Crown Commercial Service

G-Cloud 11 Call-Off Contract (version 4)

Contents

Part A - Order Form

Digital Marketplace service ID number:	257481873902339
Call-Off Contract reference:	CCSO20A80 Provision of a Foundry Data Connector - Technical Feasibility Evaluation (TFE)
Call-Off Contract title:	Provision of Border and Customs Management Services - Technical Feasibility Evaluation (TFE) and Initialisation
Call-Off Contract description:	Contract for the provision of: Phase 1 – Free Technical Feasibility Evaluation; and Phase 2 – Provision of Base Licence for Palantir Foundry and Initialisation Services. Item 24: PT-CAP-BASE - Single environment base Foundry Licence Item 41: PT-CAP-INIT -5 - Capability 5 initialisation – payable in and for 1st year of new capability. Inclusive of a maximum of 15 quarters of implementation services at an 8% discount and a maximum of 1,058 hours of training services, to be utilised in the initialisation year, and a one year Capability Licence. Item 58: IMPL REP Implementation and Engineering Services. Per Person, Per Quarter. Subject to Option Year being triggered: Item 42: PT-CAP-ON-5 - Capability 5 ongoing Capability Licence fee, payable on a per annum basis following the 1st year of capability 5 initialisation, inclusive of a maximum of 1,058 hours of training services, to be utilised on a per annum basis.
Start date:	31 August 2020
Expiry date:	Initial Period shall expire on 30 August 2021 Option to extend for further periods (to not exceed 2 such further periods) of up to 12 months each.
Call-Off Contract value:	Year 1 (Initialisation Period) = £7,850,000 for 12 months Options: Year 2 and 3 = £6,125,000 for each 12 month period (Payment profile as set out at Schedule 2 of this Call-Off Contract)
Charging method:	In accordance with Schedule 2 (Call-Off Contract Charges)

Purchase order number:	To be issued

This Order Form is issued under the G-Cloud 11 Framework Agreement (RM1557.11).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From: the Buyer	Minister for the Cabinet Office (as part of the Crown) as represented by the Cabinet Office 1 Horse Guards Road, London, SW1A 1HQ
To: the Supplier	Palantir Technologies UK, Ltd, New Penderel House, 4th Floor, 283-288 High Holborn, London WC1V 7HP (Registered number 07042994) +44 (0) 203 856 8404
Together: the 'Parties'	

Principal contact details

For the Buyer:	Title: Director, Contingency and Locations Name [redacted] Email: [redacted] Phone [redacted]
For the Supplier:	Title: Business Development Lead (UK Government) Name: [redacted] Email: [redacted] Phone: [redacted]

Call-Off Contract 'Term'

Start date:	The terms and conditions set out herein shall be effective from 31 August 2020. This Call-Off Contract Starts on 31 August 2020 and is valid for an Initial Period of 12 months.
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums or at least 30 days from the date of written notice for Ending without cause.

	The initial contractual Expiry Date is 30 August 2021. If an Option Year is triggered, the Expiry Date shall be the date falling 12 months after the start date of the period of extension (or such other period as may be agreed by the Parties). Such term is subject, at all times, to the Buyer's right to end the Contract under clause 18 of Part B - Terms and conditions.

Extension period:	This Call-Off Contract can be extended by the Buyer for 2 period(s) of up to 12 months in total each, by giving the Supplier no less than 2 weeks written notice before expiry of the (then) current Term. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. The extension period after 12 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each. Under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS) if the: ● Buyer is a central government department ● contract Term is intended to exceed 24 months

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 2- Cloud software Lot 3 - Cloud support
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: ● **Phase 1: Technical Feasibility Evaluation of the Data Connector Tool (free trial)** This work shall be provided by the Supplier for free for any potential Participating Department and at any time during the Term (including HMRC, HO, Defra, Department for Transport, Driver and Vehicle Standards Agency, Highways England and Port Health Authorities). The initial Participating Departments for this Phase 1 activity will be HMRC and Home Office, following the satisfactory completion of which, the contract will move onto Phase 2 activity. During Phase 2, the Supplier will also deliver TFE Phase 1 activity to other Participating Departments (those other than Home Office and HMRC) at no additional cost .

	● **Phase 2 – (Year 1) Code 24 (Base Licence for Palantir Foundry) and Code 41 (Size 5 Capability) Border Flow Management Capability: Initialisation.** ● **Phase 2 – (Optional Extension Years) – Code 24 (Base Licence for Palantir Foundry) and ongoing licence fees for Code 42 (size 5 Capability) Border Flow Management Capability** 15 Bundled Implementation Quarters in Year 1 1058 Bundled Training Hours In Year 1 and 1058 hours in Year 2. Phase 1 will be offered to each of the Participating Departments, each of which may have different timescales for completion. On that basis, Phase 1 could still be in place for a Participating Department whereas Phase 2 may already have commenced for Home Office and HMRC. The transition to Phase 2 and the payment terms that relate to Phase 2 will occur irrespective of whether there are Participating Departments still conducting Phase 1 TFE activity
Additional Services:	Additional Implementation services related to the Service are within the scope of this Call-Off Contract and will be ordered and paid for by the Buyer using the relevant product code as set out in the Supplier' product page on the Digital Marketplace.
Location:	The Services will be delivered to the Buyer on a remote basis. The Supplier shall store all Buyer Data in a separate dedicated partition of the Foundry SaaS platform, such partition to be for the exclusive use of Her Majesty's Government (acting as the Crown) and to be hosted in the Amazon Web Service London region.
Quality standards:	The quality standards required for the Services are set out in the Call-Off Contract.
Technical standards:	The technical standards required for the Services are set out in the Call-Off Contract.
Service level agreement:	The Supplier shall provide support services in relation to the Services in accordance with the "Palantir Service Level Agreement" in effect at the time.
Onboarding:	The on-boarding plan for the Services are as set out in the Call-Off Contract.
Offboarding:	The offboarding plan for the Services are as set out in the Call-Off Contract.
Collaboration agreement:	A collaboration agreement is not required to commence the project with Home Office and HMRC. However, should Participating Departments require it, the Supplier will use commercially reasonable endeavours to enter into collaboration agreement(s) substantially in the form of the Collaboration Agreement with third party IT providers who provide the Participating Departments' IT service, if deemed necessary by the Buyer and/or a Participating Department
Limit on Parties' liability:	In respect of all Phase 1 Services the Supplier agrees that it is creating, developing and providing the Crown with a Technical Feasibility Evaluation at entirely its own risk and cost. To the extent permitted by law, the Crown hereby excludes all liability in respect of any damage or other losses incurred by the Supplier as a result of any Technical Feasibility Evaluation being carried out by the Supplier (for the avoidance of doubt, this

	exclusion of liability does not apply to any damage or other losses incurred by the Supplier in respect of Phase 2 activity, which shall be subject to the liability provisions set out Clause 24). In respect of any other Services provided by the Supplier, the Parties' liability shall be as follows: A) The annual total liability of either Party for all Property defaults will not exceed ten million pounds (£10,000,000) B) The annual total liability for all Buyer Data defaults, in accordance with, but not limited to, any breaches of Clause 13 (Buyer Data), Clause 33 (Data Protection Legislation), Schedule 7 (GDPR Information) arising under this Call-Off Contract or arising in respect of the equivalent "Buyer Data defaults" provisions under the Access Agreements, will not exceed thirty million pounds (£30,000,000). C) The annual total liability for all other defaults will not exceed 125% of the Charges paid by the Buyer to the Supplier during the Call-Off Contract Term. Except for (B) above (which in relation to Supplier Buyer Data defaults, shall be the Supplier's entire limit of liability to the Crown for such defaults arising under this Call-Off Contract and/or under any Access Agreement), the Supplier's liability under this Call-Off Contract shall be without prejudice to (and shall be in addition to) any Supplier liability which arises under an Access Agreement.
Insurance:	The insurance(s) that the Supplier shall be required to hold to deliver the Services shall be: ● For a minimum insurance period of 6 year following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law ● Public Liability insurance cover will have a minimum of £1,000,000 for each individual claim ● Cyber and Data insurance cover will have a minimum total limit of indemnity of £10,000,000
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 90 consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits: 7.4 to 7.13

Buyer's responsibilities:	The Supplier is responsible for the delivery of the Services.
Buyer's equipment:	None. The Services will be delivered electronically and utilise a cloud hosted network infrastructure.

Supplier's information

Subcontractors or partners:	The Supplier will provide Palantir Foundry Cloud Services for use with Amazon Web Services. The Supplier also uses Proofpoint for email encryption and Datadog for telemetry.

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method:	The payment method for this Call-Off Contract is BACS
Payment profile:	The Payment Profile for this Call-Off Contract is set out at Schedule 2 (Call-Off Contract Charges)
Invoice details:	The Supplier will issue electronic invoices : i) Annually upfront in respect of the Base Licence; and ii) Quarterly in arrears in respect of the Capability Licence and any Additional Implementation Fees (if applicable) The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	APinvoices-CAB-U@gov.sscl.com
Invoice information required – for example purchase order, project reference:	All invoices must have clear breakdown so that there is full transparency and detail in relation to : 1) The Services Provided 2) The Department that is receiving the Service 3) The Purchase Order Number 4) Detailed breakdown of the services provided 5) Summary of the development work completed pursuant to that invoice 6) Planned vs completed work. 7) Departmental % breakdown of service provision.
Invoice frequency:	Invoice will be sent to the Buyer on a quarterly basis
Call-Off Contract value:	The initial value of this Call-Off Contract is £7,850,000 for Year 1 At discretion of Buyer, this will increase by £6,125,000 per year for each full Option Year exercised. If both extension options are fully exercised, the value of this Call-Off

	Contract will be £20,100,000. This excludes any Additional Implementation that the Buyer, in its discretion, may purchase.
Call-Off Contract charges:	The breakdown of the Charges is set out at Schedule 2 (Call-Off Contract Charges)

Additional Buyer terms

Performance of the service and deliverables:	(a) This Call-Off Contract will require the Supplier, during Phase 1 activity, to evaluate the feasibility of using the Palantir Data Connector to extract information from the Participating Departments' systems; to provide the Foundry Base Licence; and during Phase 2, to provide initialisation services for the Border Flow Service; as more particularly set out in the Statement of Requirements and elsewhere in this Call-Off Contract. (b) Buyer Data will be hosted in the UK in a separate dedicated partition of the Palantir Foundry System, such partition to be for the exclusive use of Her Majesty's Government (acting as the Crown) and to be hosted in the Amazon Web Service London region.
Guarantee:	Not appliable
Warranties, representations:	not used
Supplemental requirements in addition to the Call-Off terms:	In order to access a Participating Department's information and systems in order to evaluate the feasibility the Data Connector Tool and deploy it into the production environment; and to use such information and systems to develop the Border Flow Service, the Supplier shall be required to enter into an Access Agreement, as more particularly set out at Schedule 8 – Additional Term (A). .
Buyer specific amendments to/refinements of the Call-Off Contract terms:	The Supplier shall comply with the additional requirements/refinements at: Schedule 8 (Buyer Specific Amendments) Schedule 9 (Security) Schedule 10 (Service Continuity Plan) The Services provide for installation of the Products on Amazon Web Services infrastructure;
Public Services Network (PSN):	Not applicable
Personal Data and Data Subjects:	Where identified in the relevant Access Agreement, Personal Data may be provided directly to the Supplier by certain Participating Departments. The Terms and Conditions which govern the provision and use of that Personal Data shall be as set out

	in the Access Agreements to be entered into directly between the Supplier and the Participating Department and also in Annex 1 to Schedule 7. Where Personal Data is transferred by the Buyer to the Supplier directly and where the Buyer is an independent Data Controller in respect of such Personal Data, such transfer shall be subject to the terms of this Call-Off Contact

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.11.

(B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Supplier	Buyer
Name:	Matt Long	[Enter text]
Title:	General Counsel	[Enter text]
Signature:	X_____	X_____
Date:	[Enter text]	[Enter text]

Schedule 1 - Services

[redacted]

Schedule 2 - Call-Off Contract charges

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	

[redacted]

	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Part B - Terms and conditions

1. Call-Off Contract start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)

- 8.49 to 8.51 (Publicity and branding)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.58 (data protection)
- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)
- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

- a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- a reference to 'CCS' will be a reference to 'the Buyer'
- a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as 'incorporated Framework clause XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
- are confident that they can fulfil their obligations according to the Call-Off Contract terms
- have raised all due diligence questions before signing the Call-Off Contract
- have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within

10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

- a broker's verification of insurance
- receipts for the insurance premium

- evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- promptly notify the insurers in writing of any relevant material fact under any insurances
- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

- premiums, which it will pay promptly
- excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.78 to 8.86. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't

obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

- rights granted to the Buyer under this Call-Off Contract
- Supplier's performance of the Services
- use by the Buyer of the Services

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

- modify the relevant part of the Services without reducing its functionality or performance
- substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
- buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.7 Clause 11.5 will not apply if the IPR Claim is from:

- the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
- other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

- comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data
- only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
- take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection Legislation

and following the Buyer's instructions

- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
- providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

The Supplier must not remove any proprietary notices in the Buyer Data.

13.1 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policy and all Buyer requirements in the Order Form.

13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

- the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets at https://www.cpni.gov.uk/protection-sensitive-information-and-assets
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/collection/risk-management-collection
- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6 The Buyer will specify any security requirements for this project in the Order Form.

13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

- Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
- Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start Date:

- an executed Guarantee in the form at Schedule 5

- a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
- an Insolvency Event of the other Party happens
- the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if

clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.87 to 8.88 (Waiver and cumulative remedies)
- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- work with the Buyer on any ongoing work
- return any sums prepaid for Services which have not been delivered to the Buyer, within 10

Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

Manner of delivery	**Deemed time of delivery**	**Proof of service**
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement

Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code Of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the

Supplier's possession, power or control

- other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start Date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms

and conditions, other than in the ordinary course of business.

29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

- its failure to comply with the provisions of this clause
- any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start Date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

- work proactively and in good faith with each of the Buyer's contractors
- co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.57 and 8.58 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.57 and 8.58 are reproduced in this Call-Off Contract document at schedule 7

Schedule 3 - Collaboration agreement

This agreement is made on [enter date]

between:

1) [Buyer name] of [Buyer address] (the Buyer)
2) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
3) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
4) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
5) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]
6) [Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

together (the Collaboration Suppliers and each of them a Collaboration Supplier).

Whereas the:

- Buyer and the Collaboration Suppliers have entered into the Call-Off Contracts (defined below) for the provision of various IT and telecommunications (ICT) services
- Collaboration Suppliers now wish to provide for the ongoing cooperation of the Collaboration Suppliers in the provision of services under their respective Call-Off Contract to the Buyer

In consideration of the mutual covenants contained in the Call-Off Contracts and this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions and interpretation

1.1 As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:

- "Agreement" means this collaboration agreement, containing the Clauses and Schedules
- "Call-Off Contract" means each contract that is let by the Buyer to one of the Collaboration Suppliers
- "Contractor's Confidential Information" has the meaning set out in the Call-Off Contracts
- "Confidential Information" means the Buyer Confidential Information or any Collaboration Supplier's Confidential Information
- "Collaboration Activities" means the activities set out in this Agreement
- "Buyer Confidential Information" has the meaning set out in the Call-Off Contract
- "Default" means any breach of the obligations of any Collaboration Supplier or any default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties
- "Detailed Collaboration Plan" has the meaning given in clause 3.2
- "Dispute Resolution Process" means the process described in clause 9
- "Effective Date" means [insert date]

- "Force Majeure Event" has the meaning given in clause 11.1.1
- "Mediator" has the meaning given to it in clause 9.3.1
- "Outline Collaboration Plan" has the meaning given to it in clause 3.1
- "Term" has the meaning given to it in clause 2.1
- "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales

1.2 General

1.2.1 As used in this Agreement the:

1.2.1.1 masculine includes the feminine and the neuter

1.2.1.2 singular includes the plural and the other way round

1.2.1.3 A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment.

1.2.2 Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.

1.2.3 References to Clauses and Schedules are, unless otherwise provided, references to clauses of and schedules to this Agreement.

1.2.4 Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.

1.2.5 The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

2. Term of the agreement

2.1 This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the "Term").

2.2 A Collaboration Supplier's duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

3. Provision of the collaboration plan

3.1 The Collaboration Suppliers will, within 2 weeks (or any longer period as notified by the Buyer in writing) of the Effective Date, provide to the Buyer detailed proposals for the Collaboration Activities they require from each other (the "Outline Collaboration Plan").

3.2 Within 10 Working Days (or any other period as agreed in writing by the Buyer and the Collaboration Suppliers) of [receipt of the proposals] or [the Effective Date], the Buyer will prepare a plan for the Collaboration Activities (the "Detailed Collaboration Plan"). The Detailed Collaboration Plan will include full details of the activities and interfaces that involve all of the Collaboration Suppliers to ensure the receipt of the services under each Collaboration Supplier's respective [contract] [Call-Off Contract], by the Buyer. The Detailed Collaboration Plan will be based on the Outline Collaboration Plan and will be submitted to the Collaboration Suppliers for approval.

3.3 The Collaboration Suppliers will provide the help the Buyer needs to prepare the Detailed Collaboration Plan.

3.4 The Collaboration Suppliers will, within 10 Working Days of receipt of the Detailed Collaboration Plan, either:

3.4.1 approve the Detailed Collaboration Plan

3.4.2 reject the Detailed Collaboration Plan, giving reasons for the rejection

3.5 The Collaboration Suppliers may reject the Detailed Collaboration Plan under clause 3.4.2 only if it is not consistent with their Outline Collaboration Plan in that it imposes additional, more onerous, obligations on them.

3.6 If the parties fail to agree the Detailed Collaboration Plan under clause 3.4, the dispute will be resolved using the Dispute Resolution Process.

4. Collaboration activities

4.1 The Collaboration Suppliers will perform the Collaboration Activities and all other obligations of this Agreement in accordance with the Detailed Collaboration Plan.

4.2 The Collaboration Suppliers will provide all additional cooperation and assistance as is reasonably required by the Buyer to ensure the continuous delivery of the services under the Call-Off Contract.

4.3 The Collaboration Suppliers will ensure that their respective subcontractors provide all co-operation and assistance as set out in the Detailed Collaboration Plan.

5. Invoicing

5.1 If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.

5.2 Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

6. Confidentiality

6.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.

6.2 Each Collaboration Supplier warrants that:

6.2.1 any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement

6.2.2 any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party

6.2.3 it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors

6.2.4 neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise

6.3 The provisions of clauses 6.1 and 6.2 will not apply to any information which is:

6.3.1 or becomes public knowledge other than by breach of this clause 6

6.3.2 in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party

6.3.3 received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure

6.3.4 independently developed without access to the Confidential Information

6.3.5 required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction

6.4 The Buyer's right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier's Confidential Information provided under this Agreement and the Collaboration Supplier's right, obligations and liabilities in relation to using and disclosing any of the Buyer's Confidential Information provided under this Agreement, will be as set out in the [relevant contract] [Call-Off Contract].

7. Warranties

7.1 Each Collaboration Supplier warrant and represent that:

7.1.1 it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier

7.1.2 its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes

7.2 Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

8. Limitation of liability

8.1 None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.

8.2 Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.

8.3 Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to [(£ ,000)].

8.4 Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to [Buyer to specify].

8.5 Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the [relevant contract] [Call-Off Contract]), in no event will any party be liable to any other for:

8.5.1 indirect loss or damage

8.5.2 special loss or damage

8.5.3 consequential loss or damage

8.5.4 loss of profits (whether direct or indirect)

8.5.5 loss of turnover (whether direct or indirect)

8.5.6 loss of business opportunities (whether direct or indirect)

8.5.7 damage to goodwill (whether direct or indirect)

8.6 Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:

8.6.1 additional operational or administrative costs and expenses arising from a Collaboration Supplier's Default

8.6.2 wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

9. Dispute resolution process

9.1 All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.

9.2 If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.

9.3 The process for mediation and consequential provisions for mediation are:

9.3.1 a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties that he is unable or unwilling to act, apply to the Chairman of the Law Society to appoint a Mediator

9.3.2 the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations

9.3.3 unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings

9.3.4 if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives

9.3.5 failing agreement, any of the parties may invite the Mediator to provide a non-binding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties

9.3.6 if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts

9.4 The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

10. Termination and consequences of termination

10.1 Termination

10.1.1 The Buyer has the right to terminate this Agreement at any time by notice in writing to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier's [respective contract] [Call-Off Contract].

10.1.2 Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their [relevant contract] [Call-Off Contract]. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

10.2 Consequences of termination

10.2.1 Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will continue to comply with their respective obligations under the [contracts] [Call-Off Contracts] following the termination (however arising) of this Agreement.

10.2.2 Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

11. General provisions

11.1 Force majeure

11.1.1 For the purposes of this Agreement, the expression "Force Majeure Event" will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.

11.1.2 Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.

11.1.3 A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.

11.1.4 The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.

11.1.5 The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

11.2 Assignment and subcontracting

11.2.1 Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub-license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.

11.2.2 Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the subcontractors.

11.3 Notices

11.3.1 Any notices given under or in relation to this Agreement will be deemed to have been properly

delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.

11.3.2 For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

11.4 Entire agreement

11.4.1 This Agreement, together with the documents and agreements referred to in it, constitutes the entire agreement and understanding between the parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.

11.4.2 Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.

11.4.3 Nothing in this clause 11.4 will exclude any liability for fraud.

11.5 Rights of third parties

11.5.1 Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.6 Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

11.7 Variations

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

11.8 No waiver

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

11.9 Governing law and jurisdiction

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

For and on behalf of the Buyer

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

Collaboration Agreement Schedule 1 - List of contracts

Collaboration supplier	Name/reference of contract	Effective date of contract

[Collaboration Agreement Schedule 2 - Outline collaboration plan]

Schedule 4 - Alternative clauses

Not used

Schedule 5 – Guarantee

Not used

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software. For the Supplier, the Supplier Products (as defined below).
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Call-Off Contract), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').

Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Call-Off Contract, including any Personal Data Breach
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: i) (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; iii) (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.11 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.

Government Procurement Card	The Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR

Processor	Takes the meaning given in the GDPR.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security Management Plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.

Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - GDPR Information

Any Personal Data which is included in the Buyer Data and which will be used for the purposes of delivery of the Services may be Controlled by either the Participating Department; or by the Buyer, as determined by the Crown. Where the Crown has determined that the Buyer shall be the Data Controller of such Personal Data, Annex 1 of this Schedule 7 shall be updated to reflect this position (in accordance with Clauses 1.5 and 1.6 of Annex 1), and this Call-Off Contract shall govern the Controller/Processor relationship for the purposes of the GDPR. Where the Crown has determined that the Participating Department shall remain the Data Controller of any Personal Data it has made available; the Access Agreement between the Participating Department and the Supplier shall govern the Controller/Processor relationship for the purposes of the GDPR.

Notwithstanding the above, Personal Data which is Controlled by the Buyer may be provided by a Participating Department directly to the Supplier

For reference, where Personal Data is provided by the Participating Department, the appropriate GDPR templates which are required to be completed in accordance with Framework Incorporated Clauses 8.57 and 8.58 are to be included within the Access Agreements.

The provisions of Schedule 4 of the Framework Agreement are deemed incorporated into this Call-Off Contract ("incorporated Framework Schedule 4"); as amended pursuant to Clause 2.2 of Part B (Terms and Condition); which will cover any Personal Data provided to the Supplier for which the Buyer is the Data Controller.

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller (the Buyer), 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 Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are: *Steve Jones, DPO, Cabinet Office, steve.jones@cabinetoffice.gov.uk*

1.2 The contact details of the Supplier's Data Protection Officer are: *Brendan Cooney, dpo@palantir.com*

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

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

1.5 This Annex 1 shall be reviewed on a regular basis by the Controller and shall be amended from time to time and notified to the Supplier (and the Controller shall take into account the view of the Processors, but the final decision as to the content of any updated Annex shall be with the Buyer at its absolute discretion)

1.6 The Buyer and/or a Participating Department shall not be required to share with the Supplier any Buyer Data which has not been included in this Annex 1 (where the Buyer is the Data Controller of such Buyer Data) or in an equivalent data processing schedule set out in an Access Agreement (where the Participating Department with the Access Agreement is the Data Controller of such Buyer Data)

Data Processing Table

Description	**Details**

Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2-15 of incorporated Framework Schedule 4 (Where one Party is a Controller and the other Party its Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the Personal Data provided by the Buyer (or at the direction of the Buyer) for the purposes of the delivery by the Supplier of the Services, Nature and purpose of Processing Data Processed in accordance with the Agreement may be subject to the following Processing activities: • performance by Palantir of activities necessary to provide products or services or otherwise perform its obligations under the Agreement; • disclosures in accordance with the Agreement, or as compelled by law.
Duration of the Processing	The Term of the Agreement (as set out in the Call-Off Order Form for this Call-Off Contract) plus the period from the expiry of the Term until the return or deletion of all Customer Personal Data by the Supplier in accordance with the Agreement and applicable law.
Nature and purposes of the Processing	Data Processed in accordance with the Agreement may be subject to the following Processing activities: • performance by the Supplier of activities necessary to provide products or services or otherwise perform its obligations under the Agreement; • disclosures in accordance with the Agreement, or as compelled by law The specific purposes for the processing are described below The aim of the project is the provision of Border Management Capability as described herein.
Type of Personal Data	In order to provide the Services or otherwise perform its obligations under the Agreement, the Supplier will process the Personal Data provided or made available to the Supplier in relation to the Agreement.
Categories of Data Subject	Data Subjects include the individuals about whom data is provided to the Supplier via the Services or otherwise by (or at the direction of) the Buyer or Buyer's users who are authorised to use the Services. These may include, but are not limited to, the following:(i) Employees, contractors, or agents of the Buyer (who are natural persons); (ii) the Buyer's users

	authorized to use the Service; (iii) the Buyer's clients, customers, or other users of the Buyer's products or services; (iv) member of the public; and/or (v) Third parties with which the Buyer conducts business and in each case, they include former, present, and/or prospective individuals in these categories.
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	Notwithstanding anything else in the Framework Agreement and / or the Call-off Contract, The Parties agree that the terms of the Supplier's terms "STANDARD EU CONTRACTUAL CLAUSES (PROCESSORS)" below shall apply to this Call-Off Contract in respect of the limited redacted telemetry data (audit and usage logs) which the Supplier sends to its Cloud Operations and Infosec teams (as permitted under Clause N1.3 of Annex A to Schedule 8).

STANDARD EU CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Minister for the Cabinet Office (as part of the Crown) as represented by the Cabinet Office, referred to as the "Buyer" in the Agreement, on behalf of itself and other entities it may receive data from or provide access to Palantir's software and services to.

(each a "**data exporter"**)

And

Name of the data importing organisation:

Palantir Technologies Inc., on behalf of itself and as an agent for and on behalf of all legal entities it directly or indirectly controls located outside of the European Economic Area, and which are from time to time serve as data processors in respect of the personal data processed by or on behalf of the data importer.

Address: 1555 Blake Street, Suite 250, Denver, Colorado 80202

(the "**data importer**")

each a "**party**"; together the "**parties**",

HAVE AGREED on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free

movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have

become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with

the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information,

in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will

accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the relevant data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data

exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the relevant data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the relevant data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of a data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES [CONFIDENTIAL]

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is, a public body that is identified in the Agreement.

Data importer

The data importer is a software company (including, where applicable, its subsidiaries and affiliates) which may from time to time process personal data upon the instruction of the data exporter in accordance with the terms of these Clauses and the G-Cloud Framework Agreement and Call-Off Contract entered into by (1) Palantir Technologies UK, Limited and (2) Minister for the Cabinet Office (as part of the Crown) as represented by the Cabinet Office (the "Agreement").

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The data subjects are users of software and services.

Categories of data

The personal data transferred concern the following categories of data (please specify):

- The data to be processed may include, but is not limited to:
  - Email, login and usage information required for the provision of software and services.

Special categories of data (if appropriate)

- The personal data transferred concern the following special categories of data (please specify):
  - The data importer does not access sensitive personal data in the ordinary performance of the services. Notwithstanding the foregoing, the data importer may access sensitive

personal data only where such access is lawful and critical in the provision of the services.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Data analytics, problem solving and data hosting and maintenance services, as defined and pursuant to the Agreement and these Clauses.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES [CONFIDENTIAL]

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The data importer will maintain appropriate administrative, physical, technical, and organizational measures against unauthorised or unlawful processing of, accidental loss, destruction or damage to, and for protection of the security, confidentiality, and integrity of personal data, including any requirements relating to such measures set out in the Agreement between the parties.

Schedule 8 – Buyer Specific Amendments

New Definitions

	"Access Agreement"	means an agreement (which will include where required, suitable data protection provisions and other specific Participating Department provisions) entered into between the Supplier and a relevant Participating Department, as required under Clause A of this Schedule 8;
	"**Border Flow Data**"	means information and data provided by a Participating Department and/or the Cabinet Office which is used for the Border Flow Service;
	"Border Flow Service"	is the service to be configured by the Supplier (under the Border Management Capability) pursuant to Phase 2 of this Call-Off Contract, namely a suite of tools for the visualisations of data and analysis, and creation of action-recommendation workflows based on a data asset of close-to-real time data related to the volume of consignments crossing the UK border. This data shall be pulled from source systems in Home Office, HMRC and other Participating Departments and combined with data about traffic volumes. It will provide key indicators on the flow and throughput of goods at and around the border to support wider government understanding of flow at the border. Strategically the Border Flow Service will sit alongside a suite of products owned by the Border Protocol and Delivery Group that combine to deliver a breadth of analytic and insight capability.
	"Crown IPR"	means any IPR which is owned by the Crown;
	"Derived Data"	means any information and/or data which has been derived, created, aggregated, generated, extracted or otherwise obtained as a result of any Processing, modification, adaptation, aggregation or other use of Buyer Data, including, without limitation, any information and/or data relating to patterns, trends, commercial positions, or other insights identified in the Buyer Data;
	"Data Connector Tool"	means the Supplier data connector software to be deployed locally by Participating Departments during Phase

		1 activity for each Participating Department which will be used to extract data from Participating Departments' systems;
	"Encrypted"	means encrypted using unbroken cryptographic algorithms and incapable of being deprecated through opportunistic controls;
	"Phase 1"	means the phase where the Supplier conducts a technical feasibility evaluation (at the Supplier's own cost) with a Participating Department to assess whether the Supplier's Data Connector Tool can be used to obtain the necessary Border Flow Data from a Participating Department's system and (where successful) deploy that Data Connector Tool;
	"Technical Feasibility Evaluation"	means the Services being provided by the Supplier pursuant to any Phase 1 delivery;
	"**Tool Design Plan"**	means the plans as more particularly described in Additional Term (C) in this Schedule 8
	"Phase 2"	means the period described as such in the Statement of Requirements;
	"Participating Department"	means a public body which the Cabinet Office has notified the Supplier is a body whose information/data needs to be ingested by the Border Flow Service
	"Statement of Requirements"	means the statement of requirements document set out at Schedule 1 (Services);
	"Product Background IPR"	means Background IPR in a specific packaged and commoditised product that is offered to the market;
	"Open Source Publication Material"	means items created pursuant to the Call-Off Contract which the Buyer may wish to publish as Open Source;
	"Supplier Documentation"	means the technical specification documentation provided to Buyer by Supplier regarding the Supplier Software, Supplier Materials, and Data Connector Tool.
	"Supplier Materials"	means any data, technology, and materials provided or made available to Buyer by Supplier for use pursuant to this Call-Off Contract, including sample code, software

		libraries, command line tools, data integration code, templates, and configuration files;
	"Supplier Product(s)"	means, together, the Supplier Software, Supplier Materials, and Supplier Documentation
	"Supplier Software"	means the Supplier proprietary software in a managed cloud-hosted environment, any third-party software, the Data Connector Tool, application programming interfaces (APIs), and models or algorithms; which are identified in the Call-Off Contract or provided or made available the Buyer as a service in connection with Call-Off Contract and any improvements, modifications, enhancements, derivative works, patches, upgrades, and Updates to any of the foregoing that Supplier provides to Buyer hereunder.
	"Updates"	means changes in Supplier Software that Supplier at its discretion may implement in the applicable generally available Supplier Software or Documentation without requiring the payment of additional fees. Updates do not include new product (capabilities, modules, extensions, or equivalent) or service offerings that Supplier makes available for an additional charge.

Amendments to Schedule 6 – Glossary and interpretations

	"Background IPRs"	Shall be replaced with: Means for each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or

		For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software. For the Supplier, the Supplier Products.
	"Buyer Data"	shall be replaced with: a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any Buyer's and Participating Department's Confidential Information and which: i) are supplied to the Supplier by or on behalf of the Buyer and/or a Participating Department; or ii) the Supplier generates, processes, stores or transmits pursuant to this Call-Off Contract; or iii) any Personal Data for which the Buyer and/or Participating Department is the Data Controller; or iv) any other content (including models and related code) that is created or provided by the Buyer or the Participating Departments, for transmission, storage, integration, import, display, distribution or use in or through use of the Supplier's cloud Service solution, including any aggregated or transformed versions thereof and any analytical output; and b) includes Derived Data and the Border Flow Data;
	"Project Specific IPRs"	shall be replaced with: Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract and derived from Buyer Data including databases, configurations, code, instructions, technical documentation and

		schema *but not* including the Supplier's Background IPRs and, for the avoidance of doubt, Supplier Products.

Additional Terms and Conditions: Clauses

Clause	Description	Wording
A.	**Access Agreement**	1.1 The Supplier shall use commercially reasonable efforts to enter into a legally binding Access Agreement with each Participating Department in a form required by the relevant Participating Department. 1.2 The Supplier acknowledges and agrees that each Participating Department will have its own specific technical, security, information/data policy and law, legal and other requirements which it must comply with. The purpose of the Access Agreement is to ensure that the Supplier's access and use of information, data and systems is compliant with the Participating Departments' policies and legal obligations. 1.3 The terms of each Access Agreement will provide no less favourable terms to each Participating Department than those in place with the Buyer under this Call-Off Contract, except in relation to the limits of liability for Buyer Data defaults, where the Supplier's total liability to the Buyer and any Participating Department under this Call-Off Contract and the Access Agreements, shall be limited as set out in the Limits on Parties' liability section of the Order Form;. 1.4 The Parties will work together in good faith and in a timely manner to agree and execute the Access Agreement during any Phase 1 delivery. 1.5 The Participating Departments may require such Access Agreements to be in place before the Supplier is given access to the Participating Departments' systems and information. 1.6 In the event that the Supplier is granted access to any Participating Department's systems or information prior to executing an Access Agreement, the Supplier agrees to indemnify the relevant Participating Department for any liabilities, costs, expenses, damages and losses suffered or incurred by that Participating Department as a result of the Supplier's access to its systems and information. The Parties agree that each Participating Department

		shall be entitled to claim directly against the Supplier under this paragraph 1.6 and the Supplier's liability for such claims shall not be subject to the limits on liability set out in Part B to this Call-Off Contract. The Supplier acknowledges and agrees that: 1.6.1 the Buyer has no obligation in respect of the provision of the Participating Departments' information and data, and any provision of information of such information and data shall be subject to and conditional upon agreement of an Access Agreement with the relevant Participating Department pursuant to clauses A1.1 to A1.5 above.; and 1.6.2 where the Buyer is to provide information and data directly to the Supplier in relation to any Participating Department, any provision of such information and data shall be subject to and conditional upon a legal gateway being established between the Buyer and the Participating Department and the conditions required to establish such legal gateway are outside of the control of the Buyer and Participating Department.
B.	**Schedule 9 - Security**	The additional provisions set out at Schedule 9 of this Call-Off Contract shall be incorporated.
C.	**Security Assurance**	1.1 At the request of the Buyer, the Supplier shall: 1.1.1 in respect of any Phase 1 delivery (in relation to the Data Connector Tool); and 1.1.2 in respect of Phase 2 delivery (in relation to its general development of the Border Flow Service); provide the Buyer (and specifically the Buyer's security assurance team) with a detailed plan setting out its proposals for the implementation of the Supplier Software (each, a "Tool Design Plan") 1.2 The Tool Design Plans shall be sufficiently detailed and must provide the Buyer and its security team with sufficient information to enable them to fully consider and assess risks around the Data Connector Tool and Border Flow Service and to enable the Buyer and its security team to consider any controls which may need to be put in place to neutralise or mitigate those risks to acceptable levels.

		1.3 The Supplier shall, if requested, submit a draft of the Tool Design Plan to the Buyer: 1.3.1 In respect of the Data Connector Tool: as soon as reasonably practicable upon notification by the Buyer that a Participating Department is to be onboarded (but following any reasonable period of due diligence which the Supplier may need to undertake before it can develop the plan); and 1.3.2 In respect of the Palantir Foundry System: as soon as reasonably practicable at the commencement of any Phase 2 work. 1.4 The Supplier shall not execute the Tool Design Plan unless: 1.4.1 The Buyer has approved the plan; and 1.4.2 the relevant Access Agreements are in place which provide authority to the Supplier to proceed with those items of the Tool Design Plan which are subject to additional Participating Department terms and conditions. 1.5 If the Buyer rejects the Tool Design Plan, the Supplier shall use reasonable endeavours to promptly update the Tool Design Plan and resubmit it for Approval, taking into account any reasonable requests from the Buyer and its security team. 1.6 Notwithstanding the Approval of the Tool Design Plan, the Supplier acknowledges and agrees that design and integration of the Tool will need to comply with the security requirements set out in this Call-Off Contract and those set out in any Access Agreement (including any specific requirements specified by the Buyer's security assurance team). 1.7 The Supplier shall update the Tool Design Plans and resubmit them for Approval whenever there is any change to the circumstances which has the potential to affect the risk profile of the Tool and/or the Supplier's plans for the Tools need to be amended. Until the updated Tool Design Plan is Approved, the Supplier shall continue to comply with the latest Approved version of the Tool Design Plan(s).
D. `	**Schedule 10 – Service Continuity Plan**	The additional provisions set out at Schedule 10 of this Call-Off Contract shall be incorporated.

E.	**Order Of Precedence**	**Order of Precedence** If there is any conflict or ambiguity between the Call-Off Contract and an Access Agreement, the Supplier shall notify the Cabinet Office as soon as is reasonably practicable. The Cabinet Office will liaise with the Supplier and the affected Participating Department(s) in good faith; and shall notify the Supplier of which provision shall prevail.
F.	**Future Procurement**	1.1 If the Buyer or a Participating Department acting in its absolute discretion, chooses to procure the Services in the future, it will be required by the Public Contract Regulations 2015 (as updated, amended or replaced from time to time) (the **PCR**) to carry out such a procurement via a fair and transparent competition. The Supplier agrees to assist the Buyer or other Participating Department to comply with its obligations under the PCR including but not limited to: 1.1.1 supplying all information in respect of the Services which the Buyer or other Participating Department may reasonably be expected use in an invitation to tender; 1.1.2 if invited to tender, using a different bid team to those who developed the Border Flow Service 1.1.3 establishing ethical walls between any bid team and the team who developed the Border Flow Service. to the extent that such measures are reasonably necessary in order to secure compliance with: the Public Contracts Regulations 2015; the TFEU Treaty Principles and/or any Cabinet Office policies in relation to procurement. 1.2 This clause F shall survive the termination of this Call-Off Contract.
G.	**Termination**	1.1 Where the Buyer Ends this Call-Off Contract pursuant to Clause 18, it shall only be liable for Services and licences (on a prorated basis) which have been delivered up to the End Date specified in the notice. 1.2 In addition, the Supplier shall refund all pre-paid fees relating to any periods after the End Date (including any licence fees (pro-rated) pre-paid in respect of

		such periods) in accordance with the worked example set out at Schedule 2. 1.3 The Buyer shall not be liable for any further charges except as expressly provided for under Clause 18.3 of the Call-Off Contract.
H.	**Phase 1**	1.1 To avoid any doubt, at no time under this Call-Off Contract shall the Crown be required to pay the Supplier any sum for or in relation to any Phase 1 activity or for any ongoing or future use by the Crown of the Data Connector Tool aside from the fees specified in this Call-Off Contract.
I.	**Additional Security Requirements**	1.1 The Supplier acknowledges and agrees that Phase 1 activity and Phase 2 development work may reveal additional security risks to the Buyer and the Participating Departments. 1.2 The Parties shall work in good faith and in a timely manner to agree any additional security provisions which need to be included within this Call-Off Contract and/or within an Access Agreement. 1.3 The Parties shall review the security provisions during any Phase 1 activity and at regular intervals during Phase 2 activity. Any changes to the security provisions shall be subject to the Variation Process. 1.4 The Supplier acknowledges and agrees that security is of paramount importance to the Buyer and Participating Departments, and in the event that the Supplier cannot agree to a security requirement that is reasonably required by the Buyer and/or a Participating Department, the Buyer may End this Call-Off Contract without liability.
J.	**Personal Data**	In addition to the provisions set out in this Call-Off Contract which relate to the protection of Personal Data and Buyer Data, the Supplier shall comply with all provisions relating to the protection of Personal Data and other information/data, as may be provided to the Supplier by a Participating Department and as more particularly set out in the relevant Access Agreement.

K.	**Phase 1 (TFE) and Phase 2 Acceptance Criteria**	The Supplier shall ensure that the following high level success criteria are satisfied at the relevant testing stages: See attachment Phase 1 (TFE) & Phase 2 Acceptance criteria - Final - 2020921
L.	**Not Used**	
M.	**Intellectual Property Rights**	Clauses 11.1, 11.2, and 11.4 shall be deleted. Clause 11.8 shall be amended to read: "If the Supplier does not comply with Clause M as set out at Annex A to this Schedule 8, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services." The definitions and provisions set out under Clause M at Annex A to this Schedule 8 shall be incorporated.
N.	**Additional Buyer Data and Derived Data Provisions**	The provisions set out under Clause N at Annex A to this Schedule 8 shall be incorporated.
O.	**Documentation**	The provisions set out under Clause O at Annex A to this Schedule 8 shall be incorporated.
A.	**Tool Removal**	The Data Connector Tool shall be removed by the Supplier at no cost on request by the Buyer (unless the Buyer chooses to

		remove the Tool itself, in which case the Supplier shall provide all reasonable assistance at no cost to Buyer to facilitate its removal of the Tool).
B.	**Not Used**	
C.	**Incorporated Framework Clauses**	A further bullet point shall be added to Clause 2.2 of Part B (Terms and Conditions) as follows: ● where a Framework Agreement clause has been incorporated under Clause 2.1 of Part B (Terms and Conditions), a reference in an incorporated Framework Clause to a 'Schedule' shall be a reference to that Schedule as incorporated into this Call-Off Contract
D.	**Schedule 7(GDPR) – Annex 1. Data Processing Schedule**	The Parties acknowledge and agree that the nature of the Services and the use of different Participating Department data means that not all Personal Data and Data Processing activity can be identified at the Start Date. The Parties agree that Annex 1 of Schedule 7 (GDPR) shall be kept under review and shall be updated in accordance with paragraph 1.5 and 1.6 of Annex 1 to Schedule 7 (GDPR) to ensure that it covers such Personal Data before it is Processed.
E.	**Rights of Third Parties**	Clause 27 shall be amended to read: 27.1 Except as specified in clause 29.8 and Clause A1.6 (Additional terms and Conditions) of Schedule 8 (Specific Buyer Amendments), a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

Annex A

M. INTELLECTUAL PROPERTY RIGHTS

1. Allocation of title to IPR

1.1 Save as expressly granted elsewhere under this Call Off Contract:

(a) the Buyer shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Supplier or its licensors, namely:

(i) the Supplier Product;

(ii) the Supplier Background IPR; and

(ii) any third party IPR.

(b) the Supplier shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Buyer or its licensors, including the:

(I) Buyer Background IPR;

(ii) Project Specific IPRs; and

(ii) Crown IPRs.

1.2 Where either Party acquires, by operation of Law, title to Intellectual Property Rights that is inconsistent with the allocation of title set out in Clause M1.1, it shall assign in writing such Intellectual Property Rights as it has acquired to the other Party on the request of the other Party (whenever made).

1.3 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services, nor shall a Party make any announcements or statements in relation to any of its products or services that it is endorsed, sanctioned or otherwise approved by the other (except to the extent permitted under the Framework Agreement where the Supplier is offering its products and services as a Framework Supplier) without the other Party's prior written consent.

1.4 Where requested by the Buyer:

(a) Project Specific IPR Items shall be created in a format able to be converted into a format, which is:

(i) suitable for publication by the Buyer as Open Source; and

(ii) based on Open Standards (where applicable);;

(b) where the Project Specific IPR Items are written in a format that requires conversion before publication as Open Source or before complying with Open Standards, the Buyer is responsible for such conversion; but the Supplier shall provide

reasonable assistance to the Buyer to make the conversion.

1.5 References to the Buyer's Background IPRs in this Call-Off Contract includes Crown IPRs and any Background IPRs which are owned and/or licensed to a Participating Department.

1.6 Notwithstanding anything to the contrary in this Call-Off Contract, the Parties acknowledge that save for the grant of limited licence described below at 3(a) there is no transfer of rights in Supplier Product.

2 Assignments granted by the Supplier: Project Specific IPR

2.1 The Supplier hereby assigns to the Buyer with full guarantee (or shall procure from the first owner the assignment to the Buyer), title to and all rights and interest in the Project Specific IPRs. The assignment under this Clause M2.1 shall take effect as a present assignment of future rights that will take effect immediately on the coming into existence of the relevant Project Specific IPRs.

2.2 The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Project Specific IPRs are properly transferred to the Buyer.

2.3 Subject to Clause M2.4, to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Project Specific IPRs (but only after Supplier has failed to separate out such Project Specific IPRS from Supplier Background IPRs or third party IPRs), the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use and sub-licence any Supplier Background IPRs (or part thereof) or third party IPRs (or part thereof) that are embedded in or which are an integral part of the Project Specific IPR Items (except for any rights in relation to the Supplier Product, or and any third party Product Background IPRs, which shall be otherwise agreed between the Parties subject to entering into acceptable commercial terms)

2.4 The Supplier shall ensure that the items in which the Project Specific IPRs subsist which are developed by the Supplier or made available to the Buyer via the Supplier Product, are created in a format and structure which complies with good industry standard practices in respect of portability and interoperability; so that the Buyer can obtain the full benefit of such Project Specific IPRs after the End Date without needing a licence to any Supplier Background IPRs or any third party IPRs in respect of those Project Specific IPRs.

3 Licences granted by the Supplier: Supplier Background IPR

3.1 Subject to paragraph (b) below, Clause 2 (Grant of Limited Licence) of the Supplier Terms (Palantir Licence Terms and Conditions (Licence)) (as those terms appear in the GCloud Marketplace hosted by CCS at the date of this Call-Off Contract) shall

apply in full as Supplier Terms, save as expressly varied below in 3(b) and 3(c). Such Licence is for the sole and exclusive purpose of the Border Management Capability. Defined terms in the Licence bear the same meanings where used in this Call-Off Contract;

3.2 During the term of this Call-Off contract and subject always to the prior agreement of Supplier, the Buyer has the right to sublicence the Supplier Product to Participating Departments.

3.3 The Buyer acknowledges that its use of the Services (as described in Schedule 1) is for its internal business purposes and strictly in relation to the Border Flow Service. It further acknowledges that the same restrictions applies to any sublicences that it may grant to Participating Departments.

4 Not used

5 Buyer's right to assign/novate Supplier licences

5.1 The Buyer may assign, novate or otherwise transfer its rights and obligations under Clause M3.1 to:

5.1.1 any Central Government Body;

5.1.2 any body (including any private sector body) controlled by the Crown; and

5.1.3 subject to the prior written approval of the Supplier (not to be unreasonably withheld or delayed), any body (including any private sector body) which is partially controlled by the Crown;

which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

6 Third Party IPR

6.1 The Supplier shall procure that the owners or the authorised licensors of any third party IPR which the Supplier uses in the delivery of the Services and which is reasonably required by the Buyer in order to make use of those Services grants a licence that is equivalent to that granted by the Supplier under Clause M3.1

6.2 If the Supplier cannot obtain for the Buyer a licence that is equivalent with the terms set out in Clause M3.1 in respect of any such third party IPR, the Supplier shall:

(a) notify the Buyer in writing giving details of what licence terms can be obtained from the relevant third party and whether there are alternative arrangements which could be used; and

(b) shall only use such third party IPR if the Buyer approves the terms of the licence from the relevant third party.

6.3 Without prejudice to any other right or remedy of the Buyer, if the Supplier becomes aware at any time, including after Ending and/or the Expiry Date, that any Intellectual Property Rights for which the Buyer does not have a licence in accordance with Clause 2.3 subsist in the Project Specific IPR Items, then the Supplier must notify the Buyer within 10 days of what those rights are and which parts of the Project Specific IPR Items they are found in.

7 Licence granted by the Buyer

Buyer IPRs

7.1 The Buyer hereby grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call Off Contract Period to use the Buyer Background IPR and the Project Specific IPRs solely to the extent necessary for providing the Services in accordance with this Call Off Contract including (but not limited to) the right to grant sub-licences to Subcontractors provided that the Supplier shall not without Approval use the materials licensed under this Clause for any other purpose other than the delivery of the Services to the Buyer and/or Participating Departments.

8 Termination of licenses

8.2 The licence granted pursuant to Clause M7 shall terminate automatically on the Expiry Date or End Date (whichever is the earlier) and the Supplier shall:

(a) immediately cease all use of the Buyer Background IPR (including the Buyer Data within which the Buyer Background IPR may subsist);

(b) at the discretion of the Buyer, return or destroy documents and other tangible materials that contain any of the Buyer Background IPR and the Buyer Data, provided that if the Buyer has not made an election within six months of the termination of the licence, the Supplier shall (subject to the duty to notify under Schedule 9 (Security Management Plan), destroy the documents and other tangible materials that contain any of the Buyer Background IPR and the Buyer Data (as the case may be); and

(c) ensure that any Buyer Background IPR and Buyer Data that are held in electronic, digital or other machine-readable form ceases to be accessible from any computer, word processor, voicemail system or any other device of the Supplier containing such Buyer Background IPR and/or Buyer Data.

9 Open Source Publication

9.1 Subject to Clause 9.2, the Supplier agrees that the Buyer may subject to prior consultation with Supplier publish as Open Source all or part of the Project Specific IPR Items, provided always that such publication will not infringe Supplier Products.

9.2 Where the Buyer has approved a request by the Supplier for any part of the Project Specific IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Background IPRs, Supplier Products, and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

(a) as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

(b) include in the written details provided under Clause 9.2(a) information about the impact that inclusion of such IPRs and items or Deliverables based on such IPRs will have on any other Project Specific IPRs items and the Buyer's ability to publish such other items or Deliverables as Open Source.

N. ADDITIONAL BUYER DATA AND DERIVED DATA PROVISIONS

1.1 The Supplier acknowledge and agrees that the Buyer Data (which includes the Derived Data) is confidential and commercially sensitive to the Buyer and Participating Departments.

1.2 Subject to Clause N1.3, the Supplier shall not:

a) process the Buyer Data and shall not create any Derived Data, except as expressly permitted under this Call-Off Contract or as otherwise instructed by Buyer;;

b) use any Buyer Data for inclusion in or for the development of, any Supplier product or service other than the Services as delivered to the Buyer under this Call-Off Contract;

c) collect, perform or retain any inspection, analysis, aggregation, evaluation, reproduction, metrics or analytics of Buyer Data or use Buyer Data or any information derived from it as the basis for any product or service,

1.3 The Supplier may use Buyer Data for the provision of the Services, namely:

a) for purposes relating to the information security of the Services (but only to the extent that such processing is reasonably required); and

b) purposes relating to usage and diagnostics data for the purposes of analysis, maintenance and improvement of the Supplier Product and services, but only to the extent that:

i) the data relates only to the performance, management and efficiency metrics of the Supplier Product; and

ii) the data is not Personal Identifying Information.

1.5 In respect of any Buyer Data which is Personal Data, the Supplier shall not take or permit Supplier Staff to take any action directed towards: the identification of any data subject, the reversal of any pseudonymisation applied to such data, the attribution of personal data to a data subject or the acquisition or processing of any additional information in pursuit of any of those objectives, unless otherwise requested by Buyer as part of Service performance.

O. DOCUMENTATION AND EXIT

1.1 The Supplier shall ensure that, for the purposes of retender and exit, it prepares explanatory documentation in relation to all initialisation and configuration work with a reasonably sufficient level of detail and transparency of process to enable the Buyer to reasonably understand how that work has been created, as may be relevant to the development of a Border Flow Service (provided that, and without prejudice to Clause M of this Annex A, a Replacement Supplier shall not be entitled to receive any of the Supplier's commercially sensitive information contained in documentation)

Schedule 9 – Security

Part 1 – Security Aspects Letter

This document is a Security Aspects Letter (SAL) issued by the Cabinet Office Border Flow Service for the Services.. It defines the security provisions which the Palantir project team shall comply with in dealing with information and delivery of Phase 1 and Phase 2 of the Services. The Security requirements set out in this Schedule are those that are required by the Buyer. These provisions shall apply to all aspects of Service delivery. In addition, the Supplier shall comply with any additional security requirements as may be required by a Participating Department and agreed between the Participating Department and the Supplier in a separate Access Agreement.

It is necessary that the material relating to the Border Flow Service must be protected. Baseline protection controls are defined by the Security Policy Framework and NCSC guidance, varying with the level of protective marking. Material passed to you will bear the protective marking appropriate to it.

To assist you in allocating any necessary protective marking to material which the Services may produce during the development and implementation of the project and thus enable you to provide the appropriate degree of protection to it, this letter formally advises you of the correct protective marking to apply to the various aspects of the project and the correct method of storing and transmitting such information.

Classification Level

The overall level of security classification of the activities related to this project is up to OFFICIAL caveated SENSITIVE and may include Personal Identifiable Information.

Mandatory Security Requirements

1. **Designing and managing secure solutions**

Palantir shall implement their solution to mitigate the security risks in accordance with the NCSC's Software as a Service Security Principles https://www.ncsc.gov.uk/collection/saas-security/saas-security-principles https://www.ncsc.gov.uk/collection/cyber-security-design-principles.

Palantir must assess their systems against the NCSC Cloud Security Principles: https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. Palantir must document that assessment and make that documentation available to the Cabinet Office on request.

2. **Data Processing, Storage, Management and Destruction**

Palantir must not Process any Government Data outside the UK without written authorisation from the Cabinet Office which may impose conditions on that permission.

Palantir must ensure that all Government Data is Encrypted at rest and in transit.

Palantir must securely erase any or all Government Data held by Palantir when requested to do so by the Cabinet Office.. Prior to any such deletion Supplier will notify the Buyer of its intention to delete and the means through which it will achieve such deletion.

3. **Palantir must ensure that only the minimum number of staff required have access to the Border Management System and a written list must be maintained of all staff having such access along with their clearance levels. This list must be provided to the Cabinet Office.Personnel Security**

Palantir must perform appropriate checks on their staff before they may participate in the provision and or management of the Border Flow Service. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

Palantir must ensure that any staff with administrative access permissions, which means such persons whohave access to the bulk data provided for or generated by the Border Flow Service, obtain Security Check (SC) clearance in order to Process Government Data.

Palantir must ensure that only the minimum number of staff required have access to the Border Flow Service and a written list must be maintained of all staff having such access along with their clearance levels. This list must be provided to the Cabinet Office.

4. **End User Devices**

Palantir shall ensure that any Government Data stored (for any period of time) on a mobile, removable or physically uncontrolled device is Encrypted. Palantir must follow the Information Commissioner's Office guidance on implementing encryption, which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/.

Palantir shall ensure that any device used to process Government Data meets all the security requirements set out in the NCSC End User Devices Platform Security Guidance, which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

Palantir must put technical controls in place and disable any ports to prevent any downloading of bulk data from the End User Devices of Supplier.

5. **Networking**

Palantir shall ensure that any Government Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be Encrypted when transmitted.

6. **Patching and Vulnerability Scanning**

Palantir must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.

7. **Third Party Subcontractors**

Palantir must not transmit or disseminate the Border Flow Service data to any other person or entity unless specifically authorised by the Cabinet Office. Such authorisation must be in writing to be effective and may be subject to conditions.

Palantir must not, when performing any part of the Border Management System, use any software to process the Border Flow Service data where the licence terms of that software purport to grant the licensor rights to process the Government Data greater than those rights strictly necessary for the use of the software.

Protective Marking – Aspects

The aspects of the project that require to be protectively marked are:

Aspect	Protective Marking
Existence of the Project	OFFICIAL
Totality of bulk data	OFFICIAL - SENSITIVE
Personal Identifiable Information (PII)	OFFICIAL - SENSITIVE
Documentation that details contractual matters relevant to the project	OFFICIAL - COMMERCIAL
General system description documentation with no specific details of the aspects listed below.	OFFICIAL
Other Documentation	OFFICIAL
Details of Software used in the development or operational environment (Dependent on function)	OFFICIAL
Firewalls, Switches, Routers (Dependent on network used for certain aspects)	OFFICIAL
System Administration projects	OFFICIAL
Hosting Platforms (Dependent on content)	OFFICIAL
Auditing	OFFICIAL
Specific and explicit information relating to the interconnection detail and existence of other inter-connected networks and domains	OFFICIAL

It is possible that other sensitive matters will be identified during the development and support of this project. When such matters are identified, Palantir will be instructed on the protective marking assigned to that particular subject and any restrictions relevant to its dissemination and use.

You are requested to acknowledge receipt of this letter and to confirm that the levels of protective marking associated with the requirements listed above have been brought to the attention of the individuals directly responsible for the provision of the Border Flow Service. Additionally, that they are fully understood, and that the required security controls can and will be taken to safeguard the material concerned.

Schedule 9 Part 2 – Security Management

1. Definitions

In this Schedule, in addition to those other definitions in the Agreement, the following definitions shall apply:

"Cabinet Office Premises"	premises owned, controlled or occupied by the Crown which are made available for use by Palantir or its Sub-contractors for provision of the Border Flow Service
Cabinet Office System	the Cabinet Office's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Cabinet Office or Palantir in connection with this Call-Off Contract which is owned by the Cabinet Office or licensed to it by a third party and which interfaces with the Palantir System or which is necessary for the Cabinet Office to receive the Border Flow Service;
" Risk Management Documentation"	has the meaning given in Paragraph 6.3;
" Information Management System"	means the Core Information Management System and the Wider Information Management System;
"Accreditation"	the assessment of the Core Information Management System in accordance with Paragraph 6 by the Cabinet Office or an independent information risk manager/professional appointed by the Cabinet Office, which results in an Accreditation Decision;
"Accreditation Decision"	is the decision of the Cabinet Office, taken in accordance with the process set out in Paragraph 6, to issue Palantir with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;
"Accreditation Plan"	Palantir's plan to attain an Accreditation Approval Statement from the Cabinet Office, which is prepared by Palantir and approved by the Cabinet Office in accordance with Paragraph 6.4;
"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Cabinet Office Premises, the Sites, Palantir System, the Cabinet Office System and/or any information or

	data (including the Confidential Information and the Crown Information) used by the Cabinet Office, Palantir or any Sub-contractor in connection with this Call-Off Contract; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Crown Information), including copies of such information or data, used by the Cabinet Office, Palantir or any Sub-contractor in connection with this Call-Off Contract; and/or (c) any part of Palantir System ceasing to be compliant with the Certification Requirements, in each case as more particularly set out in the security requirements in Schedule 5 Part 1 and the Baseline Security Requirements;
"Certification Requirements"	the requirements set out in Paragraph 7;
"Core Information Management System"	the specific account for the Buyer on the Cloud Software which will be used by the Supplier and the Buyer to build and operate the capabilities of the Border Flow Service. In so-doing, the Core Information Management System may Process Crown Information and comprises those information assets, ICT systems and/or Sites which will be used by Palantir and/or its Sub-contractors to Process Crown Information, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources, which the Cabinet Office has determined in accordance with Paragraph 4.2 shall be subject to Accreditation;
"**Information"**	all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form
"IT Health Check"	has the meaning given Paragraph 8.1.1;
"**Palantir System"**	the Supplier's Commercial Off-the-Shelf technology, provided to the Buyer as a SaaS offering, on which the Core Information

	Management System runs and using which the Border Flow Service capabilities are implemented. This includes but is not limited to any software, equipment, configuration and management utilities, calibration and testing tools and related cabling(but excluding the Cabinet Office System);
Personal Data	has the meaning given in the Data Protection Legislation;
Personal Data Breach	has the meaning given in the Data Protection Legislation;
Personal Data Processing Statement	sets out: (i) the types of Personal Data which Palantir and/or its Sub-contractors are Processing on behalf of the Cabinet Office; (ii) the categories of Data Subjects whose Personal Data Palantir and/or its Sub-contractors are Processing on behalf of the Cabinet Office; the nature and purpose of such Processing; (iii) the locations at which Palantir and/or its Subcontractors Process Crown Information; and, (iv) the Protective Measures that Palantir and, where applicable, its Subcontractors have implemented to protect the Crown Information against a Security Breach including a Personal Data Breach, which shall be prepared by Palantir in accordance with Paragraph 6.4 of this Schedule 5 Part 2 (Security Management) and included in the Risk Management Documentation;
"Process Crown Information"	any operation which is performed on Crown Information, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing, structuring, transmitting or otherwise using Crown Information;
"Required Changes Register"	is a register which forms part of the Risk Management Documentation which records each of the changes that Palantir has agreed with the Cabinet Office shall be made to the Core Information System and/or the Risk Management Documentation as a consequence of the occurrence of any of the events set out in Paragraph 6.13.1 to 6.13.8 together with the date on which each such change shall be implemented and the date on which each such change was implemented;

“Restricted Country”	is any country identified as a restricted country by any department of the Crown from time to time
"Risk Management Approval Statement"	a notice issued by the Cabinet Office which sets out the information risks associated with using the Core Information Management System and confirms that the Cabinet Office is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Cabinet Office;
"Risk Management Reject Notice"	has the meaning given in Paragraph 6.7.2;
"Security Test"	has the meaning given Paragraph 8.1; and
“**Sites**”	any premises (including the Cabinet Office Premises, the Palantir’s premises or third party premises): (a) from, to or at which: (i) the Border Flow Service is (or is to be) provided; or (ii) Palantir manages, organises or otherwise directs the provision or the use of the Border Flow Service; or (b) where: (i) any part of the Palantir System is situated; or (ii) any physical interface with the Cabinet Office System takes place
"Statement of Information Risk Appetite"	has the meaning given in Paragraph 5.1;.
"Vulnerability Correction Plan"	has the meaning given in Paragraph 8.3.3(a); and
"Wider Information Management System"	those information assets, ICT systems and/or Sites which will be used by Palantir and/or its Sub-contractors to Process Crown Information which have not been determined by the Cabinet Office to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources.

2. Introduction

2.1 This Schedule sets out:

2.1.1 the principles which Palantir shall comply with when performing its obligations under this Call-Off Contract in order to ensure the security of the Crown Information, the Border Flow Service, Border Flow Service and the Agreement Information Management System;

2.1.2 the process which shall apply to the Accreditation of the Core Information Management System in Paragraph 6;

2.1.3 the Certification Requirements applicable to the Wider Information Management System in Paragraph 7;

2.1.4 the Security Tests which Palantir shall conduct during the Term in Paragraph 8;

2.1.5 the Security Tests which the Cabinet Office may conduct during the Term in Paragraph 8.6;

2.1.6 the requirements to patch vulnerabilities in the Core Information Management System in Paragraph 9;

2.1.7 the obligations on Palantir to prevent the introduction of Malicious Software into the Information Management System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Information Management System in Paragraph 10; and

2.1.8 each Party's obligations in the event of an actual or attempted Breach of Security in Paragraph 11.

2.2 Palantir shall not delete or remove any proprietary notices contained within or relating to the Crown Information.

2.3 Palantir shall not store, copy, disclose, or use the Crown Information except as necessary for the performance by Palantir of its obligations under this Call-Off Contract or as otherwise expressly authorised in writing by the Cabinet Office.

2.4 To the extent that Crown Information is held and/or processed by Palantir, Palantir shall supply that Crown Information to the Cabinet Office as requested by the Cabinet Office in the format it specifies.

2.5 Palantir shall preserve the integrity of the Crown Information and prevent the corruption or loss of Crown Information at all times that the relevant Crown Information is under its control or the control of any Sub-contractor.

2.6 Palantir shall perform secure back-ups of all Crown Information and shall ensure that up-to-date back-ups are stored off-site in accordance with the Service Continuity Plan.

2.7 Palantir shall ensure that any system on which Palantir holds any Crown Information, including back-up data, is a secure system that complies with the Security Requirements.

2.8 If at any time Palantir suspects or has reason to believe that Crown Information has or may become corrupted, lost or sufficiently degraded in any way for any reason, then Palantir shall notify the Cabinet Office immediately and inform the Cabinet Office of the remedial action Palantir proposes to take.

2.9 Palantir shall comply with the requirements set out in this Schedule 9 (Security Management)

2.10 The Cabinet Office shall notify Palantir of any changes or proposed changes to the Baseline Security Requirements.

3. Principles of Security

3.1 Palantir acknowledges that the Crown places great emphasis on the confidentiality, integrity and availability of the Crown Information and, consequently on the security of:

3.1.1 Border Flow Service; and

3.1.2 the Information Management System.

3.2 Notwithstanding the involvement of the Cabinet Office in the Accreditation of the Core Information Management System, Palantir shall be and shall remain responsible for:

3.2.1 the security, confidentiality, integrity and availability of the Crown Information whilst that Crown Information is under the control of Palantir or any of its Sub-contractors;

3.2.2 the security of Border Flow Service; and

3.2.3 the security of the Information Management System.

3.3 The Cabinet Office shall monitor and may also provide recommendations to Palantir on the Accreditation of the Core Information Management System.

3.4 Each Party shall provide access to members of its information assurance personnel to facilitate Palantir's design, implementation, operation, management and continual improvement of the Risk Management Documentation and the security of Border Flow Service and the Information Management System and otherwise at reasonable times on reasonable notice.

4. Information Management System

4.1 The Information Management System comprises the Core Information Management System and the Wider Information Management System.

4.2 The Cabinet Office shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Cabinet Office to make such determination, Palantir shall provide the Cabinet Office with such documentation and information that the Cabinet Office may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by Palantir or any Sub-contractor to Process Crown Information together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). The Cabinet Office shall notify Palantir, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.

4.3 Any proposed change to the component parts of and/or boundary of the Core Information Management System shall be notified and processed in accordance with the Variation process (clause 32 Schedule 2).

5. Statement of Information Risk Appetite and Baseline Security Requirements

5.1 Palantir acknowledges that the Cabinet Office has provided and Palantir has received a statement of information risk appetite for Palantir System and the Services (the "**Statement of Information Risk Appetite**").

5.2 The Cabinet Office's Baseline Security Requirements in respect of the Core Information Management System are set out in Annex 1.

5.3 The Statement of Information Risk Appetite and the Baseline Security Requirements shall inform the Accreditation of the Core Information Management System.

6. Accreditation of the Core Information Management System

6.1 The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 6.

6.2 The Accreditation shall be performed by the Cabinet Office or its appointed representatives.

6.3 Prior to the Operational Services Commencement Date, Palantir shall prepare and submit to the Cabinet Office the risk management documentation for the Core Information Management System, which shall comply with,

and be subject to approval by the Cabinet Office in accordance with, this Paragraph 6 (the **Risk Management Documentation**").

6.4 The Risk Management Documentation shall be structured in accordance with the template as set out in Annex 3 and include:

6.4.1 the Accreditation Plan, which shall include:

(a) the dates on which each subsequent iteration of the Risk Management Documentation will be delivered to the Cabinet Office for review and staged approval; and

(b) the date by which Palantir is required to have received a Risk Management Approval Statement from the Cabinet Office together with details of each of the tasks which must be completed by Palantir and the Cabinet Office Responsibilities which must be completed in order for Palantir to receive a Risk Management Approval Statement pursuant to Paragraph 6.7.1

6.4.2 a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;

6.4.3 unless such requirement is waived by the Cabinet Office, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Cabinet Office Premises, the Sites, Palantir System, the Cabinet Office System (to the extent that it is under the control of Palantir) and any IT, Information and data (including the Crown's Confidential Information and the Crown Information) to the extent used by the Cabinet Office or Palantir in connection with this Call-Off Contract or in connection with any system that could directly or indirectly have an impact on the Crown Information, Information, data and/or the Border Flow Service;

6.4.4 the Required Changes Register;

6.4.5 evidence that Palantir and each applicable Sub-contractor is compliant with the Certification Requirements; and

6.4.6 a Personal Data Processing Statement.

6.5 If the Risk Management Documentation submitted to the Cabinet Office pursuant to Paragraph 6.3 (or Paragraph 6.10, as applicable) is approved by the Cabinet Office, it shall be adopted by Palantir immediately and thereafter operated and maintained in accordance with this Schedule. If the Risk Management Documentation is not approved by the Cabinet Office, Palantir shall amend it within 5 Working Days of a notice of non-approval from the Cabinet Office and re-submit it to the Cabinet Office 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 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Cabinet Office. If the Cabinet Office does not approve the Risk Management Documentation following its resubmission, the matter shall be resolved in accordance with clauses 8.64 to 8.77 of Schedule 1. No approval to be given by the Cabinet Office pursuant to this Paragraph may be unreasonably withheld or delayed. However, any failure to approve the Risk Management Documentation on the grounds that it does not comply with the requirements set out in Paragraph 6.4 shall be deemed to be reasonable.

6.6 To facilitate Accreditation of the Core Information Management System, Palantir shall provide the Cabinet Office and its authorised representatives with:

6.6.1 access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and

6.6.2 such other information and/or documentation that the Cabinet Office or its authorised representatives may reasonably require,

to enable the Cabinet Office to establish that the Core Information Management System is compliant with the

Risk Management Documentation.

6.7 The Cabinet Office shall, by the relevant date set out in the Accreditation Plan, review the identified risks to the Core Information Management System and issue to Palantir either:

6.7.1 a Risk Management Approval Statement which will then form part of the Risk Management Documentation, confirming that the Cabinet Office is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Cabinet Office; or

6.7.2 a rejection notice stating that the Cabinet Office considers that the residual risks to the Core Information Management System have not been reduced to a level acceptable by the Cabinet Office and the reasons why (**"Risk Management Rejection Notice"**).

6.8 If the Cabinet Office issues a Risk Management Rejection Notice, Palantir shall, within 10 Working Days of the date of the Risk Management Rejection Notice:

6.8.1 address all of the issues raised by the Cabinet Office in such notice; and

6.8.2 notify the Cabinet Office that the Core Information Management System is ready for an Accreditation Decision.

6.9 If the Cabinet Office determines that Palantir's actions taken pursuant to the Risk Management Rejection Notice have not reduced the residual risks to the Core Information Management System to an acceptable level and issues a further Risk Management Rejection Notice, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Cabinet Office may by terminate this Call-Off Contract with immediate effect on written notice to Palantir.

6.10 The process set out in Paragraph 6.7 and Paragraph 6.8 shall be repeated until such time as the Cabinet Office issues a Risk Management Approval Statement to Palantir or terminates this Call-Off Contract.

6.11 Palantir acknowledges that it shall not be permitted to use the Core Information Management System to Process Crown Information prior to receiving a Risk Management Approval Statement.

6.12 Palantir shall keep the Core Information Management System and Risk Management Documentation under review and shall update the Risk Management Documentation annually in accordance with this Paragraph and the Cabinet Office shall review the Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 6.13.

6.13 Palantir shall notify the Cabinet Office within 2 Working Days after becoming aware of:

6.13.1 a significant change to the components or architecture of the Core Information Management System;

6.13.2 a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;

6.13.3 a change in the threat profile;

6.13.4 a Sub-contractor failure to comply with the Core Information Management System code of connection;

6.13.5 a significant change to any risk component;

6.13.6 a significant change in the quantity of Personal Data held within the Core Information Management System;

6.13.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or

6.13.8 an audit report produced in connection with the Certification Requirements indicates significant concerns,

update the Required Changes Register and provide the updated Required Changes Register to the Cabinet Office for review and approval within 10 Working Days after the initial notification or such other timescale as may be agreed with the Cabinet Office.

6.14 If Palantir fails to implement a change which is set out in the Required Changes Register by the date agreed with the Cabinet Office, such failure shall constitute a material Default and Palantir shall:

6.14.1 immediately cease using the Core Information Management System to Process Crown Information until the Default is remedied, unless directed otherwise by the Cabinet Office in writing and then it may only continue to Process Crown Information in accordance with the Cabinet Office's written directions; and

6.14.2 where such Default is capable of remedy, Palantir shall remedy such Default within the timescales set by the Cabinet Office and, should Palantir fail to remedy the Default within such timescales, the Cabinet Office may terminate this Call-Off Contract with immediate effect on written notice to Palantir.

6.15 Palantir shall review each Change Request against the Risk Management Documentation to establish whether the documentation would need to be amended should such Change Request be agreed and, where a Change Request would require an amendment to the Risk Management Documentation, Palantir shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change Request for consideration and approval by the Cabinet Office.

6.16 Palantir shall be solely responsible for the costs associated with developing and updating the Risk Management Documentation and carrying out any remedial action required by the Cabinet Office as part of the Accreditation process.

7. Certification Requirements

7.1 Palantir shall ensure, at all times during the Term, that Palantir and any Subcontractor with access to Crown Information or who will Process Crown Information are certified as compliant with:

7.1.1 Cyber Essentials PLUS,

and shall provide the Cabinet Office with a copy of each such certificate of compliance before Palantir or the relevant Sub-contractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Crown Information. Any exceptions to the flow-down of the certification requirements to third party contractors and sub-contractors must be agreed with the Cabinet Office; and

7.1.2 CSA Star or SOC2:2

Except the requirement to comply with 7.1.2 shall not apply to any UK Subcontractor which is not a cloud provider.

7.2 Palantir shall ensure, at all times and to the extent applicable during the Term, that Palantir and each Sub-contractor who is responsible for the secure destruction of Crown Information:

7.2.1 securely destroys Crown Information only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013.; and

are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Cabinet Office. Palantir shall provide the Cabinet Office with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before Palantir or the

relevant Sub-contractor (as applicable) shall be permitted to carry out the secure destruction of the Crown Information.

7.3 Palantir shall notify the Cabinet Office as soon as reasonably practicable and, in any event within 2 Working Days, if Palantir or any Sub-contractor ceases to be compliant with the Certification Requirements and, on request from the Cabinet Office, shall or shall procure that the relevant Sub-contractor shall:

7.3.1 immediately ceases using the Crown Information; and

7.3.2 procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Crown Information in accordance with Baseline Security Requirements.

8. Security Testing

8.1 Palantir shall, at its own cost and expense:

8.1.1 as soon as reasonably practicable and in any event no later than 3 months after the date of the Accreditation Decision, procure a CHECK IT Health Check of the Core Information Management System (an "**IT Health Check**") by a NCSC approved member of the CHECK Scheme:

(a) if directed to do so by the Cabinet Office in accordance with Paragraph 8.4.

8.1.2 conduct an assessment as soon as reasonably practicable following receipt by Palantir or any of its Sub-contractors of a critical vulnerability alert from a Palantir of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and

8.1.3 conduct such other tests as are required by:

(a) any Vulnerability Correction Plans;

(b) the Risk Management Documentation; and

(c) the Cabinet Office following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

(each a "**Security Test**").

8.2 Palantir shall provide the Cabinet Office with the results of such Security Tests (in a form approved by the Cabinet Office in advance) as soon as practicable after completion of each Security Test.

8.3 Palantir shall conduct vulnerability scanning and assessments of the Core Information Management System.

8.4 In relation to each IT Health Check, Palantir shall:

8.4.1 agree with the Cabinet Office the aim and scope of the IT Health Check;

8.4.2 promptly, following receipt of each IT Health Check report, provide the Cabinet Office with a copy of the IT Health Check report;

8.4.3 in the event that the IT Health Check report identifies any vulnerabilities, Palantir shall:

(a) prepare a remedial plan for approval by the Cabinet Office (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

(i) how the vulnerability will be remedied;

(ii) the date by which the vulnerability will be remedied;

(iii) the tests which Palantir shall perform or procure to be performed (which may, at the discretion of the Cabinet Office, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(b) comply with the Vulnerability Correction Plan; and

(c) conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

8.5 The Security Tests shall be designed and implemented by Palantir so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Cabinet Office.

8.6 The Cabinet Office shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to Palantir's obligations under Paragraph 8.3, Palantir shall provide the Cabinet Office with the results of such Security Tests (in a form approved by the Cabinet Office in advance) as soon as practicable after completion of each Security Test.

8.7 The Cabinet Office and/or its authorised representatives shall be entitled, on reasonable written notice to Palantir and subject to Palantir's written consent, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information System and/or Palantir's compliance with the Risk Management Documentation ("**Cabinet Office Security Tests**"). The Cabinet Office shall take reasonable steps to notify Palantir prior to carrying out such Cabinet Office Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature of the Cabinet Office Security Test.

8.8 The Cabinet Office shall notify Palantir of the results of such Cabinet Office Security Tests after completion of each Cabinet Office Security Test.

8.9 The Cabinet Office Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services

8.10 Without prejudice to the provisions of Paragraph 8.4.3, where any Security Test carried out pursuant to this Paragraph 8 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), Palantir shall promptly notify the Cabinet Office of any changes to the Core Information Management System and/or the Risk Management Documentation (and the implementation thereof) which Palantir proposes to make in order to correct such failure or weakness. Subject to the Cabinet Office's prior written approval, Palantir shall implement such changes to the Core Information Management System and/or the Risk Management Documentation and repeat the relevant Security Tests in accordance with the timetable agreed with the Cabinet Office or, otherwise, as soon as reasonably possible.

8.11 If the Cabinet Office unreasonably withholds its approval to the implementation of any changes proposed by Palantir to the Risk Management Documentation in accordance with Paragraph 8.11 above, Palantir shall not be deemed to be in breach of this Call-Off Contract to the extent it can be shown that such breach:

8.11.1 has arisen as a direct result of the Cabinet Office unreasonably withholding its approval to the implementation of such proposed changes; and

8.11.2 would have been avoided had the Cabinet Office given its approval to the implementation of such proposed changes.

8.12 For the avoidance of doubt, where a change to the Core Information Management System and/or the Risk Management Documentation is required to remedy non-compliance with the Risk Management Documentation,

the Baseline Security Requirements and/or any obligation in this Call-Off Contract, Palantir shall effect such change at its own cost and expense.

8.13 If any repeat Security Test carried out pursuant to Paragraph 8.10 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Cabinet Office may by terminate this Call-Off Contract with immediate effect on written notice to Palantir.

8.13.1 Palantir shall ensure that its supply chain (including sub-contractors) adheres to the standards set out in NCSC Cloud Security Principle 8.

9. Vulnerabilities and Corrective Action

9.1 The Cabinet Office and Palantir acknowledge that from time to time vulnerabilities in the Information System will be discovered which unless mitigated will present an unacceptable risk to the Crown Information.

9.2 The severity of vulnerabilities for Palantir COTS Software and Third Party COTS Software shall be categorised by Palantir as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Risk Management Documentation 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 at 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 Subject to Paragraph 9.4, Palantir shall procure the application of security patches to vulnerabilities in the Core Information Management System within:

9.3.1 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

9.3.2 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

9.3.3 60 days after the public release of patches for those vulnerabilities categorised as 'Other'.

9.4 The timescales for applying patches to vulnerabilities in the Core Information Management System set out in Paragraph 9.3 shall be extended where:

9.4.1 Palantir can demonstrate that a vulnerability in the Core Information Management System is not exploitable within the context of the Border Flow Service (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by Palantir within the timescales set out in Paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;

9.4.2 the application of a 'Critical' or 'Important' security patch adversely affects Palantir's ability to deliver the Border Flow Service in which case Palantir shall be granted an extension to such timescales of 5 days, provided Palantir had followed and continues to follow the security patch test plan agreed with the Cabinet Office; or

9.4.3 the Cabinet Office agrees a different maximum period after a case-by-case consultation with Palantir under the processes defined in the Risk Management Documentation.

9.5 The Risk Management Documentation shall include provisions for major version upgrades of all Palantir COTS Software and Third Party COTS Software to be kept up to date such that all Palantir COTS Software and Third Party COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Cabinet Office in writing.

9.6 Palantir shall, on receipt of reasonable written notice:

9.6.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;

9.6.2 promptly notify NCSC of any actual or sustained attempted Breach of Security;

9.6.3 ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.6.4 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Term;

9.6.5 pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Risk Management Documentation;

9.6.6 from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent month during the Term, where requested provide the Cabinet Office with a written report which details both patched and outstanding critical vulnerabilities in the Core Information Management System, the 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 and any failure to comply with the timescales set out in Paragraph 9.3 for applying patches to vulnerabilities in the Core Information Management System;

9.6.7 propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;

9.6.8 and

9.6.9 inform the Cabinet Office when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.

9.7 If Palantir is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 10, Palantir shall immediately notify the Cabinet Office.

9.8 If Palantir fails to patch vulnerabilities in the Core Information Management System in accordance with Paragraph 9.3, such failure shall constitute a material Default and the Cabinet Office may terminate this Call-Off Contract with immediate effect on written notice to Palantir.

10. Malicious Software

10.1 Palantir shall install and maintain anti-Malicious Software or procure that anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Crown Information and ensure that such anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

10.2 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Crown Information, assist each other to mitigate any Losses and to restore the Border Flow Service to their desired operating efficiency.

10.3 any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 10.2 shall be borne by the Parties as follows:

10.3.1 by Palantir where the Malicious Software originates from Palantir Software, the Third Party Software supplied by Palantir or the Crown Information (whilst the Crown Information was under the control of Palantir) unless Palantir can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Cabinet Office when provided to Palantir; and

10.3.2 otherwise by the Cabinet Office.

11. Breach of Security

11.1 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Risk Management Documentation.

11.2 The security incident management process set out in the Risk Management Documentation shall, as a minimum, require Palantir upon becoming aware of a Breach of Security or an attempted Breach of Security to:

11.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Cabinet Office which shall be completed within such timescales as the Cabinet Office may reasonably require) necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Information System against any such potential or attempted Breach of Security;

(c) apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by Palantir, if the mitigation adversely affects Palantir's ability to deliver the Border Flow Service so as to meet any Performance Indicator, Palantir shall be granted relief against the failure to meet such affected Performance Indicator for such period as the Cabinet Office, acting reasonably, may specify by written notice to Palantir; and

(d) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;

11.2.2 as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Cabinet Office full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Cabinet Office.

11.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the Information System and/or the Risk Management Documentation with the Baseline Security Requirements and/or this Call-Off Contract, then such action and any required change to the Information System and/or Risk Management Documentation shall be completed by Palantir at no cost to the Cabinet Office.

11.4 If Palantir fails to comply with its obligations set out in this Paragraph 11, such failure shall constitute a material Default, which if not remedied to the satisfaction of the Cabinet Office, shall permit the Cabinet Office to terminate this Call-Off Contract with immediate effect on written notice to Palantir.

12. Data Processing, Storage, Management and Destruction

12.1 In addition to the obligations on Palantir in respect of Processing Personal Data and compliance with the DPA, Palantir shall:

12.1.1 save as otherwise provided in Schedule 7 ensure that the Buyer Data is hosted only in the UK only at the Sites and such Sites must not be located in a Restricted Country except where the Cabinet Office has given its consent to a transfer of the Crown Information to such Restricted Country;

12.1.2 on demand, provide the Cabinet Office with all Crown Information in an agreed open format;

12.1.3 have documented processes to guarantee availability of Crown Information in the event of Palantir ceasing to trade;

12.1.4 securely erase any or all Crown Information held by Palantir when requested to do so by the Cabinet Office; and

12.1.5 securely destroy all media that has held Crown Information at the end of life of that media in accordance with any specific requirements in this Call-Off Contract and, in the absence of any such requirements, as directed by the Cabinet Office.

Annex 1: Baseline Security Requirements

1. Security Classification of Information

If the provision of the Border Flow Service requires Palantir to Process Crown Information which is classified as:

12.2 OFFICIAL-SENSITIVE, Palantir shall implement such additional measures as agreed with the Cabinet Office from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or

12.3 SECRET or TOP SECRET, Palantir shall only do so where it has notified the Cabinet Office prior to receipt of such Crown Information and Palantir shall implement additional measures as agreed with the Cabinet Office from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2. End User Devices

12.4 Palantir shall ensure that any Crown Information which resides on a mobile, removable or physically uncontrolled device is stored Encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Cabinet Office except where the Cabinet Office has given its prior written consent to an alternative arrangement.

12.5 Palantir shall ensure that any device which is used to Process Crown Information meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

3. Networking

Palantir shall ensure that any Crown Information which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be Encrypted when transmitted.

4. Personnel Security

12.6 All Palantir's employees, agents or subcontractors working on the Border Flow Service (the **Palantir Personnel**) shall be subject to a pre-employment check before they may participate in the provision and or management of the Border Flow Service. Such pre-employment checks must include all pre-employment checks which are required by the CROWN Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

12.7 The Cabinet Office and Palantir shall review the roles and responsibilities of Palantir Personnel who will be involved in the management and/or provision of the Border Flow Service in order to enable the Cabinet Office to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Crown Information or data which is classified as OFFICIAL-SENSITIVE.

12.8 Palantir shall not permit Palantir Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Border Flow Service except where the Cabinet Office has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Border Flow Service.

12.9 Palantir shall ensure that Palantir Personnel are only granted such access to Crown Information as is necessary to enable Palantir Personnel to perform their role and to fulfil their responsibilities.

12.10 Palantir shall ensure that Palantir Personnel who no longer require access to the Crown Information (e.g. they cease to be employed by Palantir or any of its Sub-contractors), have their rights to access the Crown Information revoked within 1 Working Day.

5. Identity, Authentication and Access Control

12.11 Palantir shall operate an access control regime to ensure:

12.11.1 all users and administrators of the Palantir System are uniquely identified and authenticated when accessing or administering the Services; and

12.11.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

12.12 Palantir shall apply the 'principle of least privilege' when allowing persons access to Palantir System and Sites so that such persons are allowed access only to those parts of the Sites and Palantir System they require.

12.13 Palantir shall retain records of access to the Sites and to Palantir System and shall make such record available to the Cabinet Office on request.

6. Audit and Protective Monitoring

12.14 Palantir shall collect audit records which relate to security events in the Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Palantir audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Crown Information.

12.15 Palantir and the Cabinet Office shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

12.16 The retention periods for audit records and event logs must be agreed with the Cabinet Office and documented in the Risk Management Documentation.

13. **Secure Architecture**

1.1 Palantir shall design the Core Information Management System in accordance with:

1.1.1 the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(a) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(c) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(d) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that Palantir should have a security governance framework which coordinates and directs its management of the Border Flow Service and information within it;

(e) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Border Flow Service need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Palantir Personnel have access to Crown Information and/or the Cabinet Office System that those personnel be subject to appropriate security screening and regular security training;

(g) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Border Flow Service be designed and developed to identify and mitigate threats to their security;

(h) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires Palantir to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;

(i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires Palantir to make the tools available for the Cabinet Office to securely manage the Cabinet Office's use of the Border Flow Service;

(j) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires Palantir to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(k) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Border Flow Service should be identified and appropriately defended;

(l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires Palantir to be able to provide the Cabinet Office with the audit records it needs to monitor access to the Border Flow Service and the Crown Information held by Palantir and/or its Sub-contractors;

(n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires Palantir to educate Palantir Personnel on the safe and secure use of the Information Management System.

Schedule 10 – Service Continuity Plan

PART 1: SERVICE CONTINUITY PLAN

11 DEFINITIONS

1.1 In this Schedule, in addition to those other definitions in the Agreement, the following definitions shall apply:

Authority	means the Cabinet Office as defined in the Agreement
"Business Continuity Plan"	has the meaning given in Paragraph 2.2(a)(ii);
"Business Continuity Services"	has the meaning given in Paragraph 4.2(b);
"Department"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: *(a)* Government Department; or *(b)* Non-Ministerial Department.
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part of the Services will be unavailable or which is reasonably anticipated will mean that the Services or a material part of the Services will be unavailable for that period;
"Disaster Recovery Plan"	has the meaning given in Paragraph 2.2(a)(iii);
"Disaster Recovery Services"	the services embodied in the processes and procedures for restoring the Services following the occurrence of a Disaster;
"Disaster Recovery System"	the system identified by Palantir in the Border Flow Service which shall be used for the purpose of delivering the Disaster Recovery Services;
"Insolvency Continuity Plan"	has the meaning given in Paragraph 2.2(a)(iv).
"Related Service Provider"	any person who provides services to the Buyer in relation to this Call-Off Contract from time to time
"Review Report"	has the meaning given in Paragraphs 7.2(a) to 7.2(c);
"Service Continuity Plan"	means the plan prepared pursuant to Paragraph 2 of this Schedule which incorporates the Business Continuity Plan, Disaster Recovery Plan and the Insolvency Continuity Plan;

1.2 On receipt of reasonable written notice following the start of the Term, Palantir shall prepare and deliver to the Buyer for the Buyer's written approval a plan, which shall detail the processes and arrangements that Palantir shall follow to:

(a) ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services (including where caused by a Supplier Insolvency Event of Palantir, any Key Sub-contractor and/or any Supplier Group member); and

(b) the recovery of the Services in the event of a Disaster.

1.3 The Service Continuity Plan shall:

(a) be divided into four parts:

(i) Part A which shall set out general principles applicable to the Service Continuity Plan;

(ii) Part B which shall relate to business continuity (the "Business Continuity Plan");

(iii) Part C which shall relate to disaster recovery (the "Disaster Recovery Plan");

(iv) Part D which shall relate to a Supplier Insolvency Event of Palantir, any Key Sub-contractors and/or any Supplier Group member (the "Insolvency Continuity Plan"); and

(b) unless otherwise required by the Buyer in writing, be based upon and be consistent with the provisions of Paragraphs 2, 3, 4 and 5.

1.4 Following receipt of the draft Service Continuity Plan from Palantir, the Buyer shall:

(a) review and comment on the draft Service Continuity Plan as soon as reasonably practicable; and

(b) notify Palantir in writing that it approves or rejects the draft Service Continuity Plan no later than 20 Working Days after the date on which the draft Service Continuity Plan is first delivered to the Buyer.

1.5 If the Buyer rejects the draft Service Continuity Plan:

(a) the Buyer shall inform Palantir in writing of its reasons for its rejection; and

(b) Palantir shall then revise the draft Service Continuity Plan (taking reasonable account of the Buyer's comments) and shall re-submit a revised draft Service Continuity Plan to the Buyer for the Buyer's approval within 20 Working Days of the date of the Buyer's notice of rejection. The provisions of Paragraph 1.4 and this Paragraph 1.5 shall apply again to any resubmitted draft Service Continuity Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

12 SERVICE CONTINUITY PLAN: PART A – GENERAL PRINCIPLES AND REQUIREMENTS

2.1 Part A of the Service Continuity Plan shall:

(a) set out how the business continuity, disaster recovery and insolvency continuity elements of the plan link to each other;

(b) provide details of how the invocation of any element of the Service Continuity Plan may impact upon the operation of the Services and any services provided to the Buyer by a Related Service Provider;

(c) contain an obligation upon Palantir to liaise with the Buyer and (at the Buyer's request) any Related Service Provider with respect to issues concerning business continuity, disaster recovery and insolvency continuity where applicable;

(d) detail how the Service Continuity Plan links and interoperates with any overarching and/or connected disaster recovery, business continuity and/or insolvency continuity plan of the Buyer and any of its other Related Service Providers in each case as notified to Palantir by the Buyer from time to time;

(e) contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels (including but without limitation a web-site (with FAQs), e-mail, phone and fax) for both portable and desk top configurations, where required by the Buyer;

(f) contain a risk analysis, including:

(i) failure or disruption scenarios and assessments and estimates of frequency of occurrence;

(ii) identification of any single points of failure within the Services and processes for managing the risks arising therefrom;

(iii) identification of risks arising from the interaction of the Services with the services provided by a Related Service Provider;

(iv) identification of risks arising from a Supplier Insolvency Event of Palantir, any Key Sub-contractors and/or Supplier Group member; and

(v) a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;

(g) provide for documentation of processes, including business processes, and procedures;

(h) set out key contact details (including roles and responsibilities) for Palantir (and any Sub-contractors) and for the Buyer;

(i) identify the procedures for reverting to "normal service";

(j) set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to ensure that there is no more than the accepted amount of data loss and to preserve data integrity;

(k) identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the Service Continuity Plan; and

(l) provide for the provision of technical advice and assistance to key contacts at the Buyer as notified by the Buyer from time to time to inform decisions in support of the Buyer's business continuity plans.

2.2 The Service Continuity Plan shall be designed so as to ensure that:

(a) the Services are provided in accordance with this Call-Off Contract at all times during and after the invocation of the Service Continuity Plan;

(b) the adverse impact of any Disaster; service failure; a Supplier Insolvency Event of Palantir, any Key Sub-contractor and/or any Supplier Group member; or disruption on the operations of the Buyer, is minimal as far as reasonably possible;

(c) it complies with the relevant industry standards from time to time in force; and

(d) there is a process for the management of disaster recovery testing detailed in the Service Continuity Plan.

2.3 The Service Continuity Plan shall be upgradeable and sufficiently flexible to support any changes to the Services, to the business processes facilitated by and the business operations supported by the Services, and/or changes to Palantir Group structure.

2.4 Palantir shall not be entitled to any relief from its obligations under the Performance Indicators or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by Palantir of this Call-Off Contract.

13 SERVICE CONTINUITY PLAN: PART B - BUSINESS CONTINUITY

PRINCIPLES AND CONTENTS

3.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the Services remain supported and to ensure continuity of the business operations supported by the Services including, unless the Buyer expressly states otherwise in writing:

(a) the alternative processes (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the Services; and

(b) the steps to be taken by Palantir upon resumption of the Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

3.2 The Business Continuity Plan shall:

(a) address the various possible levels of failures of or disruptions to the Services;

(b) set out the services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services (such services and steps, the “Business Continuity Services”);

(c) specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Business Continuity Plan; and

(d) clearly set out the conditions and/or circumstances under which the Business Continuity Plan is invoked.

14 SERVICE CONTINUITY PLAN: PART C – DISASTER RECOVERY

PRINCIPLES AND CONTENTS

4.1 The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster Palantir ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

4.2 The Disaster Recovery Plan shall be invoked only upon the occurrence of a Disaster.

4.3 The Disaster Recovery Plan shall include the following:

(a) the technical design and build specification of the Disaster Recovery System;

(b) details of the procedures and processes to be put in place by Palantir in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including but not limited to the following:

(i) data centre and disaster recovery site audits;

(ii) backup methodology and details of Palantir's approach to data back-up and data verification;

(iii) identification of all potential disaster scenarios;

(iv) risk analysis;

(v) documentation of processes and procedures;

(vi) hardware configuration details;

(vii) network planning including details of all relevant data networks and communication links;

(viii) invocation rules;

(ix) Service recovery procedures; and

(x) steps to be taken upon resumption of the Services to address any prevailing effect of the failure or disruption of the Services;

(c) any applicable Performance Indicators with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Disaster Recovery Plan;

(d) details of how Palantir shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

(e) ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

(f) access controls to any disaster recovery sites used by Palantir in relation to its obligations pursuant to this Schedule; and

(g) testing and management arrangements.

15 SERVICE CONTINUITY PLAN: PART D – INSOLVENCY CONTINUITY PLAN PRINCIPLES AND CONTENTS

5.1 The Insolvency Continuity Plan shall be designed by Palantir to permit continuity of the business operations of the Buyer supported by the Services through continued provision of the Services following a Supplier Insolvency Event of Palantir, any Key Sub-contractor and/or any Supplier Group member with, as far as reasonably possible, minimal adverse impact.

5.2 The Insolvency Continuity Plan shall include the following:

(a) communication strategies which are designed to minimise the potential disruption to the provision of the Services, including key contact details in respect of the supply chain and key contact details for operational and contract Supplier Personnel, Key Sub-contractor personnel and Supplier Group member personnel;

(b) identification, explanation, assessment and an impact analysis of risks in respect of dependencies between Palantir, Key Sub-contractors and Supplier Group members where failure of those dependencies could reasonably have an adverse impact on the Services;

(c) plans to manage and mitigate identified risks;

(d) details of the roles and responsibilities of Palantir, Key Sub-contractors and/or Supplier Group members to minimise and mitigate the effects of a Supplier Insolvency Event of such persons on the Services;

(e) details of the recovery team to be put in place by Palantir (which may include representatives of Palantir, Key Sub-contractors and Supplier Group members); and

(f) sufficient detail to enable an appointed insolvency practitioner to invoke the plan in the event of a Supplier Insolvency Event of Palantir.

16 REVIEW AND AMENDMENT OF THE SERVICE CONTINUITY PLAN

6.1 Palantir shall review and update the Service Continuity Plan (and the risk analysis on which it is based):

(a) on a regular basis and as a minimum once every 6 months;

(b) within three calendar months of the Service Continuity Plan (or any part) having been invoked pursuant to Paragraph 8;

(c) within 14 days of a Financial Distress Event;

(d) within 30 days of a Corporate Change Event; and

(e) where the Buyer requests any additional reviews (over and above those provided for in Paragraphs 7.1(a) to 7.1(c)) by notifying Palantir to such effect in writing, whereupon Palantir shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, Palantir shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that Palantir shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

6.2 Each review of the Service Continuity Plan pursuant to Paragraph 6.1 shall be a review of the procedures and methodologies set out in the Service Continuity Plan and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the Service Continuity Plan or the last review of the Service Continuity Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the Service Continuity Plan. The review shall be completed by Palantir within the period required by the Service Continuity Plan or, if no such period is required, within such period as the Buyer shall reasonably require. Palantir shall, within 20 Working Days of the conclusion of each such review of the Service Continuity Plan, provide to the Buyer a report (a "Review Report") setting out:

(a) the findings of the review;

(b) any changes in the risk profile associated with the Services; and

(c) Palantir's proposals (the "Supplier's Proposals") for addressing any changes in the risk profile and its proposals for amendments to the Service Continuity Plan following the review detailing the impact (if any and to the extent that Palantir can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any services or systems provided by a third party.

6.3 Following receipt of the Review Report and Palantir's Proposals, the Buyer shall:

(a) review and comment on the Review Report and Palantir's Proposals as soon as reasonably practicable; and

(b) notify Palantir in writing that it approves or rejects the Review Report and Palantir's Proposals no later than 20 Working Days after the date on which they are first delivered to the Buyer.

6.4 If the Buyer rejects the Review Report and/or Palantir's Proposals:

(a) the Buyer shall inform Palantir in writing of its reasons for its rejection; and

(b) Palantir shall then revise the Review Report and/or Palantir's Proposals as the case may be (taking reasonable account of the Buyer's comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised Review Report and/or revised Supplier's Proposals to the Buyer for the Buyer's approval within 20 Working Days of the date of the Buyer's notice of rejection. The provisions of Paragraph 6.3 and this Paragraph 6.4 shall apply again to any resubmitted Review Report and Supplier's Proposals, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

6.5 Palantir shall as soon as is reasonably practicable after receiving the Buyer's approval of Palantir's Proposals (having regard to the significance of any risks highlighted in the Review Report) effect any change in its practices or procedures necessary so as to give effect to Palantir's Proposals. Any such change shall be at Palantir's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

17 TESTING OF THE SERVICE CONTINUITY PLAN

7.1 Palantir shall test the Service Continuity Plan on a regular basis (and in any event not less than once in every Contract Year). Subject to Paragraph 7.2, the Buyer may require Palantir to conduct additional tests of some or all aspects of the Service Continuity Plan at any time where the Buyer considers it necessary, including where there has been any change to the Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the Service Continuity Plan.

7.2 If the Buyer requires an additional test of the Service Continuity Plan, it shall give Palantir written notice and Palantir shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the Service Continuity Plan. Palantir's costs of the additional test shall be borne by the Buyer unless the Service Continuity Plan fails the additional test in which case Palantir's costs of that failed test shall be borne by Palantir.

7.3 Palantir shall undertake and manage testing of the Service Continuity Plan in full consultation with the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer in this regard. Each test shall be carried out under the supervision of the Buyer or its nominee.

7.4 Palantir shall ensure that any use by it or any Sub-contractor of “live” data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

7.5 Palantir shall, within 20 Working Days of the conclusion of each test, provide to the Buyer a report setting out:

(a) the outcome of the test;

(b) any failures in the Service Continuity Plan (including the Service Continuity Plan's procedures) revealed by the test; and

(c) Palantir's proposals for remedying any such failures.

7.6 Following each test, Palantir shall take all reasonable measures requested by the Buyer, (including requests for the re-testing of the Service Continuity Plan) to remedy any failures in the Service Continuity Plan and such remedial activity and re-testing shall be completed by Palantir, at no additional cost to the Buyer, by the date reasonably required by the Buyer and set out in such notice.

7.7 For the avoidance of doubt, the carrying out of a test of the Service Continuity Plan (including a test of the Service Continuity Plan’s procedures) shall not relieve Palantir of any of its obligations under this Call-Off Contract.

7.8 Palantir shall also perform a test of the Service Continuity Plan in the event of any major reconfiguration of the Services or as otherwise reasonably requested in writing by the Buyer.

18 INVOCATION OF THE SERVICE CONTINUITY PLAN

8.1 In the event of a loss of any critical part of the Service or a Disaster, Palantir shall immediately invoke the business continuity and disaster recovery provisions in the Service Continuity Plan, including any linked elements in other parts of the Service Continuity Plan, and shall inform the Buyer promptly of such invocation. In all other instances Palantir shall invoke the business continuity and disaster recovery plan elements only with the prior consent of the Buyer.

8.2 The Insolvency Continuity Plan element of the Service Continuity Plans, including any linked elements in other parts of the Service Continuity Plan, shall be invoked by Palantir:

(a) where an Insolvency Event of a Key Sub-contractor and/or Supplier Group member (other than Palantir) could reasonably be expected to adversely affect delivery of the Services; and/or

(b) where there is a Supplier Insolvency Event of Palantir and the insolvency arrangements enable Palantir to invoke the plan.