

DPS Schedule 6 (Order Form Template and Order Schedules)
Crown Copyright 2020

DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE: C289973

THE BUYER: The Secretary of State for Health and Social Care acting as part of the Crown

BUYER ADDRESS 39 Victoria Street,
Westminster,
London,
SW1H 0EU

THE SUPPLIER: Radio Technical Services Limited

SUPPLIER ADDRESS: 40-42 Jaggard Way, London, SW12 8SG

REGISTRATION NUMBER: 03184447

DUNS NUMBER: 458336922

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 17th June 2024.

It's issued under the DPS Contract with the reference number RM6225 for the Provision of Audio-visual services for the Lampard Inquiry

DPS FILTER CATEGORIES:

Discovery - User Requirements / Business Analysis, Project Management, Technical Advisor, Technical Design & Integration Plan, Audio Visual Turnkey Delivery & Warranty, Monitoring, New or Renewal, On-site, Remote Management & Support

ORDER INCORPORATED TERMS

The following documents are incorporated into this Order Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

This Order Form including the Order Special Terms and Order Special Schedules.

1. Joint Schedule 1(Definitions and Interpretation) RM6225
2. DPS Special Terms
3. The following Schedules in equal order of precedence:

- Joint Schedules for RM6225
 - Joint Schedule 2 (Variation Form)

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)
- Joint Schedule 12 (Supply Chain Visibility)
- Order Schedules for C289973
 - Order Schedule 2 (Staff Transfer)
 - Order Schedule 3 (Continuous Improvement)
 - Order Schedule 5 (Pricing Details)
 - Order Schedule 6 (ICT Services)
 - Order Schedule 7 (Key Supplier Staff)
 - Order Schedule 8 (Business Continuity and Disaster Recovery)
 - Order Schedule 9 (Security) Long Form
 - Order Schedule 10 (Exit Management)
 - Order Schedule 11 (Installation Works)
 - Order Schedule 14 (Service Levels)
 - Order Schedule 15 (Order Contract Management)
 - Order Schedule 16 (Benchmarking)
 - Order Schedule 18 (Background Checks)
 - Order Schedule 20 (Order Specification)
 - Order Schedule 22 (Lease Terms)

4. CCS Core Terms (DPS version) v1.0.3

5. Joint Schedule 5 (Corporate Social Responsibility) RM6225

6. Order Schedule 4 (Order Tender) as long as any parts of the Order Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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

ORDER SPECIAL TERMS

None

ORDER START DATE: 1st August 2024

ORDER EXPIRY DATE: 31st July 2026

ORDER INITIAL PERIOD: 2 Years

ORDER OPTIONAL EXTENSION 1 Year

DELIVERABLES

See details in Order Schedule 20 (Order Specification)

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

MAXIMUM LIABILITY

The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £1,460,000.00 ex VAT Estimated Charges in the first 12 months of the Contract. The Buyer must always provide a figure here.

ORDER CHARGES

See details in Order Schedule 5 (Pricing Details)

The Charges will not be impacted by any change to the DPS Pricing. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Indexation
- Specific Change in Law
- Benchmarking using Order Schedule 16 (Benchmarking)

REIMBURSABLE EXPENSES

N/A

PAYMENT METHOD

PO / Invoice monthly in arrears

BUYER'S INVOICE ADDRESS:

39 Victoria Street, London, SW1H 0EU

BUYER'S AUTHORISED REPRESENTATIVE

For general inquiries

[Redacted]

For commercial inquiries

[Redacted]

BUYER'S ENVIRONMENTAL POLICY

<https://www.gov.uk/government/publications/greening-government-commitments-2021-to-2025/greening-government-commitments-2021-to-2025>

BUYER'S SECURITY POLICY

<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>

SUPPLIER'S AUTHORISED REPRESENTATIVE

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning

Project Version: v1.1

Model Version: v1.3

DPS Schedule 6 (Order Form Template and Order Schedules)
Crown Copyright 2020

[Redacted]

SUPPLIER'S CONTRACT MANAGER

[Redacted]

or, in their absence,

[Redacted]

PROGRESS REPORT FREQUENCY
On the first Working Day of each calendar month

PROGRESS MEETING FREQUENCY
Quarterly on the first Working Day of each quarter

KEY STAFF

[Redacted]

[Redacted]

KEY SUBCONTRACTOR(S)

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Briault Reporting Limited

Stirling House Carriers Fold, Church Road, Wombourne, West Midlands, WV5 9DJ

Company Registration: 12314028

E-AUCTIONS

N/A

COMMERCIALLY SENSITIVE INFORMATION

N/A

SERVICE CREDITS

Service Credits will accrue in accordance with Order Schedule 14 (Service Levels).

The Service Credit Cap is: a 5% reduction of the overall invoice for each hearing day

The Service Period is: Applies to any given hearing day over the lifetime of the contract.

A Critical Service Level Failure is: Where 99.9% of connectivity issues are not resolved within one hour.

ADDITIONAL INSURANCES

A minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract

GUARANTEE

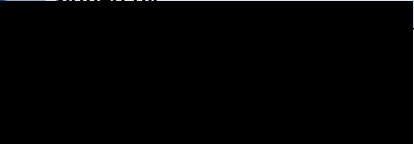



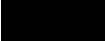
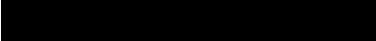
Not applicable

SOCIAL VALUE COMMITMENT

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

DPS Schedule 6 (Order Form Template and Order Schedules)
Crown Copyright 2020

Signed:

For and on behalf of the Supplier:	For and on behalf of the Buyer:
Signed by: 	DocuSigned by: 
Full Name: 	Full Name: 
Job Title/Role: 	Job Title/Role: 
Date Signed: 02082024	Date Signed: 5th August 2024

Joint Schedule 11 (Processing Data)

Definitions

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

“Processor Personnel”	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;
----------------------------------	---

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

- (a) “Controller” in respect of the other Party who is “Processor”;
- (b) “Processor” in respect of the other Party who is “Controller”;
- (c) “Joint Controller” with the other Party;
- (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (c) ensure that :
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
 - (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
 - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
- 7.** Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Personal Data Breach.
- 8.** The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
- 9.** Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Personal Data Breach; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- 10.** The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
 - (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
 - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 11.** The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 12.** The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- 13.** Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
 - (a) notify the Controller in writing of the intended Subprocessor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
 - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
- 14.** The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
- 15.** The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
- 16.** The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

- 17.** In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 8 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
22. The Parties shall only provide Personal Data to each other:
 - (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
- 26.** Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
- 27.** Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
- 28.** Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
- 29.** Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 27 of this Joint Schedule 11.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Annex 1 - Processing Personal Data

- . This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer are:

[REDACTED]

1.1.1.2 The contact details of the Supplier's Data Protection Officer are:

[REDACTED]

1.1.1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>in regards to the provision of AV, transcript and presentation of electronic evidence services to the Lampard Inquiry.</p>
Duration of the Processing	Duration of the contract
Nature and purposes of the Processing	<ul style="list-style-type: none"> • Inquiry will have live hearings, during which, RTS will • provide the Lampard Inquiry with AV services for the hearings • including ensuring all hearings are live streamed (with agreed restrictions) on online platforms such as Youtube or recorded (video and audio). • These recordings will be reviewed, edited, redacted and then • published on online platforms such as YouTube. • The Lampard Inquiry will be able to review any recordings via a secure online platform such as eXchange • RTS will also publish transcripts from the hearings. • RTS will also present electronic evidence at the hearings via screens. RTS will be sent evidence via a secure online platform such as eXchange . If eXchange or an alternative secure platform was • unavailable then this would be sent via eMail or encrypted USB.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Type of Personal Data	<ul style="list-style-type: none"> Personal data - voice, images, demographics, employer information, financial information Special category data - health, religion, ethnicity and criminal data.
Categories of Data Subject	Members of the public, experts, legal teams and any other witnesses to the Inquiry.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	<ul style="list-style-type: none"> Data will be retained by the supplier until the contract end date, shortly before which time the supplier will be required to handle data according to the instructions of the Inquiry. RTS must not share data with any third parties, unless with explicit agreement with the Inquiry.

2. Data Protection Breach

1.1.2.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
- (b) all reasonable assistance, including:
 - (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
 - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
 - (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

1.1.2.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

3. Audit

1.1.3.1 The Supplier shall permit:

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

1.1.3.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

4. Impact Assessments

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

1.1.4.1 The Parties shall:

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

5. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

6. Liabilities for Data Protection Breach

1.1.6.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

- (a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;
- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
- (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

1.1.6.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

1.1.6.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

- (a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
- (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

1.1.6.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

7. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

8. Sub-Processing

1.1.8.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

9. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

1. Order Schedule 4 (Order Tender)

SCOPE OF REQUIREMENT

- 1.1 Provision of a fully rigged hearing room and back office at the Inquiry's hearing sites in London and Chelmsford that meets the requirements of the Inquiry as outlined in this Statement of Requirement. Multiple venues, some not yet confirmed, will be used over the course of the Inquiry. Therefore, on site assessment of the needs of each venue will be required ahead of the first Hearing in each new venue.
- 1.2 Live AV web streaming for hearing centre and online for Core Participants (CPs) and other key Inquiry personnel.
- 1.3 A delayed broadcast via YouTube for the public – the delay length to be decided by the Chair.
- 1.4 Voice distortion to protect the anonymity of witnesses and/or other anonymity provisions such as screens.
- 1.5 Live on-site stenography services (including stenographer, stenography systems and editing) for all hearing days.
- 1.6 Provision and management of video conferencing platform licences and management of video conferencing platform for meetings.
- 1.7 For remote Hearings if required CPs that are required to input into a hearing and in the event of remote participation of Chair, witnesses, legal representatives, Counsel to the Inquiry (CTI) and other key Inquiry stakeholders) and video conferences (for extended, non-speaking CPs).
- 1.8 Electronic Presentation of Evidence (EPE) to include an Electronic Presentation Operator for all hearing days, EPE software services and systems that are compatible with materials held on or exported from the Inquiry's evidence management system (Relativity).
- 1.9 On-site technicians for testing days and all hearings days.
- 1.10 All equipment is to be left in-situ at the Inquiry's hearing site during sitting and non-sitting periods where this delivers value for money for the Inquiry. This will reduce costs that would be incurred by repeated installation and removal of equipment, and to mitigate the risk of delays during set-up and testing.
- 1.11 Recording of any further events related to the Inquiry that may be required.
- 1.12 All requirements in this document are mandatory.
- 1.13 The requirements set out in this document may be subject to change between now and the Inquiry hearings and therefore flexibility is required from the Supplier. Any changes to the requirements would be flagged to the Supplier with as much notice as possible.

2. THE REQUIREMENT

- 2.1 All content in this section pertains to the hearing sites.
- 2.2 All contracted technicians to be able to work remotely if needed (for example pandemic, unable to access building etc.)

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- 2.3 Require the ability to conduct hearings online if needed through the provision IT kit sent to key Inquiry stakeholders and the use of video conferencing facilities in the event of the requirement of remote participation.
- 2.4 On-site visit and assessment of the specific requirements needed to successfully deliver a fit for purpose hearing to be conducted ahead of the first hearing within each venue. The supplier shall produce detailed layout schematics to enable the Inquiry to visualise potential layouts for each venue.
- 2.5 Require experience of working on difficult topics and the ability to handle sensitive evidence and engage with vulnerable and/or distressed hearing participants appropriately.
- 2.6 Requirements laid out below will vary depending on the venue, different layouts and equipment is likely to be required for each hearing venue, however, the supplier will need to meet the below minimum requirements.

Area	Item	Requirements
Hearing Room	Broadcasting set up	<ul style="list-style-type: none"> - Cameras to ensure consistent video feed across the hearing room - PA System and microphone points to ensure effective participation from all parties including Chair, legal, witnesses
	Evidence presentation system and on site viewing	<ul style="list-style-type: none"> - Screens on participants desk which enable sight of the evidence being displayed - Video and evidence licencing and distribution - Evidence presentation system technology (and that the evidence presentation links to the Inquiry evidence management system, Relativity) - Evidence presentation technology assistant to carry out evidence presentation - Provide identifiers of documents presented during the course of hearings to the Inquiry team each day of hearings
	In room screens and accessibility functions	<ul style="list-style-type: none"> - Large, High-definition monitors to ensure all in person attendees can view the Chair and witnesses depending on

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

		<p>line of site in the room</p> <ul style="list-style-type: none"> - Additional mobile screen to potentially show Chair (if remote attendance by the Chair is required) and witnesses (if remote) - Hearing loop for hearing aid wearers
	Stenography services	<ul style="list-style-type: none"> - Transcript licencing and distribution - An in-room stenographer - An online editor (but may need to be in room if requested) - Stenography system to conduct stenography (and that the system links to the transcription service)
	Furniture, fixtures and fittings	<ul style="list-style-type: none"> - Provision and installation of Lampard Inquiry branded backdrop (subject to site survey) or a neutral backdrop if it is not possible to install an Inquiry-branded one. - Provision of all furniture, fixtures and fittings (i.e. screens, partitions, desks, chairs etc) required to achieve agreed lay out, where venue cannot provide these.
	Lighting	<ul style="list-style-type: none"> - Lighting wash - Studio-level lighting required for the hearing site so Chair/CTI/Witnesses are appropriately visible on Inquiry stream - Window treatments in the hearing room to ensure/maintain appropriate lighting levels if required
	Power supply	Venue to provide power supply but AV supplier to advise on location and provide additional extension cables if

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

		required.
	Technicians	Requisite number of staff (camera operatives, technicians, video engineer, audio engineer, floor runner, dedicated project manager if required) to run the hearings
Inquiry streaming via Inquiry YouTube channel	Video licencing	<ul style="list-style-type: none"> - Licencing and administration of live Inquiry feed - 4k vision mixer
	Public broadcast distribution	<ul style="list-style-type: none"> - Video delay units - Administration of delayed YouTube stream (delay length subject to be determined) - including establishment and management of stream. - Application of redactions to video and/or audio of hearing proceedings on the instruction of the Inquiry - Voice distortion and pixelation to protect the anonymity of witnesses. - Administration and services for the upload of finalised stream to YouTube at end of hearing day.
	Core Participants webinar	Administration of live webinar for remote CPs if required
	Remote hearing (video meeting/conference)	Administration of remote hearing for CPs with a speaking role if required
	Cloud storage	Cloud storage for hearing content
Back office (2 to 5 rooms) including for example room for	Live stream of hearing	<ul style="list-style-type: none"> - Monitor to display live feed of hearing.
	Evidence and transcription	<ul style="list-style-type: none"> - Monitor to display evidence and transcription.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

legal representatives and public overspill room	Desk Monitors	<ul style="list-style-type: none"> – Additional on desk monitors for secretariat and legal teams to use as second screens.
	Printing	<ul style="list-style-type: none"> – Installation and provision of a printer / scanner / photocopier on-site that can be connected securely for Inquiry staff to use if required.
Virtual Hearing (if required)	Streaming and effective participation of multiple remote attendees and participants	<ul style="list-style-type: none"> - Provision of secure virtual platform for participants including Chair, Core participants, legal representatives - Provision of equipment i.e. laptops, webcams etc for virtual participants <p>Virtual support for participants before and during hearings to troubleshoot issues if they arise</p>
Edit Suite	Editing suite	Provision of equipment for an on-site editing suite

- 2.7 A design and configuration of the Hearing Room is required.
- 2.8 The Supplier will provide training/guidance for all staff operating the Inquiry AV systems (both at hearing sites and online – in-person and virtual, depending on which is more appropriate) and for CPs/viewers (where required).
- 2.9 Testing of all audio-visual equipment and written assurance that all equipment is working 24 hours prior to hearings commencing.
- 2.10 Copyright of all audio-visual content created will be Crown Copyright and to be formally transferred to the Inquiry and then deleted from the Supplier's systems one week before the Contract end date.
- 2.11 The Supplier is required to confirm in writing to the Inquiry that contractual deletion of all Crown Copyrighted material has been completed one week prior to the Contract end date.
- 2.12 The supplier shall perform the services with sensitivity, taking into account the sensitivity of the Inquiry materials and potential vulnerability of the Inquiry participants.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

3. CONTRACT TERM, KEY MILESTONES AND DELIVERABLES

3.1 The contract term will be 24 months and will begin on the date that both parties have signed the contract. An optional extension period of one year will be available at the sole discretion of the Inquiry. This extension period, if exercised shall not increase the available budget outlined in paragraph 13.4 and will be solely for the purpose of completing the project.

3.2 The following Contract milestones/deliverables shall apply (all timings estimated)

Milestone / Deliverable	Description	Timeframe or Delivery Date
Opening Statement and first impact evidence hearings - Civic Centre, Chelmsford, Essex		
AV design finalised	Complete AV design and configuration of hearing room	Within two weeks of contract start date
AV installation of hearing room	Full installation of all AV for hearing centre and set up of all services for delivery of onsite hearing and online viewing/participation	Opening Statement: 9/9/2024 - 13/9/2024 Impact Hearings: 16/09/2024-25/09/2024
Testing	Full testing of hearing centre AV prior to the commencement of the preliminary hearing	Preliminary Hearing 1: 6/9/2024
Further impact hearings and public hearings - Dates to be confirmed		
AV design finalised (done prior to AV contract being finalised)	Complete AV design and configuration of hearing room	TBC
AV installation of hearing room	Full installation of all AV for hearing centre and set up of all services for delivery of onsite hearing and online viewing/participation	TBC
Testing	Full testing of hearing centre AV prior to the commencement of	TBC

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

	hearings	
Hearings	Continual AV support for all sitting days for hearings	TBC
Hearings Contingency		TBC

4. MANAGEMENT INFORMATION/REPORTING**4.1 The supplier's responsibilities include:**

- 4.1.1 Contributing updates following each hearing week via a virtual or in-person meeting to reflect on any audio-visual challenges (e.g. quality of live stream, positioning of cameras), mitigations to these to aid progress, and highlighting beneficial activity.
- 4.1.2 With the Inquiry team, maintenance of progress trackers, for example, to create an overview of the progress of video editing and uploading.
- 4.1.3 Prompt highlighting, and efforts to work towards a resolution, of any performance or contractual issues.
- 4.1.4 Daily provision to the Inquiry of identifiers of documents/material referred to in hearings through Inquiry-specified platforms.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

5. VOLUMES

- 5.1 The Inquiry's Opening Statements are running for one week in September 2024 followed immediately by two weeks of impact evidence.
- 5.2 Further impact evidence hearings and then public hearings will run from November 2024 to September 2026. Up to 33 weeks made up of blocks of sitting periods of 2-3 weeks are intended during this time period which includes additional contingency weeks.
- 5.3 A standard hearing week is likely to be 4 sitting days per week (Mon-Fri), 09:30am – 16:30pm, with specific tasks (such as set-up, testing, transcript finalisation etc.) taking place outside of these hours.

6. CONTINUOUS IMPROVEMENT

- 6.1 The Supplier is expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
- 6.2 The Supplier should present new ways of working to the Authority during quarterly Contract review meetings.
- 6.3 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed upon prior to any changes being implemented.

7. SUSTAINABILITY / SOCIAL VALUE

- 7.1 The supplier should include examples of how they help deliver social value through their work, with regards to how they demonstrate action to support health and wellbeing, including physical and mental health, in the contract workforce.
- 7.2 The Authority follows the Social Value model created by the Government and that include 5 themes and 8 policy outcomes. This contract supports:

Theme 2: Tackling economic inequality. MAC 3.3: Modernising delivery and increasing productivity

Activities that demonstrate and describe the tenderer's existing or planned:

- Understanding of scalable and future-proofed new methods to drive greater modernisation of delivery and increase productivity.
- Approach to organisational learning and continuous improvement.
- Creation of a design and tendering environment that is conducive to the development of scalable and future-proofed new methods to modernise delivery and increase productivity

8. QUALITY

- 8.1 The Supplier must have a proven track record of supporting and delivering high-quality AV services, at a high-profile inquiry or inquest, or similar proceedings in the last 5 years.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

9. PRICE AND BUDGET

- 9.1 All potential suppliers are required to itemise the price of goods/and services per hearing day for sitting days/weeks and per week for non-sitting weeks.
- 9.2 Prices must be itemised per service function, number/quantity of items equipment provided, design and set up/rigging, de-rigging, staff costs etc.
- 9.3 Prices are to be submitted via the Atamis procurement portal response document 3-Commercial Envelope excluding VAT and including all other expenses relating to Contract delivery.
- 9.4 The maximum budget for this contract is £2,920,000 ex VAT.

10. STAFF AND CUSTOMER SERVICE

- 10.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
- 10.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
- 10.3 The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract. Terms of Reference can be found here <https://lampardinquiry.org.uk/terms-of-reference/>

11. SERVICE LEVELS AND PERFORMANCE

- 11.1 The Authority will measure the quality of the Supplier's delivery by (indicative SLAs to be finalised prior to the contract being finalised):

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

SLA	Service Area	KPI/SLA description	Target
1	Video Redaction	Redaction of videos of public hearings to be completed and shared with identified Inquiry team point of contact for sign-off within one week of hearing being complete	98%
2	Video publication	Videos of public hearings to be published within one calendar day of approval from identified Inquiry team point of contact	98%
3	Transcript redaction	<p>Supplier to provide the identified Inquiry team point of contact with a redacted transcript for review and publication, ready for publication, within 4 hours of the hearing day concluding (publication of transcript dependent on Inquiry team approval)</p> <p>Failure to comply with this SLA would result in the deduction of 5% of the invoice for each hearing day when the SLA is not met (where it is the fault of the supplier)</p>	100%
4	Core infrastructure	<p>The availability of the core platform infrastructure is 99.9% uptime with support available Monday to Friday 09.30 – 17.30 excluding public holidays</p> <ul style="list-style-type: none"> Issues regarding the connectivity of the core infrastructure should be resolved in one hour (in instances 	99.9% and connectivity issues resolved in 1 hour

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

		<p>where this issue is with supplier's software)</p> <p>Failure to comply with this SLA would result in the deduction of 5% of the overall invoice for each hearing day when the SLA is not met (where it is the fault of the supplier)</p>	
5	Site visit and lay out recommendations	In-person visits to all proposed hearing venues made at request of Inquiry team with one week notice. Proposed layouts provided to Inquiry team within one week of visit taking place.	90% of all requests

12. SECURITY AND CONFIDENTIALITY REQUIREMENTS

- 12.1 All personnel must hold valid security clearances to BPSS level at a minimum. Higher security clearance may be required for specific roles if handling sensitive information (e.g. evidence handler).
- 12.2 All activity undertaken by the supplier must comply with the Data Protection Act, and the Inquiry's Privacy Information Notice in particular with regard to the collection and storage of personal data

13. PAYMENT AND INVOICING

- 13.1 The payment profile for this Call-Off Contract is monthly in arrears.
- 13.2 The Supplier will issue electronic invoices monthly in arrears.
- 13.3 The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
- 13.4 All invoices must include a valid Purchase Order number, Contract reference and a clear, transparent breakdown of the charges.
- 13.5 Invoices will be sent to the Buyer monthly.
- 13.6 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
- 13.7 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.
- 13.8 Invoices should be submitted to: The Lampard Inquiry, C/O DHSC, 39 Victoria Street, London SW1H 0EU, UK

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

14. CONTRACT MANAGEMENT

- 14.1 Supplier attendance at quarterly Contract Review meetings (either in-person or virtual) shall be at the Supplier's own expense.

15. LOCATION

- 15.1 The location of services will be carried out at the Inquiry's hearing centres [REDACTED]
[REDACTED] Venue locations will be confirmed 2 months before hearings take place.
- 15.2 There may be occasion for further or other hearings to be held remotely.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Order Schedule 5 (Pricing Details)

Line Number	Requirement	Quantity	Price per item per sitting hearing day	Total Cost per sitting hearing day	Price per item per non sitting hearing day	Total Cost per non sitting hearing day
1. Hearing Room						
1						

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning

Project Version: v1.1

Model Version: v1.3

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

6						
2. Back Office						
1						

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning
Project Version: v1.1
Model Version: v1.3

T		T	
----------	--	----------	--

3

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Figure 1 displays a sequence of 8 panels arranged in a 2x4 grid, illustrating the evolution of a black pattern on a white background. The top row shows the initial state (leftmost panel) and the first three steps of evolution. The bottom row shows the next three steps, including the formation of a complex structure (third panel from the top row) and its subsequent simplification (fourth panel from the top row).

[illegible]

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

--	--

Day Rates

Line Number	Requirement	Product/Service Description	Quantity	Price per item or rate per sitting hearing day	Price per item or rate per non sitting hearing day
Services + Equipment					

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning

Project Version: v1.1

Model Version: v1.3

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

3					

DPS Schedule 6 (Order Form Template and Order Schedules)
Crown Copyright 2020

Order Schedule 9 (Security) Part B: Long Form Security Requirements

1. Definitions

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

"Breach of Security"	<p>means the occurrence of:</p> <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/or b) 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, <p>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;</p>
"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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

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:

[REDACTED]
[REDACTED]

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 3.6.

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 a Further Competition 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

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

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 (Tiers 1-4)(<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 3.3 shall be deemed to be references to such items as developed and

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

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 3.3, 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 3.6 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 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

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

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;

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- 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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- 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 d.
- 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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- 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;

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- 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 3.3.5;
 - 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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

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 National Cyber Security Centre ("NCSC") to at least Foundation Grade, for example, under the NCSC 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 NCSC 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;

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- 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 NCSC, 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 NCSC certification (<https://www.ncsc.gov.uk/section/products-services/ncsc-certification>) 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

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Order Schedule 14 (Service Levels)**1. Definitions**

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

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"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;

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning

Project Version: v1.1

Model Version: v1.3

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

- (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).
- 2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:
 - 2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
 - 2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
 - 2.5.3 there is no change to the Service Credit Cap.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

- 3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
- 3.2 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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Supplier:

- 1.1 is likely to or fails to meet any Service Level Performance Measure; or
- 1.2 is likely to cause or causes a Critical Service Failure to occur,

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

- 1.a.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
- 1.a.2 instruct the Supplier to comply with the Rectification Plan Process;
- 1.a.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
- 1.a.4 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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

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

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Core infrastructure	Availability	99.9% uptime with support available Monday to Friday 09.30 – 17.30 excluding public holidays	99.9% connectivity and issues regarding the connectivity of the core infrastructure should be resolved in one hour (in instances where this issue is with supplier's software)	Failure to comply with this SLA would result in the deduction of 5% of the overall invoice for each hearing day when the SLA is not met (where it is the fault of the supplier)
Video Redaction	Completion	Redaction of videos of public hearings to be completed and shared with solicitor team for sign-off within one week of hearing being complete	98%	Failure to comply with this SLA would result in the deduction of 5% of the overall invoice for each hearing day when the SLA is not met (where it is the fault of the supplier)

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Video publication	Completion	Videos of public hearings to be published within one calendar day of approval from lead solicitor	98%	Failure to comply with this SLA would result in the deduction of 5% of the overall invoice for each hearing day when the SLA is not met (where it is the fault of the supplier)
Transcript redaction	Completion	Supplier to provide the Inquiry solicitor with a redacted transcript for review and publication, ready for publication, within 4 hours of the hearing day concluding (publication of transcript dependent on solicitor approval)	100%	Failure to comply with this SLA would result in the deduction of 5% of the overall invoice for each hearing day when the SLA is not met (where it is the fault of the supplier)

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

- 3.1 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.
- 3.2 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:
 - 3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
 - 3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;
 - 3.2.3 details of any Critical Service Level Failures;
 - 3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
 - 3.2.5 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
 - 3.2.6 such other details as the Buyer may reasonably require from time to time.
- 3.3 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:
 - 3.3.1 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;
 - 3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and
 - 3.3.3 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.
- 3.4 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.
- 3.5 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.

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

4. Satisfaction Surveys

- 4.1 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 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

Number	Award Criterion	Question and Guidance	Weighting	Maximum Word Count
Q1	<ul style="list-style-type: none"> Meeting the AV requirements 	<ul style="list-style-type: none"> Please demonstrate how you will deliver the requirements as detailed in section 5 (Scope of Requirement), section 6 (The Requirement) and section 7 (Key Milestones and Deliverables) of 'Attachment 2 - Statement of Requirements' at the hearing site. Your response should include but should not be limited to: <ul style="list-style-type: none"> Please demonstrate how your skilled/qualified staff will conduct specific aspects of the requirement. Please reference the tools and services you will utilise to deliver the requirements. 	60%	1500 Words

Insert answer to Q1 in box below:

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

[illegible]

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

[illegible]

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning
Project Version: v1.1
Model Version: v1.3

Number	Award Criterion	Question and Guidance	Weighting	Maximum Word Count
		[REDACTED]		
I		[REDACTED]		
I		[REDACTED]		
I		[REDACTED]		
I		[REDACTED]		
I		[REDACTED]		
I		[REDACTED]		
		[REDACTED]		
Q2	Maintaining quality and providing contingency	• Please demonstrate how you will ensure a quality service is provided for all key Inquiry hearing stakeholders (for example the Chair, Counsel, Core Participants, legal teams, the media, the public etc.):	25%	1000 Words

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Number	Award Criterion	Question and Guidance	Weighting	Maximum Word Count
		<ul style="list-style-type: none"> • Please demonstrate how you will use previous experience of delivering similar audio-visual services (to those outlined in 'Attachment 2-Statement of requirements') to ensure a quality service is maintained throughout the life of the contract. • Please demonstrate how you will add value, deliver efficiencies and innovation to achieve maximum value while ensuring the quality of the service is not compromised. 		

Insert answer to Q2 in box below:

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning
Project Version: v1.1
Model Version: v1.3

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning
Project Version: v1.1
Model Version: v1.3

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

Number	Award Criterion	Question and Guidance	Weighting	Maximum Word Count
Q3	Maintaining quality and providing contingency	<ul style="list-style-type: none"> Please demonstrate the contingency measure you will put in place if the Inquiry's hearings required to change at short notice including: <ul style="list-style-type: none"> Move to alternative hearing venue Move to wholly virtual or hybrid (part in person, part virtual): <ul style="list-style-type: none"> How you will maintain a quality service in the event of remote hearings. How you will deal with changes to the Inquiry's plans, including, but not limited to, changes to venue, hearing dates or the number of hearings. How you will minimise risks in the delivery. 	15%	1000 Words

Insert answer to Q3 in box below:

• [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

[illegible]

DPS Ref: RM6225 Audio Visual Technical Consultancy & Commissioning
Project Version: v1.1
Model Version: v1.3

DPS Schedule 6 (Order Form Template and Order Schedules)
Crown Copyright 2020

Social Value Response:

Introduction

[Redacted text block]

- [Redacted list item]

2. Strengthening Digital Infrastructure

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

[Redacted Content]

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020

5. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

6. **Promoting Continuous Learning and Development**

[REDACTED]

[REDACTED]

DPS Schedule 6 (Order Form Template and Order Schedules)

Crown Copyright 2020



The image shows a large rectangular box with a black border. Inside the box, there are four horizontal black bars of varying lengths, representing redacted content. The bars are arranged vertically, with the first bar being the longest, followed by a shorter one, then another long one, and finally a shorter one at the bottom.

DPS Schedule 6 (Order Form Template and Order Schedules)
Crown Copyright 2020