and Cyber Defence and Risk policy and guidance to achieve accreditation.
 - 15.1.2 **Infrastructure Accreditation.** To maintain system RMADS and DART entry for the AHE and JSF and all supporting documentation to ensure continued accreditation. Engage with the Accreditor as and when necessary to keep them informed of any changes to the system that impacts on security and seek guidance from the accreditor when required. Arrange quarterly SWG's, ensuring all compliance documents are up to date and produce minutes for the meeting.
 - 15.1.3 **Remedy.** Where a change, incident or task is raised that has a security element, review the ticket to ensure security is not compromised and policy is being followed. Where a security control, process or procedure needs to be introduced, raise a request on Remedy
 - 15.1.4 **Threat Reports / Security Vulnerability Announcements.** When threat reports are issued, or security vulnerabilities are announced (e.g. MODCERT) determine if they are relevant to the ADS environments and ensure all relevant stakeholders are informed.
 - 15.1.5 **Security Events.** When a security event is reported determine if the event is an event that needs to be passed on to WARP.
 - 15.1.6 **Security Architecture.** Where required provide security advice on system/application security requirements such as security enforcing

functions and design to ensure that policy is being followed and that no legal Acts are being violated.

- 15.1.7 **Policy and Procedure.** Maintain system security related policy and procedures such as SyOps, Forensic Readiness, Accreditation Management Plan, Protective Monitoring, Information Exchange, Access Control, Data masking. Where new policy or procedures are required, produce appropriate documentation.
 - 15.1.8 **Security Risk Register.** Maintain the security risk register.
 - 15.1.9 **Audit.** Carry out audits to ensure that security policy and procedures are being followed.
- 15.2 Initially ADS require additional resources to supplement the existing in-house Compliance team. As a guide Table 1 provides a breakdown of the scale of effort likely to represent the initial requirement at contract commencement. Considering the level of autonomy and velocity that ADS requires, and again presented as a guide, the Authority would anticipate the annotated minimum SFIA levels against each role as stated in Table 1. However, the determination of the specific roles, team structure and associated SFIA levels of the technical resources that are to be engaged in delivering this capability is to be determined by the individual service provider so as to maintain this capability 'as a service'.

Table 1 – Minimum FTE Resource Structure

Ser	Role	Expected minimum FTE	SFIA ¹ Level
1	Security Assurance	1	3
2	Security Assurance	1	4

16. ESSENTIAL SKILLS AND EXPERIENCE

- 16.1 Overall, the Authority's requirement is for outcomes likely to be delivered by poly-skilled resource and the following details the skills and experience which are mandatory to ensure the Supplier can meet the Authority's current and potential future requirements for this "as a Service":
 - 16.1.1 Strong knowledge of MoD ICT Security and policies, and a familiarity of general security policies. Producing supporting security documentation including policies in co-ordination with stakeholders.
 - 16.1.2 ICT network and application accreditation including all supporting documentation, for example Risk Management Accreditation Documentation set (RMADs).
 - 16.1.3 Security Auditing.
 - 16.1.4 Gap analysis and remediation, knowledge of Information Assurance Maturity Model (IAMM) and the MOD Cyber Compliance Framework.
 - 16.1.5 Security management, governance and risk management.
 - 16.1.6 Network and application security and architecture, incident response, forensic investigation and business continuity management.

¹ Skills Framework for the Information Age - <https://www.sfia-online.org/en>

- 16.1.7 Knowledge of Data Protection and bulk data.
- 16.1.8 Professional designation such as CESG Certified Professional (CCP) (Security and Information Risk Advisor, practitioner level) CISSP, CISA CISM or ISO 27001 Lead Auditor.
- 16.2 Desirable skills and experience of resources supplied are to be:
 - 16.2.1 NCSC certified professionals, ex-CLAS or of equivalent experience.
 - 16.2.2 Knowledge of protective monitoring.
 - 16.2.3 Knowledge of NIST
- 16.3 Where requested the Supplier would be expected to justify SFIA levels of resources utilised in this work in terms of professional memberships, training, qualifications/certifications and above all examples of prior work and experience that is relevant to the role(s) they are assigned against.
- 16.4 The Supplier and the resources it provides must be free of any commercial ties or obligations to any hardware or software vendors.
- 16.5 The Supplier will be required to provide a client interface to agree business prioritisations and deliverables.
- 16.6 It is desirable that resources have current working knowledge of MoD systems and networks and have evidence of previously providing services to MoD or security services.
- 17. **LOCATION**
 - 17.1 The normal place of work for this requirement is ADS in Andover, Hampshire, United Kingdom. Although a proportion of this work will be suitable for remote working, under an agile approach there will be routine occasions where team collaboration is essential, as is engagement with the user community, and ADS departments. As such it is not considered to be appropriate that this requirement is satisfied by off-shore resources working outside the U.K.
- 18. **SCALING**
 - 18.1 The ability for the Authority to scale up or down rapidly is a key requirement in order to respond to the dynamic needs of ADS, including the ability to resource urgent operational requirements. As such, and subject to demand and budget, the Authority requires the ability to scale up and down the resource requirements in relation to outputs. In essence, this means that there will be a minimum (core) level below which the quantity of outputs will not fall and beyond this a discretionary level that the Authority may choose to exploit in part or whole at various stages throughout the contract.
 - 18.2 The requirement for the provision of additional resources would take 2 forms:
 - 18.2.1 **Additional roles (expansion)** - if an initiative requires a new/further set of skills. For example, a new application is developed for which the outputs commensurately require a new Security Assurance Co-ordinator capability to be established. This would be over and above the current 'on-going' outputs and resource provision.

or,

- 18.2.2 **Replacement of a role (re-prioritisation)** - if there is need to pivot outputs in response to the Authority's demands which may require a different skill-set. For example, as the expansion of a particular application evolves there is a need to re-balance the resources associated with it. In this example this could be the provision of an additional Level 1 resource at the expense of an alternative resource (or vice versa).
- 18.3 The Authority will require confirmed rate cards for the provision of resources to deliver new work. This would involve the ability to select pre-defined service offerings in relation to new outputs that would be above the core service. Due to budgetary constraints it is envisaged that the service would be on a capped T&M basis that would enable the Supplier to confirm a maximum cost to meet the outputs required over a set period.
- 18.4 Although the requirement will not fall below the minimum level of the contract the Authority may also require discontinuing of certain activity at its discretion which in turn may lead to exit (off-boarding) of certain resources.

SCHEDULE 3 – SERVICE LEVELS

19. PROVISIONING

- 19.1 The Service Supplier is expected to use their 'best endeavours' to provide resources to meet the priorities specified by ADS. Specifically:
- 19.1.1 Provision of further resources within twenty-five (25) calendar days.
- 19.1.2 Exit of current resources no longer required within seven (7) calendar days.

20. SECURITY REQUIREMENTS

- 20.1 All outputs that fulfil this requirement will need to have a minimum level of Security Clearance and be subject to vetting. The minimum standard is MOD Security Clearance (SC), although on occasion the Authority may prescribe a higher level of Security Clearance. This will be applied on a case-by-case basis to both existing and new resources where the Authority has the requirement to do so. The Service Supplier warrants that all staff used to supply their service hold current, MOD applicable, Security Clearances at SC level or above and are willing and eligible to obtain higher clearance levels if the role requires it.

21. CONTINUOUS IMPROVEMENT

- 21.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
- 21.2 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

Order Schedule 21 - Northern Ireland Law – N/A

Order Schedule 22 – Secret Matters

1. Associated definitions

- 1.1 In this Order Schedule 22, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Document"	includes specifications, plans, drawings, photographs and books;
"Secret Matter"	means any matter connected with or arising out of the performance of this Order Contract which has been, or may hereafter be, by a notice in writing given by the Customer to the Supplier be designated 'top secret', 'secret', or 'confidential';
"Servant"	where the Supplier is a body corporate shall include a director of that body and any person occupying in relation to that body the position of director by whatever name called.

2. Disclosure

- 2.1 The Supplier shall not, either before or after the completion or termination of this Order Contract, do or permit to be done anything which it knows or ought reasonably to know may result in information about a Secret Matter being:
- 2.1.1 without the prior consent in writing of the Buyer, disclosed to or acquired by a person who is an alien or who is a British subject by virtue only of a certificate of naturalisation in which his name was included;
 - 2.1.2 disclosed to or acquired by a person as respects whom the Buyer has given to the Supplier a notice in writing which has not been cancelled stating that the Buyer requires that Secret Matters shall not be disclosed to that person;
 - 2.1.3 without the prior consent in writing of the Buyer, disclosed to or acquired by any person who is not a Servant of the Supplier; or
 - 2.1.4 disclosed to or acquired by a person who is an employee of the Supplier except in a case where it is necessary for the proper performance of this Order Contract that such person shall have the information.

3. Safeguarding

- 3.1 Without prejudice to the provisions of Paragraph 2, the Supplier shall, both before and after the completion or termination of this Order Contract, take all reasonable steps to ensure:
- 3.1.1 no such person as is mentioned in Paragraph 2.1, 2.1.1 or 2.1.2, thereof shall have access to any item or Document under the control of the Supplier containing information about a Secret Matter except with the prior consent in writing of the Buyer;
 - 3.1.2 that no visitor to any premises in which there is any item to be supplied under this Order Contract or where Goods are being supplied shall see or discuss with the Supplier or any person employed by him any Secret Matter unless the visitor is authorised in writing by the Buyer so to do;

- 3.1.3 that no photograph of any item to be supplied under this Order Contract or any portions of the Goods shall be taken except insofar as may be necessary for the proper performance of this Order Contract or with the prior consent in writing of the Buyer, and that no such photograph shall, without such consent, be published or otherwise circulated;
- 3.1.4 that all information about any Secret Matter and every Document, model or other item which contains or may reveal any such information is at all times strictly safeguarded, and that, except insofar as may be necessary for the proper performance of this Order Contract or with the prior consent in writing of the Buyer, no copies of or extracts from any such Document, model or item shall be made or used and no designation of description which may reveal information about the nature or contents of any such Document, model or item shall be placed thereon; and
- 3.1.5 that if the Buyer gives notice in writing to the Supplier at any time requiring the delivery to the Customer of any such Document, model or item as is mentioned in Paragraph 3.1.4, that Document, model or item (including all copies of or extracts therefrom) shall forthwith be delivered to the Buyer who shall be deemed to be the owner thereof and accordingly entitled to retain the same.

4. Decision of the Buyer

- 3.1 The decision of the Buyer on the question whether the Supplier has taken or is taking all reasonable steps as required by the foregoing provisions of Order Schedule 22 shall be final and conclusive.

5. Particulars of People

- 5.1 If and when directed by the Buyer, the Supplier shall furnish full particulars of all people who are at any time concerned with any Secret Matter.

6. Official Secrets Act

- 6.1 If and when directed by the Buyer, the Supplier shall secure that any person employed by it who is specified in the direction, or is one of a class of people who may be so specified, shall sign a statement that he understands that the Official Secrets Act, 1911 to 1989 and, where applicable, the Atomic Energy Act 1946, apply to the person signing the statement both during the carrying out and after expiry or termination of the Order Contract.

7. Information concerning the Contract

- 7.1 If, at any time either before or after the expiry or termination of this Order Contract, it comes to the notice of the Supplier that any person acting without lawful authority is seeking or has sought to obtain information concerning this Order Contract or anything done or to be done in pursuance thereof, the matter shall be forthwith reported by the Supplier to the Buyer and the report shall, in each case, be accompanied by a statement of the facts, including, if possible, the name, address and occupation of that person, and the Supplier shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any person employed by it, that person shall forthwith report the matter to the Supplier with a statement of the facts as aforesaid.

8. Duty to observe obligations

- 8.1 The Supplier shall place every person employed by it, other than a Sub contractor, who in its opinion has or will have such knowledge of any Secret Matter as to appreciate its

significance, under a duty to the Supplier to observe the same obligations in relation to that Secret Matter as are imposed on the Supplier by Paragraphs 2 and 3 and shall, if directed by the Buyer, place every person who is specified in the direction or is one of a class of people so specified, under the like duty in relation to any Secret Matter which may be specified in the direction, and shall at all times use its best endeavours to ensure that every person upon whom obligations are imposed by virtue of this Part A to Order Schedule 22 observes the said obligations, and the Supplier shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the said obligations, report the facts to the Supplier with all necessary particulars.

9. Sub-Contract Obligations

- 9.1 The Supplier shall, if directed by the Buyer, include in the Sub-Contract provisions in such terms as the Buyer may consider appropriate for placing the Sub-Contractor under obligations in relation to secrecy and security corresponding to those placed on the Supplier by this Order Schedule 22, but with such variations (if any) as the Buyer may consider necessary. Further the Supplier shall:
- 9.2 give such notices, directions, requirements and decisions to its Sub Contractors as may be necessary to bring the provisions relating to secrecy and security which are included in Sub-Contracts under this Order Schedule 22 into operation in such cases and to such extent as the Buyer may direct;
- 9.3 if there comes to its notice any breach by the Sub-Contractor of the obligations of secrecy and security included in their Sub-Contracts in pursuance of this Order Schedule 22, notify such breach forthwith to the Customer; and
- 9.4 if and when so required by the Buyer, exercise its power to determine the Sub-Contract under the provision in that Sub-Contract which corresponds to Paragraph 12.

10. Information to the Buyer

- 10.1 The Supplier shall give the Buyer such information and particulars as the Buyer may from time to time require for the purposes of satisfying the Buyer that the obligations imposed by or under the foregoing provisions of this Order Schedule 22 have been and are being observed and as to what the Supplier has done or is doing or proposes to do to secure the observance of those obligations and to prevent any breach thereof, and the Supplier shall secure that a representative of the Buyer duly authorised in writing shall be entitled at reasonable times to enter and inspect any premises in which anything is being done or is to be done under this Order Contract or in which there is or will be any item to be supplied under this Order Contract, and also to inspect any Document or item in any such premises or which is being made or used for the purposes of this Order Contract and that any such representative shall be given all such information as he may require on the occasion of, or arising out of, any such inspection.

11. Exclusion

- 11.1 Nothing in this Order Schedule 22 shall prevent any person from giving any information or doing anything on any occasion when it is, by virtue of any enactment, the duty of that person to give that information or do that thing.

12. Grounds for Termination

- 12.1 If the Buyer shall consider that any of the following events has occurred:

- 12.1.1 that the Supplier has committed a breach of, or failed to comply with any of, the foregoing provisions of this Order Schedule 22; or
- 12.1.2 that the Supplier has committed a breach of any obligations in relation to secrecy or security imposed upon it by any other contract with the Buyer, or with any department or person acting on behalf of the Crown; or
- 12.1.3 that by reason of an act or omission on the part of the Supplier, or of a person employed by the Supplier, which does not constitute such a breach or failure as is mentioned in Paragraph 12.1.4, information about a Secret Matter has been or is likely to be acquired by a person who, in the opinion of the Buyer, ought not to have such information;
- 12.1.4 and shall also decide that the interests of the state require the termination of this Order Contract, the Buyer may by notice in writing terminate this Order Contract forthwith.

13. Buyer Decision to Terminate

- 13.1 A decision of the Buyer to terminate this Order Contract in accordance with the provisions of Paragraph 12 shall be final and conclusive and it shall not be necessary for any notice of such termination to specify or refer in any way to the event or considerations upon which the Buyer's decision is based.

14. Supplier's notice

- 14.1 The Supplier may within five (5) Working Days of the termination of this Order Contract in accordance with the provisions of Paragraph 12, give the Buyer notice in writing requesting the Buyer to state whether the event upon which the Buyer's decision to terminate was based is an event mentioned in Paragraphs 12.1.1, 12.1.2 or 12.1.3 and to give particulars of that event; and
- 14.2 the Buyer shall within ten (10) Working Days of the receipt of such a request give notice in writing to the Supplier containing such a statement and particulars as are required by the request.

15. Matters pursuant to termination

- 15.1 The termination of this Order Contract pursuant to Paragraph 12 shall be without prejudice to any rights of either Party which shall have accrued before the date of such termination;
- 15.2 The Supplier shall be entitled to be paid for any work or thing done under this Order Contract and accepted but not paid for by the Buyer at the date of such termination either at the price which would have been payable under this Order Contract if the Order Contract had not been terminated, or at a reasonable price;
- 15.3 The Buyer may take over any work or thing done or made under this Order Contract (whether completed or not) and not accepted at the date of such termination which the Buyer may by notice in writing to the Supplier given within thirty (30) Working Days from the time when the provisions of this Order Schedule 22 shall have effect, elect to take over, and the Supplier shall be entitled to be paid for any work or thing so taken over a price which, having regard to the stage which that work or thing has reached and its condition at the time it is taken over, is reasonable. The Supplier shall in accordance with directions given by the Buyer, deliver any work or thing taken over under this Paragraph 15.3, and take all such other steps as may be reasonably necessary to enable the Buyer to have the full benefit of any work or thing taken over under this Paragraph 15.3; and

15.4 Save as aforesaid, the Supplier shall not be entitled to any payment from the Buyer after the termination of this Order Contract.

16. Rights & Obligations after Termination

16.1 If, after notice of termination of this Order Contract pursuant to the provisions of Paragraph 12:

16.1.1 the Buyer shall not within ten (10) Working Days of the receipt of a request from the Supplier, furnish such a statement and particulars as are detailed in Paragraph 14.1; or

16.1.2 the Buyer shall state in the statement and particulars detailed in Paragraph 14.2 that the event upon which the Buyer's decision to terminate this Order Contract was based is an event mentioned in Paragraph.12.1.3,

16.2 the respective rights and obligations of the Supplier and the Buyer shall be terminated in accordance with the following provisions:

16.2.1 the Buyer shall take over from the Supplier at a fair and reasonable price all unused and undamaged materials, bought-out parts and components and articles in course of manufacture in the possession of the Supplier upon the termination of this Order Contract under the provisions of Paragraph 12 and properly provided by or supplied to the Supplier for the performance of this Order Contract, except such materials, bought-out parts and components and articles in course of manufacture as the Supplier shall, with the concurrence of the Buyer, elect to retain;

16.2.2 the Supplier shall prepare and deliver to the Buyer within an agreed period or in default of agreement within such period as the Buyer may specify, a list of all such unused and undamaged materials, bought-out parts and components and articles in course of manufacture liable to be taken over by or previously belonging to the Buyer and shall deliver such materials and items in accordance with the directions of the Buyer who shall pay to the Supplier fair and reasonable handling and delivery charges incurred in complying with such directions;

16.2.3 the Buyer shall indemnify the Supplier against any commitments, liabilities or expenditure which are reasonably and properly chargeable by the Supplier in connection with this Order Contract to the extent to which the said commitments, liabilities or expenditure would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Order Contract;

16.2.4 if hardship to the Supplier should arise from the operation of this Paragraph 16 it shall be open to the Supplier to refer the circumstances to the Buyer who, on being satisfied that such hardship exists shall make such allowance, if any, as in its opinion is reasonable and the decision of the Buyer on any matter arising out of this Paragraph 16.5 shall be final and conclusive; and

16.2.5 subject to the operation of Paragraphs 16.2.1, 16.2.2, 16.2.3, and 16.2.4 termination of this Order Contract shall be without prejudice to any rights of either party that may have accrued before the date of such termination.