Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	Project_25753 Security Service Edge
THE BUYER:	Department for Works and Pensions
BUYER ADDRESS	2 St. Peter's Square, Manchester, M23AA
THE SUPPLIER:	Softcat Plc]
SUPPLIER ADDRESS:	Head Office, Fieldhouse Lane, Marlow SL7 1LW
REGISTRATION NUMBER:	02174990]
DUNS NUMBER:	[N/A]
SID4GOV ID:	[N/A]

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 19th February 2024.

It's issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

CALL-OFF LOT(S):

Lot 3: Software and Associated Services

CALL-OFF INCORPORATED TERMS

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

1 This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.

2 Joint Schedule 1(Definitions and Interpretation) RM6068

3 The Framework Special Terms

4 The following Schedules in equal order of precedence:

- Joint Schedules for RM6068
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements)

- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

- Call-Off Schedules for Project_25753 Security Service Edge
- Call-Off Schedule 4 (Call-off Tender) Call-Off Schedule 5 (Pricing Details) Call-Off Schedule 14 (Service Levels) Call-Off Schedule 20 (Call-Off Specification) CCS Core Terms (version 3.0.6)

5 Joint Schedule 5 (Corporate Social Responsibility) RM6068

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

CALL-OFF SPECIAL TERMS

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

Special Term 1: Failure of the product during Implementation or Deployment resulting in the failure of user transition will then require the supplier to reimburse any costs incurred by the Authority during the Implementation and Deployment phases.

Special Term 2: For the purpose of Clause 10.3 of the Core Terms “Ending the contract without a reason”, Buyer shall not terminate this Call-Off contract without cause.

CALL-OFF START DATE:	10th March 2024
CALL-OFF EXPIRY DATE:	23rd April 2027
CALL-OFF INITIAL PERIOD:	3 Years, 1 Month and 20 days
CALL-OFF OPTIONAL EXTENSION PERIOD	2 x 12 month optional extensions.

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)

LOCATION FOR DELIVERY

2 St. Peter’s Square, Manchester, M2 3AA

Title to Goods is transferred to the Buyer on payment to the Supplier in full (save in respect of software where title to the same shall remain at all times with the relevant licensor).

DATES FOR DELIVERY OF THE DELIVERABLES

Contract to commence on 10/03/2024 with the engineering tenant. Main tenant to transition on 24/04/2024.

TESTING OF DELIVERABLES

Not Applicable

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be 90 Days.

MAXIMUM LIABILITY

Each Party's total aggregate liability in each Contract Year under this Call-Off Contract (whether in tort, contract or otherwise) is no more than the lower of £5 million or 125% of the Estimated Yearly Charges.

The Estimated Year 1 Charges used to calculate liability in the first year of the Contract is **REDACTED**

CALL-OFF CHARGES

37 Month Initial Term commitment - Governed Value:

£8,813,375.69 Net (VAT is recoverable)

Published Contract Value – This includes 2 optional 12-month extensions that are subject to confirmation of price at the time of renewal.

£15,276,517.90 Net (VAT is recoverable)

Further pricing details are in Call-Off Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

Annual BAC’s payment

Suppliers must be prepared to use electronic purchase to pay (P2P) routes, including Catalogue and eInvoicing. Suppliers must be prepared to work with DWP to set up and test all electronic P2P routes. This may involve creating technical ordering and invoice files,

including working with our ERP system service suppliers and systems.

BUYER'S INVOICE ADDRESS:

REDACTED

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED

BUYER'S ENVIRONMENTAL POLICY

Not Applicable

BUYER'S SECURITY POLICY

DWP Information Security Policy version 1

DWP Acceptable Use Policy version 2.5

DWP Physical Security Policy version 2.0

DWP Information Management Policy version 4.1

Available at: https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards

SUPPLIER'S AUTHORISED REPRESENTATIVE

REDACTED

SUPPLIER'S CONTRACT MANAGER

REDACTED

PROGRESS REPORT FREQUENCY

Quarterly – First working Day.

QBR Report including data on the three agreed Silver Contract KPIs.

PROGRESS MEETING FREQUENCY

Quarterly

KEY STAFF

N/A

KEY SUBCONTRACTOR(S)

N/A

COMMERCIALLY SENSITIVE INFORMATION

Supplier's pricing and/or any Supplier specific solution(s) for the period of the Call-Off Term +2 years.

SERVICE CREDITS

As per detail in Call-Off Specification 14 (Service Levels).

ADDITIONAL INSURANCES

Not Applicable

GUARANTEE

Not Applicable

SOCIAL VALUE COMMITMENT

Not Applicable

For and on behalf of the Supplier:

REDACTED

For and on behalf of Buyer:

REDACTED

Call-Off Schedule 4 (Call Off Tender)

FURTHER COMPETITION

FOR

SECURITY SERVICE EDGE (SSE)

Project_25753

CONTRACT

UNDER FRAMEWORK RM6068 TECHNOLOGY PRODUCTS AND ASSOCIATED SERVICES

CONTENTS

1. GLOSSARY

1.1. In this Further Competition Invitation the following words and phrases have the following meanings:

“Authority” means Department for Work and Pensions;

“Call-Off Tender” means the tender submitted by the Supplier in response to the Buyer’s Invitation to Tender following a Further Competition Procedure;

“CCS” means the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;

“Contract” means the Call-Off Contract;

“Deliverables” means Goods and/or Services that may be ordered under the Contract;

“Further Competition Template and Invitation to Tender (ITT)” means this document and all related documents published by the Authority in relation to this Further Competition;

“Marking Scheme” means the range of marks that may be given to a Potential Provider depending on the quality of its response to a question which is located in the boxes next to the applicable question;

“Minimum Total Score” means the minimum score that the Potential Provider must obtain in order to be awarded the Contract;

“Order Form” means a completed Order Form Template (or equivalent information issued by the Authority) used to create a Call-Off Contract;

“Order Form Template” means the template in Framework Schedule 6 Order Form Template and Call-Off Schedules;

“Potential Provider” means a company that submits a Call-Off Tender in response to the Further Competition Invitation;

“Schedules” means any attachment to a Framework Contract or Call-Off Contract which contains important information specific to each aspect of buying and selling;

“Supplier” means the person, firm or company identified in the Order Form;

“Tender Clarifications Deadline” means the time and date set out in paragraph 4 for the latest submission of clarification questions; and

“Tender Submission Deadline” means the time and date set out in paragraph 4 for the latest uploading of Tenders.

“Total Score Available” means the maximum potential score that can be awarded for a response to a question.

2. INTRODUCTION

2.1. The Authority is currently seeking a solution to enable secure access to the public internet via a cloud hosted outbound gateway (OWG) and a private application gateway (PAG) service to provide remote client access to services hosted within our private network (both on premise and cloud based), the combination of services being hereafter known as the Security Service Edge (SSE) services.

2.2. The Authority currently has approximately 113,000 users with approximately 113.000 primary devices (desktops and laptops running Windows and MacOS) plus approximately 20,000 mobile devices (mobile phones and tablets running Android, ChromeOS and IOS). It is anticipated that the number of users / primary devices will increase over time to approximately 124,000, whilst the number of mobile devices will decrease to approximately 10,000.

2.3. Currently, the Authority uses the Zscaler Internet Access (ZIA) as its OWG service and the Zscaler Private Access (ZPA) as its PAG service.

2.4. There are two contracts currently in place:

2.4.1. A contract for the provision of ZIA and ZPA for the Authority's 3,000 engineering users running MAC OS devices. This contract expires on 09/03/2024

2.4.2. A contract for the provision of ZIA and ZPA for its main user base of consisting 110,000 users. This contract expires on 23/4/2024.

2.5. The Authority is seeking to combine the contracts for the provision of the OWG and PAG services for the 2 user bases described above.

2.6. This Further Competition Invitation relates to the provision of these SSE services and must be capable of supporting all the Customer's expected 124,000 users and their primary client devices (desktop and laptops) plus approximately 25,000 secondary devices (mobile phones, tablets etc).

2.7. Any solution proposed for either the OWG or PAG requirement that is not one of the existing products listed above i.e., ZIA or ZPA, will need to be 'Proof-of-Concept' (PoC) tested before contract signature as further described in Appendix B to confirm its fitness for purpose. Details of the PoC for each product are further described in Appendix B. It is estimated that the PoC for each product will take 3 months.

2.8. Once the contract is signed, the new solution will also need to be installed, configured, and brought into use with no impact on the current service delivery model and within business constraints and time scales. It is estimated that it will take up to 9 months from the date of contract signature for a product to be fully implemented and brought into use.

2.9. This Further Competition Invitation contains the information and instructions the Potential Provider needs to submit a Tender.

2.10. This Further Competition is being conducted under the CCS Technology Products and Associated Services Framework Agreement (reference RM6068) Lot 3: Software and Associated Services.

2.11. This Further Competition does not oblige the Authority to award a contract or to any level of minimum spend or volume of work.

3. OVERVIEW OF INVITATION TO TENDER

3.1. The following appendices accompany this ITT:

3.1.1. Appendix A – Order Form (Framework Schedule 6 Order Form Template and Call-Off Schedules)

Sets out the rights and obligations which apply to the Potential Provider and the Authority during this Further Competition as per the core terms of the contract and specific Schedules.

3.1.2. Appendix B – Statement of Requirements

A statement issued by the Authority detailing its requirements in respect of Deliverables issued in accordance with the Further Competition Procedure.

3.1.3. Appendix C – Tender Questionnaire

The questionnaire created by the Authority to test the suitability of the Potential Provider to meet necessary criteria in order to provide the required goods and associated services. This is used to provide final scoring and decide the Supplier.

The Tender Questionnaire will tell the Potential Provider how their bid will be evaluated by clearly describing the evaluation model including criteria and relative importance.

4. FURTHER COMPETITION TIMETABLE

4.1. The timetable for this Further Competition is set out in the table below.

4.2. The Authority may change this timetable at any time. Potential Providers will be informed if changes to this timetable are necessary.

4.3. The Authority must receive all Call-Off Tenders before the Tender Submission Deadline.

4.4. Call-Off Tenders received on or after the Tender Submission Deadline may be rejected by the Authority to ensure that all Potential Providers are treated fairly. The decision whether to reject a Call-Off Tender received after the Tender Submission Deadline is made entirely at the Authority's discretion.

DATE ACTIVITY

27/07/2023 Publication of the ITT

31/08/2023 Clarification period starts

07/08/2023 17:00 BST Clarification period closes ("Tender Clarification Deadline")

09/08/2023

17:00 BST Deadline for the publication of responses to Tender Clarification questions

21/08/2023

17:00 BST Deadline for submission of a Tender to the Authority ("Tender Submission Deadline")

21/08/2023 Commencement of Evaluation Process

08/09/2023 Announcement of intention to award and commencement of 'PoC testing (where applicable).

TBC Expected commencement date for the Contract (date dependent on requirement for PoC)

TBC On-boarding and testing date dependent on requirement for PoC)

5. QUESTIONS AND CLARIFICATIONS

5.1. Potential Providers may raise questions or seek clarification regarding any aspect of this Further Competition at any time prior to the Tender Clarification Deadline.

5.2. Please email any clarifications to ed.desktopbag@dwp.gov.uk.

5.3. The Authority will not enter into exclusive discussions regarding the requirements of this Further Competition with Potential Providers.

5.4. To ensure that all Potential Providers have equal access to information regarding this Further Competition, the Authority will publish all its responses to questions raised by Potential Providers on an anonymous basis.

5.5. Responses will be published in a questions and answers document to all Potential Providers who were invited to tender.

5.6. At times the Authority may issue communications to the email address for the Potential Provider contact provided in the Tender Questionnaire, therefore please ensure that this mailbox is reviewed on a regular basis.

6. PRICE

6.1. Tenders will be evaluated on the cost of the Potential Provider quotations.

6.2. The Baseline User Base for the purposes of price evaluation will be 110,000 users/primary devices and 10,000 secondary devices. Potential Providers must declare if their pricing increment (unit of measure) is per user, regardless of the number of devices that user uses, or if their pricing increment (unit of measure) is per device.

6.3. Potential Providers will be asked to submit pricing for the following items:

6.3.1. The provision of technical support resource for the implementation of the products including the provision of technical support during the user roll-out period (Implementation Cost).

6.3.2. The annual running cost for the products for the proposed Baseline User Base for a 5-year period with a minimum term of 2 years with the option for 3 single year extensions. Firm prices need to be provided for the initial 2-year period (2-year Minimum Cost). Variable pricing will also need to be provided for users/devices from 0 users/devices in 1,000 unit increments i.e., 1,000 additional users or 1,000 additional devices.

6.3.3. The annual running cost for the products for the proposed Baseline User Base for a 5-year period with a minimum term of 3 years with the option for 2 single year extensions. Firm prices need to be provided for the initial 3-year period (3-year Minimum Cost). Variable pricing will also need to be provided for users/devices from 0 users/devices in 1,000-unit increments i.e., 1,000 additional users or 1,000 additional devices.

6.4. The price evaluated based upon the total of the Implementation Cost + 2-year Minimum Cost + 3-year Minimum Cost.

6.5. The annual running costs will commence as users/devices are successfully migrated to the new products, in the associated 1,000 unit price band.

7. SUBMITTING A TENDER

7.1. Please submit all bids to ed.desktopbag@dwp.gov.uk within the timeframe specified.

7.2. If a Potential Provider wishes to propose more than one product for consideration, please ensure the tenders are submitted separately.

7.3. A tender must remain valid and capable of acceptance by the Authority for a period to allow the Proof of Concept to be completed this is estimated to be in the region of 90 days following the Announcement of Intention to Award. A Tender with less than 120 days validity after the Announcement of Intention to Award period may be rejected.

8. TENDER EVALUATION

8.1. Tenders will be evaluated in line with the Marking Scheme set out in the accompanying Tender Questionnaire.

8.2. The Total Score Available for each question set out in the Tender Questionnaire is as follows:

QUESTIONNAIRE NUMBER	QUESTIONNAIRE SECTION	TOTAL SCORE AVAILABLE
[1]	Company Information	0%
Information Only		
[1]	Potential Provider Contact Information	0%
Information Only		
[2]	Mandatory Questionnaire	Pass / Fail
[3]	Quality, Solution Implementation and Support	55%
[4]	Price Questionnaire	45%
Total		100%

8.3. If a Potential Provider is evaluated to have scored below 3 for their response to question 7 in Section B of the Quality worksheet in the ITT Questionnaire regarding implementation, that bid will be deemed as non-compliant and will be excluded from the competition.

9. CONTRACT AWARD

9.1. The Potential Provider/s that achieve the highest total score may be invited, subject to the successful conclusion of a period of user and proof of concept testing (where applicable), to contract for the SSE services.

9.2. If two or more Potential Providers obtain the highest total score, the Potential Provider with the highest score for the Price element of the tender evaluation may be invited to contract.

9.3. Upon contract award Potential Providers will be notified of the tender outcome by email.

9.4. The provisions of this paragraph 9 do not supersede the provisions of paragraph 5 of Schedule 7 (No requirement to award).

APPENDIX A TERMS OF THE FURTHER COMPETITION

1. INTRODUCTION

1.1. Sets out the rights and obligations which apply to the Potential Provider and the Authority during this Further Competition as per the core terms of the contract and specific Schedules.

1.2. All Call-Off Schedules and Joint Schedules applicable to this Call-Off contract can be found within Framework Schedule 6 Order Form Template and Call-Off Schedules which are included as part of this Invitation to Tender.

2. CONDUCT

The Potential Provider agrees to abide by these Further Competition Terms and any instructions given in the Further Competition Invitation and agrees to ensure that any of its staff, contractors, subcontractors, consortium members and advisers involved or connected with the Further Competition abide by the same.

2.1. Contact and Canvassing During the Further Competition

The Potential Provider must not directly or indirectly canvass any Minister, public sector employee or agent regarding this Further Competition or attempt to procure any information from the same regarding the Further Competition (except where permitted by the Further Competition Invitation). Any attempt to do so may result in the Potential Provider's disqualification from this Further Competition.

2.2. Collusive Behaviour:

The Potential Provider must not (and shall ensure that its subcontractors, consortium members, advisors or companies within its Group do not:

a) fix or adjust any element of the Tender by agreement or arrangement with any other person,

b) communicate with any person other than the Authority about the value, price or rates set out in the Tender; or information which would enable the precise or approximate value, price, or rates to be calculated by any other person,

c) enter into any agreement or arrangement with any other person, so that person refrains from submitting a Tender,

d) share, permit or disclose to another person access to any information relating to the Tender (or another Tender to which it is party) with any other person,

e) offer or agree to pay, give or does pay, give any sum or sums of money, inducement or valuable consideration directly or indirectly to any other person, for doing or having done or causing or having caused to be done in relation to the Tender any other Tender or proposed Tender, any act or omission,

f) except where such prohibited acts are undertaken with persons who are also participants in the Potential Provider's Tender, such as subcontractors, consortium members, advisors, or companies within its group, or where disclosure to such person is made in confidence in order to obtain quotations necessary for the preparation of the Tender or obtain any necessary security.

2.3. If the Potential Provider breaches paragraphs 2.1 and/or 2.2, the Authority may (without prejudice to any other criminal or civil remedies available to it) disqualify the Potential Provider from further participation in the Further Competition.

2.4. The Authority may require the Potential Provider to put in place any procedures or undertake any such action(s) that the Authority in its sole discretion considers necessary to prevent or curtail any collusive behaviour.

3. COMPLIANCE

3.1. The Potential Provider agrees that in cases where their Tender is deemed non-complaint when compared with the requirements set out within the Invitation to Tender (e.g. budget, terms and conditions) they will be excluded from the Further Competition.

4. RIGHT TO CANCEL OR VARY THE FURTHER COMPETITION

4.1. The Authority reserves the right:

a) To amend, clarify, add to or withdraw all or any part of the Further Competition Invitation at any time during the Further Competition.

b) To vary any timetable or deadlines set out in the Further Competition Invitation.

c) Not to conclude a contract for some or all, of the goods and/or services (as applicable) for which Tenders are invited.

d) to cancel all or part of the Further Competition at any stage at any time.

4.2. The Potential Provider accepts and acknowledges that by issuing the Further Competition Invitation, the Authority is not bound to accept a Tender or obliged to conclude a contract with the Potential Provider at all.

APPENDIX B STATEMENT OF REQUIREMENTS

1. INTRODUCTION AND BACKGROUND TO THE AUTHORITY

1.1. The Department for Work and Pensions (the Authority) is the UK government's largest public service department with the biggest annual budget, touching every citizen in the country at some point in their lives.

1.2. We are delivering a modern, fair and affordable welfare system that makes a sustainable positive difference to citizens' lives. We are supporting everyone who can or wants to work to do so by extending opportunity, strengthening personal responsibility, and enabling fulfilment of personal potential.

1.3. The Authority is currently running SSE services from Zscaler for its 113,000 users.

2. OVERVIEW OF REQUIREMENT

2.1. The Authority is looking to implement a platform to enable secure access to the public internet via a cloud hosted outbound gateway (OWG) service and to enable private application gateway (PAG) services to provide remote client access to services hosted within our private network (both on premise and cloud based).

The solution must ensure that all traffic to and from an Authority client is fully encrypted (except where the Authority defined policy allows unencrypted flow) and is subject to inspection and data protection protocols. The service must support all the departments client devices, specifically:

- Windows 10
- Windows 11
- MacOS
- ChromeOS
- IOS
- Android.

2.2. The Authority's curent estate consists of circa 113,000 colleagues utilising circa 113,000 traditional primary devices (desktops and laptops) and circa 20,000 secondary mobile devices, all of which will need secure access to the public IP and the Authority's private IP address spaces. Additionally, provision for a separate Engineering and three additional test environments is required. Each environment must be logically separate, with a separate identity provider (IDP) and no mixing of data streams or policy.

2.3. The Authority is a user of the Microsoft 365 platform and as such the OWG service must support the delivery of encrypted traffic to Microsoft365 in volumes to support our entire user community (including real time traffic such as Teams media). The solution MUST enforce an automated mechanism to inspect the M365 traffic in accordance with Microsoft's own recommendations. For the avoidance of doubt, automated in this instance means that changes to the Microsoft guidance on what protocols \ services to inspect are applied rapidly (<24 hours) to the system with no intervention required by the Authority.

2.4. The OWG service will also offer curated categories (e.g., Gambling, Adult Content etc.) which can be used by the Authority to grant or deny access based on both a global policy and a granular policy down to AzureAD group level. The service must allow the Authority to create its own categories of URL such that we may construct bespoke policies (i.e., Access to category x is denied except where a user is in AAD group).

2.5. The PAG service must provide secure access to the Authority private IP address space for the purposes of application or service access. This should be done in a way which is compliant with the Authority zero trust principles which enforce authentication and deny inbound traffic routes.

2.6. The PAG service must, as a minimum:

- Support up to 300 discrete private network endpoints (each with multiple IP ranges) with no cross-network routing available.
- Support the connection of users to these address spaces allowing that the address spaces may be hosted on premise or in our strategic cloud partner environments (AWS, Azure and GoogleCloud).
- Ensure both IPv6 and v4 are supported.
- Allow for routes to be defined on allowed IPs and ports (i.e., IP address on port x and y is allowed, but all other ports are blocked).
- Support a direct route for data flow, whilst maintaining the encryption and security of the data but avoiding 'tromboning' through a single location.

3. SPECIFICATION

3.1. The Authority is seeking a minimum 2-year contract with an option to extend by further 3 x 1-year periods. The Authority reserves the right to award a contract with a minimum duration longer than 2 years at its sole discretion.

3.2. The Tender Questionnaire included as part of the Invitation to Tender sets out as Quality and Pricing requirements as part of this evaluation.

3.3. The Authority reserves the right to exclude a Potential Provider where, in the reasonable opinion of the Authority, the software terms and conditions submitted by that Potential Provider are inconsistent with the Authority's requirements.

4. PROOF-OF-CONCEPT TESTING

4.1. Prior to contract award, the Authority may require, at its sole discretion, to undertake a period of Proof-of-Concept (PoC) to ensure that the products proposed by the Potential Provider are fit for purpose in the Authority's environment. To support the PoC testing, the Potential Provider will be required to provide suitable access to the proposed products together with technical support sufficient for the Authority to determine that the product is fit for purpose. Access to the proposed products and the provision of technical support for the PoC must be provided to the Authority by the Potential Provider free of charge.

4.2. For each of the OWG and PAG services, the PoC will take approximately 3 months and will include the following activities:

- Provision of a test instance of the proposed product.
- Configuration of Authority's test infrastructure and devices (up to 30 devices) to enable testing of the product's capabilities.
- Configuration of the test instance of the product with suitable test rules etc, such that the product's functionality can be determined.
- Testing of the proposed product's capabilities to deliver the services.

- Validation that the product can be managed through the web console and that such management is business policy focused with no need for low level knowledge (e.g. networking, firewall, encryption or SDWAN) above and beyond that of the existing product (ZIA).

4.3. It is intended that the PoC for each product will run concurrently.

4.4. Details for the PoC for the OWG service are as follows:

4.4.1. The objective for the PoC is to establish that the proposed solution is capable of enabling the Authority's users to browse internet resources from 30 client devices accessing the internet from both an untrusted and trusted network, with all access authenticated against the the Authority's IDP and, access to internet content being based on a policy engine which includes an 'allow' list, a block list and the ability to add custom rules.

4.4.2. The Authority will support the PoC by providing an Azure Active Directory (AAD) environment with the following client types connected:

- Windows 10 (22H2)
- Windows 11
- MacOS
- IOS
- Android

The AAD will be configured in hybrid mode with a local Windows 2019 Domain.

Some of the Windows 10 devices will authenticate against the 2019 domain, all other clients shall authenticate against AAD.

This is shown in the diagram below.

4.4.3. During the PoC the following activities will be tested:

1 – Confirm connectivity from all client types

2 – Confirm Authentication

3 – Confirm group membership is visible

4 – Confirm group membership changes are seen

5 – Apply Allow list and link to specific groups

6 – Apply Deny list and link to specific groups

7 – Add categories to lists

8 – Add custom URLs to lists

9 – Validate correct behaviour of browsing (list filtered)

10 – Validate correct behaviour across all client types

11 – Validate associated MI

12 – Amend policy and re-validate against all client types

13 – Validate malware inspection by browsing malware test site

13 – Access Certificate Pinning site by excluding inspection

14 – Access M365 sites and confirm inspection level (in line with latest MS JSON)

15 – Simulate the generation of complex business rules within the web interface

16 – Simulate the performing of troubleshooting tasks within the web interface.

4.4.4. The success criteria for the PoC are as follows:

1 – The above activities can be completed successfully.

2 – The configuration and administration of the service are acceptable for deployment and ongoing operational use by the Authority.

3 – The ongoing administration of the service meets the DWP expectation in terms of being policy rather than protocol based. Meaning that specialised, low level knowledge is not required to successfully implement, maintain and troubleshoot the proposed solution.

4 – The Authority is confident that the solution is capable of being deployed to all client components at scale across all client types.

5 – The Authority is confident that the product is suitable to protect the Authority's infrastructure from malware.

4.5. Details for the PoC for the PAG service are as follows:

4.5.1. The objective for the PoC is to establish that the proposed solution is capable of enabling access from a collection of the Authority's clients to a private IP address range hosted in the Authority's estate and a private IP address range hosted with an AWS VPC.

4.5.2. The Authority will support the PoC by providing an Azure Active Directory (AAD) environment with the following client types connected:

- Windows 10 (22H2)
- Windows 11
- MacOS
- IOS
- Android

All clients shall authenticate against AAD.

An on-premise IP range shall be configured such that it hosts a single IP service. It shall have no connectivity or DNS presence on the public internet. It shall have a firewall that can be configured to allow specific outbound traffic onto the internet.

An Authority dedicated VPC shall be configured to host a number of private IP services, none of these services shall be directly accessible or advertised on the public internet. It shall have a firewall that can be configured to allow specific outbound traffic onto the internet.

This is shown in the diagram below.

4.5.3. During the PoC the following activities will be tested:

1 – Confirm connectivity from all client types

2 – Confirm Authentication

3 – Confirm group membership is visible

4 – Confirm group membership changes are seen

5 – Configure list to url and link to specific groups

6 – Configure list to IP\Port and link to specific groups

7 – Test basic HTTP(s) over link

8 – Test full TCP (SSH + SMB3) over link

9 – validate correct behaviour of access (allow and block)

10 – Validate correct behaviour across all client types

11 – Validate associated MI

12 – Amend policy and re-validate against all client types

13 – Simulate the generation of complex business rules within the web interface.

4.5.4. The success criteria for the PoC are as follows:

1 – The above activities can be completed successfully.

2 – The configuration and administration of the service are acceptable for deployment and ongoing operational use by the Authority.

3 – The ongoing administration of the service meets the DWP expectation in terms of being policy rather than protocol based. Meaning that specialised, low level knowledge is not required to successfully implement, maintain and troubleshoot the proposed solution.

4 – The Authority is confident that the solution is capable of being deployed to all client components at scale across all client types.

5 – The Authority is confident that the product is suitable to protect the Authority's infrastructure from malware.

6 – The Authority is confident that it will have the ability to include any client in the Authority's client build processes.

4.6. During the period of the PoC the Potential Provider should conduct its own due diligence of the Authority's IT infrastructure and estate to be able to assure itself and the Authority, that the products proposed are fit-for-purpose and will scale to meet the Authority's user/device volumes. The Authority will provide the appropriate access to its resources to support this activity.

4.7. On completion of the PoC and prior to contract award, based upon the results of the PoC and the Potential Provider's due-diligence as described above, the Potential will be required to submit a detailed implementation plan that should:

1) Be fully itemised including all steps, actions, call off schedule deliverables, dependencies, risks, issues and timings leading to implementation by dates agreed between the Authority and Potential Provider.

2) Clearly identify the activities from the Authority that are required to achieve a successful implementation, including but not limited to:

a. input and support to produce the system configuration design document

b. infrastructure and resource provision

c. system and user acceptance testing

3) Include training and support requirements (user training, support and self-guidance).

4) As part of this submission, the Potential Provider should provide a detailed RACI matrix to support the draft detailed implementation plan that clearly sets out what activities the Potential Provider is undertaking and their dependencies on the Authority and 3rd parties.

5. SUPPORT FOR IMPLEMENTATION AND END USER ROLL OUT

5.1. The Authority requires the Potential Provider to undertake and manage the implementation of the product(s) together with the deployment and roll-out to end users. The Potential Provider will need to provide sufficient resources to achieve this.

5.2. Post the PoC (where required) there will be a period of implementation and testing of the solutions. Once these have been completed to the satisfaction of the Authority they will be deployed to the end-users. The Authority anticipates the duration of implementation and testing to be approximately 3 months. The Authority anticipates the duration of end-user roll out to be approximately 3 months. This applies to both the OWG and PAG services and the Authority expects these workstreams to run concurrently.

5.3. The Authority will provide the resources shown in the table below to support the implementation and roll-out. The Authority has identified the Skills Framework for the Information Age (SFIA) level for each resource based upon the SFIA levels defined in Appendix D:

Phase/ Estimated Duration	Resource	SFIA Level	Effort (FTE)
Design – 6 weeks	Architect (product architect of the existing product)	6	0.5
	Lead Engineer (senior engineer owning the current product implementation)	6	0.5
	MacBook Engineer (owning the existing non-production service)	4	0.25
	Mobile Engineer (owning the existing implementation on mobile)	4	0.25
Test - 6 weeks	Packager (packaging expert for SCCM, InTune)	3	0.25
	Packager (AirWatch and JAMF packager)	3	0.25
	QA Tester (experienced test engineer)	3	0.5
	Infrastructure Tester (experienced test engineer)	3	1
Deployment – 12 weeks	Lead Engineer (engineering owner of the proposed solution)	6	0.5
	Product Engineer (operational owner of the proposed solution)	5	1
	level 2 Support Engineer (senior support engineer)	3	1
Oversight / Project Management – full duration	Product Owner (Digital Owner of the service line)	7	0.25
	Program Manager (experienced DWP PM to handle business liaison and impact)	6	0.5
	Project Manager (to assist in planning the deployment activity)	5	1

5.4. The Authority believes that, as a minimum, the Potential will need to provide a Technical Delivery Manager (1 FTE) for a period of 6 months (with an option to extend). This resource will be required to:

a. Contribute to and manage the project plan the implementation and roll-out of the products – working alongside the Authority's project manager.

b. Provide timely and meaningful updates on all actions outstanding with the Potential Provider.

c. Co-ordinate the Potential Provider's engineering and operational support where required.

d. Provide the Potential Provider's best practice regarding, deployment, support and support upskilling.

e. Represent the Potential Provider at Planning and project boards.

f. Represent the Potential Provider and associated actions at the risk review board.

5.5. The Potential Provider must also describe any additional resources required to complete the implementation of the solution, for example engineering and project management resource as well as specialist training support etc, in their Statement of Work provided in response to question B 7 of the Quality worksheet of the ITT Questionnaire (Appendix C).

5.6. The Potential Provider MUST provide the Skills Framework for the Information Age (SFIA) level for each resource described in their Statement of Work based upon the SFIA levels defined in Appendix D

5.7. The Potential Provider must provide a price for each resource they are providing as identified in their Statement of Work in their response to the pricing section in Appendix C.

APPENDIX C TENDER QUESTIONNAIRE

1. INTRODUCTION

1.1. The attached Excel Spreadsheet - Appendix C sets out the questions that will be evaluated as part of this Further Competition.

1.2. The following information has been provided in relation to each question (where applicable):

- Weighting – highlights the relative importance of the question,
- Guidance – sets out information for the Potential Provider to consider when preparing a response, and
- Marking Scheme – details the marks available to evaluators during evaluation.

1.3. The responses to the Mandatory and Quality questions for Lot 1 and Lot 2 and their associated evaluations, will be used as the Mandatory and Quality response and evaluation for Lot 3.

2. DOCUMENT COMPLETION

2.1. Potential Providers must provide a response to every question contained on the Tender Questionnaire.

2.2. Potential Providers must not alter / amend the document in any way.

2.3. Potential Providers must not submit any additional information other than that specifically requested in this document.

2.4. Potential Providers must provide a copy of the software terms and conditions as part of their response to the ITT.

2.5. Potential Providers must submit their response via the Tender Questionnaire.

REDACTED

Call-Off Schedule 14 (Service Levels)

Definitions

In this Part Call-Off Schedule 14, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

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

Performance Monitoring Report Means a Performance Monitoring Report as specified by Section 3 of this Call-Off Schedule 14

"Service Level Failure" means a failure to meet the Service Level Performance Measure in respect of a Service Level;

"Service Level Performance Measure" shall be as set out against the relevant Service Level in the Annex to Section 2 of this Call-Off Schedule 14; and

"Service Level Threshold" shall be as set out against the relevant Service Level in the Annex to Section 2 to this Call-Off Schedule 14

1. What happens if you don’t meet the Service Levels

1.1 The Supplier shall at all times provide the Deliverables to meet the Service Level Performance Measure for each Service Level.

1.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Section 2 to this Schedule 14 including the right to any Service Credits, which are a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier’s failure to meet any Service Level Performance Measure.

1.3 The Supplier shall send Performance Monitoring Reports to the Buyer in accordance with the provisions of Section 3 (Performance Monitoring) of this Call-Off Schedule 14.

2. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

2.1 the Buyer shall be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("Compensation for Critical Service Level Failure"),

provided that the operation of this paragraph 2 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Section 2: Service Levels and Service Credits

1. Service Levels

1.1 If the level of performance of the Supplier is likely to or fails to meet any Service Level Performance Measure the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.1.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer;

1.1.2 instruct the Supplier to comply with the Rectification Plan Process;

1.1.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.1.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

ANNEX 1 TO SECTION 2: SERVICES LEVELS

REDACTED

Section 3: Performance Monitoring

1. Performance Monitoring and Performance Review

1.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of the proposed process for monitoring and reporting of Service Levels, and the Parties will try to agree the process as soon as reasonably possible.

1.2 The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") as agreed pursuant to paragraph 1.1 above which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

1.2.1 for each Service Level, the actual performance achieved over the relevant Service Period;

1.2.2 a summary of all failures to achieve Service Levels;

1.2.3 details of any Critical Service Level Failures;

1.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

1.2.5 such other details as the Buyer may reasonably require .

1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("Performance Review Meetings") on a Quarterly basis to review by Performance Monitoring Reports. The Performance Review Meetings shall :

1.3.1 take place within one (1) week of the Performance Monitoring Reports being issued at such location and time (within normal business hours) as the Parties may agree;

1.3.2 be attended by the Supplier's Representative and the Buyer’s Representative; and

1.3.3 be fully minuted by the Supplier, with the minutes circulated by to all attendees at the relevant meeting and also any other recipients agreed at the relevant meeting.

1.4 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier for any specified Service Period.

Call-Off Schedule 20 (Call-Off Specification)

1. Specification of the System, Service and Deliverables

1.1 For the purposes of this call-off, the specification of the system, service, and deliverables "**The Specification",** is defined in accordance with the following:

1. The requirements defined in Appendix B – that has been inserted below.

2. The Supplier's response to the Further Competition Invitation to Tender for Security Service Edge as documented in the response document Appendix B - Detailed Requirements – XXXX.

1.2 The Buyer recognises that the system and services are delivered as a Software-As-A-Service (SaaS) system and services and that the Supplier's SaaS system and services are used by other customers of the Supplier.

1.3 Nothing in this call-off shall prevent the Supplier from replacing any component of the system or service with a different component or service or modifying any such component or service, provided that the Supplier shall use reasonable endeavours, in accordance with good IT industry practice, to maintain the system, its functionality and the associated services such that:

1. the performance and functionality of the replaced or modified component or service is equivalent to or greater than the performance and functionality of the original item as defined in The Specification, in all material respects; and
2. the performance and functionality of the entire system or service is equivalent to or greater than the performance and functionality of the entire system and service (incorporating such original item) as defined in The Specification, in all material respects; and
3. the terms of this call-off shall apply to the replaced or modified component or service.

REDACTED