DPS FRAMEWORK SCHEDULE 4: LETTER OF APPOINTMENT AND CONTRACT TERMS

Part 1: Letter of Appointment

Frazer – Nash Consultancy Ltd

REDACTED

5th Floor,

Malt Building,

Wilderspool Business Park,

Greenalls avenue,

Warrington,

Cheshire,

WA64 6HL

Dear Andy,

Letter of Appointment: Contract Reference CCZZ20A07

Letter of Appointment – Provision of GSG Security Assurance Dip-Sampling

This letter of Appointment dated 03/06/2020, is issued in accordance with the provisions of the DPS Agreement (RM6018) between CCS and the Supplier.

Capitalised terms and expressions used in this letter have the same meanings as in the Contract Terms unless the context otherwise requires.

Order Number:	To be provided post Award
From:	Cabinet Office: Analysis & Reporting Team, Government Security Group, Cabinet Office 70 Whitehall London SW1A 2AS
To:	Frazer – Nash Consultancy Ltd Registered Number 02562870 Registered address - Devonport Royal Dockyard, Devonport, Plymouth, PL1 4SG

Effective Date:	The contract will commence after Award of Contract on the 11th June 2020

Expiry Date:	End date of Initial period is 31st of July 2020 (37 working days not including weekends) There is no option to extend Bearing in mind the impact of Covid-19 on government organisations, should any of the participating organisations not be available to engage with FNC on a given day or require additional time, we are happy for the 37 days engagement to take place over a period of reasonable time as opposed to 37 consecutive days.

Services required:	Set out in Section 2, Part B (Specification) of the DPS Agreement and refined by: · the Customer's Project Specification attached at Annex A and the Supplier's Proposal attached at Annex B;

Key Individuals:	(Supplier) REDACTED (Customer) REDASCTED
[Guarantor(s)]	Not Applicable

Contract Charges (including any applicable discount(s), but excluding VAT):	Annex 1 - Contract Charges - Contract Terms. 1. For the avoidance of doubt, the total contract value shall not exceed £78,350.00 (excluding VAT) and will be paid on completion of the following deliverables as detailed in the table within Annex 1. 2. The Provider shall add VAT to the Contract Price at the prevailing rate as applicable and the Customer shall pay the VAT to the Provider following its receipt of a valid VAT invoice. 3. Invoices to be submitted in line with milestone payments to be agreed with the Customer. 4. Before payment can be considered, each

	invoice must include a detailed elemental breakdown of work completed and the associated costs.
Insurance Requirements	(Clause 19.1 of the Contract Terms):
Liability Requirements	Suppliers limitation of Liability (Clause of the Contract Terms);
Customer billing address for invoicing:	**REDACTED**

GDPR	Contract Terms Schedule 7 (Processing, Personal Data and Data Subjects
Alternative and/or additional provisions (including Schedule 8(Additional clauses)):	Not Applicable

FORMATION OF CONTRACT

BY SIGNING AND RETURNING THIS LETTER OF APPOINTMENT (which may be done by electronic means) the Supplier agrees to enter a Contract with the Customer to provide the Services in accordance with the terms of this letter and the Contract Terms.

The Parties hereby acknowledge and agree that they have read this letter and the Contract Terms.

The Parties hereby acknowledge and agree that this Contract shall be formed when the Customer acknowledges (which may be done by electronic means) the receipt of the signed copy of this letter from the Supplier within two (2) Working Days from such receipt

For and on behalf of the Supplier:	**For and on behalf of the Customer:**
Name and Title: **REDACTED**	Name and Title: **REDACTED**
Signature:	Signature:
Date:	Date:

ANNEX A

Customer Project Specification

1. PURPOSE

1.1 The Assurance team in the Government Security Group uses various pieces of data to assess and analyse the effectiveness of security controls across Government.

1.2 **REDACTED**

1.3 **REDACTED**

1.4 **REDACTED**

1.5 REDACTED

1.6 This higher level of validation will enable our reporting to be more accurate, and, in turn, will help Security Professionals across government to direct their resources more efficiently.

1.7 The objective of the exercise described herein is to arrive at better-informed conclusions by strategically examining a small set of controls in a small number of principal departments and Arm's Length Bodies.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The Government Security Group is part of the Cabinet Office, and the function responsible for policy, delivery and assurance of government security.

2.2 The Assurance team is responsible for examining the extent to which we are able to have confidence in the security of the government. This comprises three sub-teams:

2.2.1 The Red Team: Responsible for conducting testing exercises across government, and particularly GBEST penetration testing.

2.2.2 The Health Check Team: Responsible for coordinating the security self-assessment process completed by circa 78 government organisations and bodies.

2.2.3 The Analysis and Reporting Team: Responsible for gathering data across government in order to arise at evidence-based conclusions through effective analysis and reporting. It will be within this team that the dip-sampling exercise will be coordinated.

3. BACKGROUND TO REQUIREMENT / OVERVIEW OF REQUIREMENT

3.1 Government organisations are responsible for managing their own security, and have their own arrangements to provide assurance of security controls, through day-to-day operational and management activities (first line of defence). The Assurance team look across the whole of Government, providing independent assurance from the functional centre in a second line of defence, with internal audit acting as a third line

of defence, with further checks as required from bodies such as the National Audit Office (NAO) and the Infrastructure and Projects Authority (IPA).

3.2 The scope of the dip-testing exercise will be the UK Government departments and bodies (and not Devolved Administrations or the wider public sector/ Local Authorities).

3.3 The project will form part of our proportionate steps to obtain reasonable assurance that HMG is secure, understanding that it is never possible to provide complete assurance on any particular aspect of security; and connect our analysis on vulnerabilities with analysis on the threat and potential impacts, to support wider assessments of risk.

3.4 The setup for this project can be easily scalable. If the project is successful, further dip sampling can take place to test other organisations and other controls.

3.5 Organisations will be supported to improve their own security by sharing analysis and recommendations.

4. DEFINITIONS

Expression or Acronym	Definition
ALB	Arms-Length Body (ancillary division of a government department
GBEST	Government penetration testing regime, conducted
DCMS	Department for Digital, Culture, Media &
SFO	Serious Fraud Office
NS&I	National Savings and Investments
HSE	Health and Safety Executive
HMT	Her Majesty's Treasury

5. SCOPE OF REQUIREMENT

5.1 The organisations within scope have been chosen based on the evidence base already at the hands of the Assurance Team. The Health Check data, as well as GBEST, Technical Deep Dive Reports and other ancillary pieces of data point to areas of government for which we have a weaker understanding or confidence in departmental security.

5.2 In view of the confidence measure used, the Assurance team has chosen the following six organisations. These organisations have been selected to ensure variation, based on the following factors:

5.2.1 Size of organisation in terms of staff and budget (selecting a span of relatively small, medium and large organisations)
5.2.2 Nature of work (selecting organisations who perform different kinds of work with variety in the nature of their objectives).

5.3 In light of the above the following organisations have been chosen:

5.3.1 **REDACTED**
5.3.2 **REDACTED**

5.3.3 **REDACTED**
5.3.4 **REDACTED**
5.3.5 **REDACTED**
5.3.6 **REDACTED**

5.4 The exercise will test four controls across the organisations listed in 5.2. These controls have been chosen based on the quantity and quality of data currently held on these controls, as well as the maturity of the conclusions that can be made from this data.

5.5 The Assurance team have chosen the following controls to be measured across these government organisations:

5.5.1 **REDACTED**
5.5.2 **REDACTED**
5.5.3 **REDACTED**
5.5.4 **REDACTED**

5.6 These controls correspond to the Minimum Security Standards, which are developed by the function, and set with assistance from security professionals across governments.

5.7 The contracted party will conduct comprehensive discovery and reporting across these six organisations, indicating the following:

5.7.1 Adherence to the standard (consistency and the scale)
5.7.2 Whether the current conclusions are correct
5.7.3 Counter-measurements in place by the department
5.7.4 Barriers within the department which prevent adherence
5.7.5 Vulnerabilities within the department related to the control, but not specifically noted by the standard or control.

5.8 Evidence to support the discovery and reporting will be obtained from the organisations, and will consist of a range of qualitative and quantitative data. Examples are given below:

5.8.1 Physical:
5.8.1.1 REDACTED
5.8.1.2 REDACTED
5.8.1.3 REDACTED
5.8.1.4 REDACTED
5.8.1.5 REDACTED

5.8.2 Personnel:
5.8.2.1 REDACTED
5.8.2.2 REDACTED
5.8.2.3 REDACTED
5.8.2.4 REDACTED
5.8.2.5 REDACTED
5.8.2.6 REDACTED
5.8.2.7 REDACTED
5.8.2.8 REDACTED

5.8.3 Cyber:

5.8.3.1 REDACTED
5.8.3.2 REDACTED
5.8.3.3 REDACTED
5.8.3.4 REDACTED

5.8.4 Incident Management:

5.8.4.1 REDACTED
5.8.4.2 REDACTED
5.8.4.3 REDACTED
5.8.4.4 REDACTED

6. THE REQUIREMENT

6.1 Independent external contractors with 'SC' clearance or above with appropriate skills and experience in security and moderation will be contracted to complete the exercise.

6.2 Contractors are required to be skilled with discovery, research and audit in order to arrive at appropriate conclusions regarding the compliance to controls in each of the selected organisations.

6.3 37 working days engagement between 31st March 2020 and 21st May 2020

6.4 The reports (6 departmental, 1 cross-government project summary) will provide a comprehensive account of findings against each of the four controls stated at point 5.5.

6.5 The reports should provide a clear indication of the Departments standing in relation to adherence to the standard (consistency and the scale), whether the current conclusions are correct, counter-measurements in place by the department, barriers within the department which prevent adherence, vulnerabilities within the department related to the control, but not specifically noted by the standard or control.

6.6 All source data should be annexed and conclusions are to be referenced.

6.7 All core data generated throughout this engagement should (where appropriate) be annexed and referenced; and should be provided separately to the Assurance and Reporting Team/ Government Security Group.

6.8 All reports should be marked as OFFICIAL-SENSITIVE and treated with the appropriate degree of care and protection.

6.9 The reports will be initially supplied to The Cabinet Office at Official Sensitive, but may be disseminated further to the host organisations.

6.10 All seven reports are to be delivered in an electronic format to the contacts listed in section (8). The reports should be in either a .pdf, or Word **Document (.DOCX)** format.

6.11 The reports should detail the relevant methodologies that were used during the discovery phase. The reports should explain how any comparisons made between existing data and any new data generated through this engagement points to a

departments posture against each of the controls listed at (5.5), and how these relate to the five indicators listed at (5.7).

7. KEY MILESTONES AND DELIVERABLES

7.1 The following Contract milestones/deliverables shall apply:
7.2 Cross-Government summary report provided to CO.

Milestone/Deliverable	Description	Timeframe or Delivery Date
1	Initial inception meeting with Client and Supplier	Within week 1 of Contract Award
2	Start of Dip Sampling discovery/ data collection phase	Within week 3 of Contract Award
3	Progress meeting/ call with Assurance & Reporting Team	Within week 5 of Contract Award and every week thereafter
4	Deliver seven reports (one for each department, and a cross-government project summary.)	No later than 21/05/2020

8. MANAGEMENT INFORMATION/REPORTING

8.1 Relationship to be managed **REDACTED**
8.2 Other key contacts to include:
8.2.1 **REDACTED**
8.2.2 **REDACTED**

9. VOLUMES

9.1 We require the Supplier to complete an 8-week engagement (37-days), between 31st March 2020 and 21st May 2020, producing 7 Reports (one for each department, and a cross-government project summary).

10. CONTINUOUS IMPROVEMENT

10.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

10.2 The Supplier should present new ways of working to the Authority during weekly Contract review meetings.

10.3 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

11. SUSTAINABILITY

None.

12. QUALITY

12.1 The quality of the work will be measured against the successful delivery of the Key Milestones provided within section 7 and 15.

13. PRICE

13.1 We are seeking a fixed price across the 37-day engagement. Any considerations the Supplier makes around the number of Contractors required to look at the four controls across the six organisations (three departments and three ALB's) should consider the funding that has been stipulated by the Authority.

13.2 This translates to an engagement of 37 working days between 31st March 2020 and 21st May 2020.

13.3 Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

13.4 The Contracting Authority's Budget for this is **REDACTED**

14. STAFF AND CUSTOMER SERVICE

14.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

14.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

14.3 The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

15. SERVICE LEVELS AND PERFORMANCE

15.1 The Authority will measure the quality of the Supplier's delivery by:

KPI/SLA	Service Area	KPI/SLA Description	Target
1	Delivery Timescales	Discovery and data collection phase to take place prior to 01st May 2020	01st May 2020 Deadline
2	Quality of Output	To deliver seven reports (one for each department, and a cross-government project summary) by 7th May 2020.	21st May 2020
3	Quality of Output	**REDACTED**	21st May 2020
4	Quality of Output	The cross-government project summary will provide an	21st May 2020

		overarching commentary on the state of government security in respect of the four controls.	
5	Quality of Output	All seven reports will draw on a broad variety of data sources.	21st May 2020

15.2 The Cabinet Office reserves the right to reduce the engagement time at any point before or during the engagement.

16. SECURITY AND CONFIDENTIALITY REQUIREMENTS

16.1 All Contractors must have 'SECURITY CHECK' (SC) or 'DEVELOPED VETTING' (DV) Clearance or above at point of Contract commencement.

16.1.1 Confirmation of this is to be sent to the contracting party prior to engagement. This will be confirmed with the appropriate cluster security unit.

16.2 The reports are to be produced at a classification level of 'Official Sensitive'

16.2.1 All material is to be handled in line with the classifications policy, and the contracting party should be notified if the contractors suspect a breach at any point.

17. PAYMENT AND INVOICING

17.1 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

17.2 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

17.3 Invoices should be submitted to: REDACTED

18. CONTRACT MANAGEMENT

18.1 Attendance to be as directed by The Government Security Group (London). Contract review meetings to take place as required, and as directed by The Government Security Group.

18.2 Attendance at Contract Review meetings shall be at the Supplier's own expense.

19. LOCATION

19.1 The location of the Services will be carried out at host organisations as well as REDACTED

ANNEX B

Supplier Proposal

REDACTED