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

Order Form

CALL-OFF REFERENCE:	24950
THE BUYER:	Department for Work and Pensions
BUYER ADDRESS	Caxton House, Tothill Street, London, SW1H 9NA
THE SUPPLIER:	WFL UK Ltd.
SUPPLIER ADDRESS:	The Broadgate Tower Third Floor, 20 Primrose Street, London, EC2A 2RS, England
REGISTRATION NUMBER:	00594001
DUNS NUMBER:	216313445
SID4GOV ID:	**[Insert** if known]

This Order Form is for the provision of the Call-Off Deliverables and dated 14/3/24. It's issued under the Framework Contract with the reference number RM6177 National Fuels (2) for the provision of Fuels and Associated Services.

CALL-OFF LOT(S):

Lot Number	Lot Description	Relevant (Yes/ No)
111	Liquid Fuel - England South West – Weymouth	Yes

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) RM6177 National Fuels (2)
3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6177 National Fuels (2)
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 6 (Key Subcontractors)
        - Joint Schedule 7 (Financial Difficulties)
        - Joint Schedule 9 (Minimum Standards of Reliability)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)
        - Joint Schedule 12 (Supply Chain Visibility)
    - Call-Off Schedules for Call-Off 24950
        - Call-Off Schedule 1 (Transparency Reports)
        - Call-Off Schedule 2 (Staff Transfer)
        - Call-Off Schedule 3 (Continuous Improvement)
        - Call-Off Schedule 5 (Pricing Details)
        - Call-Off Schedule 7 (Key Supplier Staff)
        - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
        - Call-Off Schedule 9 (Security)
        - Call-Off Schedule 10 (Exit Management)
        - Call-Off Schedule 11 (Installation Works)
        - Call-Off Schedule 14 (Service Levels)
        - Call-Off Schedule 15 (Call-Off Contract Management)
        - Call-Off Schedule 16 (Benchmarking)
        - Call-Off Schedule 20 (Call-Off Specification)
4. CCS Core Terms (version 3.0.8)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6177 National Fuels (2)
6. Call-Off Schedule 4 (Supplier Response) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the 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:
Security DWP policy

Special Term	Amendment to Call Off Schedule/ Core Terms / Joint Schedule	Amendment to Clause	Further details of amendment
Security policy	Schedule 9		

CALL-OFF START DATE: **01/04/2024**

CALL-OFF EXPIRY DATE: **31/03/2026**

CALL-OFF INITIAL PERIOD: **2 Years**

CALL-OFF EXTENSION START DATE: **N/A**

CALL-OFF EXTENSION EXPIRY DATE: **N/A**

CALL-OFF EXTENSION PERIOD: **N/A**

CALL-OFF DELIVERABLES
See details in Call-Off Schedule 20 (Call-Off Specification)

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£23,217.00** Estimated Charges in the first 12 months of the Contract. The Buyer must always provide a figure here]

CALL-OFF CHARGES
See details in Call-Off Schedule 5 (Pricing Details)]
All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)]
The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- [Indexation]
- [Specific Change in Law]

- [Benchmarking using Call-Off Schedule 16 (Benchmarking)]

REIMBURSABLE EXPENSES
NOT APPLICABLE

PAYMENT METHOD
BACS payment method, monthly in arrears. Payments within 30 days of receiving an invoice.

BUYER'S INVOICE ADDRESS:
FAO - Inspired Energy
29 Progress Business Park
Kirkham
PR4 2TZ
bureau@inspiredenergy.co.

BUYER'S AUTHORISED REPRESENTATIVE
Head of Energy and Sustainability
DWP Estates
Third Floor
Caxton House
Tothill Street
London
SW1H 9NA
Email:

BUYER'S ENVIRONMENTAL POLICY
See link below

Environmental policy - GOV.UK (www.gov.uk)

BUYER'S SECURITY POLICY
Appended at Call-Off Schedule 9

SUPPLIER'S AUTHORISED REPRESENTATIVE

SUPPLIER'S CONTRACT MANAGER

PROGRESS REPORT FREQUENCY
Weekly during mobilisation, with a view to moving to monthly: On the first Working Day of each calendar month.

PROGRESS MEETING FREQUENCY

Weekly during mobilisation, with a view to moving to Quarterly: on the first Working Day of each quarter.

KEY STAFF

KEY SUBCONTRACTOR(S)
NA

COMMERCIALLY SENSITIVE INFORMATION
[Call off Schedule 4 and Call off Schedule 5 Supplier's Commercially Sensitive Information]

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
There's a guarantee of the Supplier's performance provided for all Call-Off Contracts entered under the Framework Contract

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)]

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:	22.4.24	Date:	13.3.24

Call-off Schedule 5 – pricing details

Site	**Supplier Name**	**Pence per Litre Margin (£0.0450 will be displayed as 4.50)**	**Contract Start**	**Contract Expiry**
Weymouth	WFL UK Ltd		01/04/2024	31/03/2026

CALL OFF SCHEDULE 9 – SPECIAL TERMS: SECURITY REQUIREMENTS

GENERAL

The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this Schedule [6] to the Contract (the "**Authority's Security Requirements**"). The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority's Systems Environment and the Contractor's Systems Environment.

Terms used in this Schedule 7 which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

1. DEFINITIONS

1.1 In this Schedule 7, the following definitions shall apply:

"Authority Personnel"	shall mean all persons employed by the Authority including directors, officers, employees together with the Authority's servants, agents, consultants, contractors and suppliers but excluding the Contractor and any Sub-contractor (as applicable).
"Availability Test"	shall mean the activities performed by the Contractor to confirm the availability of any or all components of any relevant ICT system as specified by the Authority.
"**CHECK**"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"**Cloud**"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.
"**Cyber Essentials**"	shall mean the Government-backed, industry-supported scheme managed by the NCSC to help organisations to protect themselves against online threats or the relevant successor or replacement

scheme which is published and/or formally recommended by the NCSC.

"**Cyber Security Information Sharing Partnership**" or "**CiSP**"	shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
"**Good Security Practice**"	shall mean: a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology); b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and c) the Government's security policies, frameworks, standards and guidelines relating to Information Security.
"**Information Security**"	shall mean: a) the protection and preservation of: i) the confidentiality, integrity and availability of any Authority Assets, the Authority's Systems Environment (or any part thereof) and the Contractor's Systems Environment (or any part thereof); ii) related properties of information including, but not limited to,

	authenticity, accountability, and non-repudiation; and b) compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets.
"**Information Security Manager**"	shall mean the person appointed by the Contractor with the appropriate experience, authority and expertise to ensure that the Contractor complies with the Authority's Security Requirements.
"**Information Security Management System ("ISMS")**"	shall mean the set of policies, processes and systems designed, implemented and maintained by the Contractor to manage Information Security Risk as certified by ISO/IEC 27001.
"**Information Security Questionnaire**"	shall mean the Authority's set of questions used to audit and on an ongoing basis assure the Contractor's compliance with the Authority's Security Requirements.
"**Information Security Risk**"	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.
"**ISO/IEC 27001, ISO/IEC 27002 and ISO 22301**	shall mean a) ISO/IEC 27001; b) ISO/IEC 27002/IEC; and c) ISO 22301 in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO.
"**NCSC**"	shall mean the National Cyber Security Centre or its successor entity (where applicable).
"**Penetration Test**"	shall mean a simulated attack on any Authority Assets, the Authority's Systems Environment (or any part thereof) or the Contractor's Systems Environment (or any part thereof).
"**Risk Profile**"	shall mean a description of any set of risk. The set of risks can contain those that relate to a whole

	organisation, part of an organisation or as otherwise applicable.
"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
"**Tigerscheme**"	shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd.
"**Vulnerability Scan**"	shall mean an ongoing activity to identify any potential vulnerability in any Authority Assets, the Authority's Systems Environment (or any part thereof) or the Contractor's Systems Environment (or any part thereof).

1.2 Reference to any notice to be provided by the Contractor to the Authority shall be construed as a notice to be provided by the Contractor to the Authority's Representative.

2. PRINCIPLES OF SECURITY

2.1 The Contractor shall at all times comply with the Authority's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. ISO/IEC 27001 COMPLIANCE AND AUDIT

3.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with ISO/IEC 27001 in relation to the Services during the Contract Period.

3.2 The Contractor shall appoint an Information Security Manager and shall notify the Authority of the identity of the Information Security Manager on the Commencement Date and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.

3.3 The Contractor shall ensure that it operates and maintains the Information Security Management System during the Contract Period and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

a) a scope statement (which covers all of the Services provided under this Contract);
b) a risk assessment (which shall include any risks specific to the Services);
c) a statement of applicability;
d) a risk treatment plan; and
e) an incident management plan

in each case as specified by ISO/IEC 27001.

The Contractor shall provide the Information Security Management System to the Authority upon request within 10 Working Days from such request.

3.4 The Contractor shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Authority.

3.5 Notwithstanding the provisions of paragraph **Error! Reference source not found.** to paragraph **Error! Reference source not found.**, the Authority may, in its absolute discretion, notify the Contractor that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Contractor shall, at its own expense, undertake those actions required in order to comply with the Authority's Security Requirements within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Authority's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A.

4. CYBER ESSENTIALS SCHEME

4.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials (the "Cyber Essentials Certificate") in relation to the Services during Contract Period. The Cyber Essentials Certificate shall be provided by the Contractor to the Authority annually on the dates as agreed by the Parties.

4.2 The Contractor shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Certificate within 2 Working Days of confirmation of such failure or revocation. The Contractor shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Certificate during the Contract Period after the first date on which the Contractor was required to provide a Cyber Essentials Certificate in accordance with paragraph **Error! Reference source not found.** (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A.

5. RISK MANAGEMENT

5.1 The Contractor shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Contract Period which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Authority's Security Requirements are met (the **Risk Assessment**). The Contractor shall provide the Risk Management Policy to the Authority upon request within 10 Working Days of such request. The Authority may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Authority's Security

Requirements. The Contractor shall, at its own expense, undertake those actions required in order to implement the changes required by the Authority within one calendar month of such request or on a date as agreed by the Parties.

5.2 The Contractor shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the threat landscape or (iii) at the request of the Authority. The Contractor shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Contractor shall notify the Authority within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

5.3 If the Authority decides, at its absolute discretion, that any Risk Assessment does not meet the Authority's Security Requirements, the Contractor shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

5.4 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Authority in relation to the Authority's own risk management processes regarding the Services.

5.5 For the avoidance of doubt, the Contractor shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph **Error! Reference source not found.**. Any failure by the Contractor to comply with any requirement of this paragraph **Error! Reference source not found.** (regardless of whether such failure is capable of remedy), shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A.

6. SECURITY AUDIT AND ASSURANCE

6.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Authority (the "**Information Security Questionnaire**") at least annually or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

6.2 The Contractor shall conduct Security Tests to assess the Information Security of the Contractor's Systems Environment and, if requested, the Authority's Systems Environment. In relation to such Security Tests, the Contractor shall appoint a third party which i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at

least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the Authority's System Environment or (iii) at the request of the Authority which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Authority. The Contractor shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Contractor shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Authority in its absolute discretion.

6.3 The Authority shall be entitled to send the Authority's Representative to witness the conduct of any Security Test. The Contractor shall provide to the Authority notice of any Security Test at least one month prior to the relevant Security Test.

6.4 Where the Contractor provides code development services to the Authority, the Contractor shall comply with the Authority's Security Requirements in respect of code development within the Contractor's Systems Environment and the Authority's Systems Environment.

6.5 Where the Contractor provides software development services, the Contractor shall comply with the code development practices specified in the Specification or in the Authority's Security Requirements.

6.6 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Contractor's Systems Environment after providing advance notice to the Contractor. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Contractor shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Authority at its absolute discretion. The Contractor shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require.

6.7 The Authority shall schedule regular security governance review meetings which the Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

7. SECURITY POLICIES AND STANDARDS

7.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.

7.2 Notwithstanding the foregoing, the Authority's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Contract Change, any change in the Authority's Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change

Procedure. Where any such change constitutes an Operational Change, any change in the Authority's Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

7.3 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

8. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

8.1 The Contractor may become a member of the Cyber Security Information Sharing Partnership in accordance with the recommendations by the NCSC during the Contract Period. The Contractor may participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

8.2 Where the Contractor becomes a member of the Cyber Security Information Sharing Partnership, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Contractor's Risk Management Policy.

ANNEX A – AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Acceptable Use Policy

b) Information Security Policy

c) Physical Security Policy

d) Information Management Policy

e) Email Policy

f) Technical Vulnerability Management Policy

g) Remote Working Policy

h) Social Media Policy

i) Forensic Readiness Policy

j) SMS Text Policy

k) Privileged Users Security Policy

l) User Access Control Policy

m) Security Classification Policy

n) Cryptographic Key Management Policy

o) HMG Personnel Security Controls – May 2018 (published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

p) NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:
https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

a) SS-001 - Part 1 - Access & Authentication Controls
b) SS-001 - Part 2 - Privileged User Access Controls
c) SS-002 - PKI & Key Management
d) SS-003 - Software Development
e) SS-005 - Database Management System Security Standard
f) SS-006 - Security Boundaries
g) SS-007 - Use of Cryptography
h) SS-008 - Server Operating System
i) SS-009 - Hypervisor
j) SS-010 - Desktop Operating System
k) SS-011 - Containerisation
l) SS-012 - Protective Monitoring Standard for External Use
m) SS-013 - Firewall Security
n) SS-014 - Security Incident Management
o) SS-015 - Malware Protection
p) SS-016 - Remote Access
q) SS-017 - Mobile Devices
r) SS-018 - Network Security Design
s) SS-019 - Wireless Network
t) SS-022 - Voice & Video Communications
u) SS-023 - Cloud Computing
v) SS-025 - Virtualisation
w) SS-027 - Application Security Testing
x) SS-028 - Microservices Architecture
y) SS-029 - Securely Serving Web Content
z) SS-030 - Oracle Database
aa) SS-031 - Domain Management
bb) SS-033 - Patching

Call-Off Schedule 20 (Call-Off Specification)