



Specification

Title: Provision of dSeries Workload Automation for Hybrid Cloud

Contract Reference: PS/25/19A

Framework Title & Reference: Technology Products and Associated Services 2 RM6098

1. Introduction 3

2. Background to the Requirement 3

3. Procurement Timetable 3

4. Scope 4

5. Implementation and Deliverables 4

6. Specifying Goods and / or Services 4

7. Quality Assurance Requirements..... 6

8. Other Requirements 6

9. Management and Contract Administration..... 13

10. Documentation..... 13

11. Arrangement for End of Contract 13

12. Response Evaluation..... 13

Annex 1 16

Evaluation Criteria 16

1. Introduction

As outlined in the Invitation to Tender (ITT), and in accordance with the terms and conditions of Technology Products and Associated Services 2 Framework RM6098 Driver and Vehicle Licensing Agency (DVLA) (**the Buyer**) invites proposals for the provision of dSeries Workload Automation for Hybrid Cloud as detailed in this Specification.

2. Background to the Requirement

The DVLA is an Executive Agency of the Department for Transport (DfT), based in Swansea. The DVLA's primary aims are to facilitate road safety and general law enforcement by maintaining accurate registers of drivers and vehicle keepers and to collect Vehicle Excise Duty (VED).

DVLA currently have a contract for the provision of Workload Automation Subscription Licences which expires 31/08/25.

DVLA have been in discussions with the Software Vendor, Broadcom, who have advised that the licensing model has changed. The solution which best suits DVLA requirements is dSeries Workload Automation for Hybrid Cloud.

Broadcom Workload Automation is an application used in DVLA for the scheduling of batch jobs. It underpins the main batch runs for DVLA's core services and runs both day and overnight 365 days a year.

The contract will be for 1 year covering period 01/09/25 – 31/08/26.

Full details included in Section 6.

3. Procurement Timetable

The timetable for this Procurement is set out in the below table. The timetable may be changed at any time but any changes to the dates will be made in accordance with the Regulations (where applicable).

Tenderers will be informed if changes to the timetable are necessary.

The key dates for this procurement (**Timetable**) are currently anticipated to be as follows:

Event	Date
Issue of the ITT	05/08/25
Deadline for receipt of clarifications	17:00hrs on 11/08/25
Deadline for the publication of responses to ITT clarification questions	17:00hrs on 12/08/25
Deadline for receipt of responses	23:59hrs on 18/08/25

Evaluation of responses	19/08/25 – 27/08/25
Notification of contract award	28/08/25
Execution (signature) of Call-Off Contract	By 01/09/25
Commencement Date of Contract / Provision of Service	01/09/25

The Buyer reserves the right to amend the above Timetable. Any changes to the Timetable shall be notified to all tenderers as soon as practicable.

4. Scope

The scope of the requirement extends to the provision of licences/services detailed in section 6 for a period of 1 year with an expected start date of 01/09/25.

5. Implementation and Deliverables

The contract start date is 01/09/25. In the event of the procurement process exceeding the contract start date, the contract will be back dated to start 01/09/25.

6. Specifying Goods and / or Services

This requirement is for the provision of dSeries Workload Automation for Hybrid Cloud as detailed in the below table:

Product Description	SKU	Quantity/Executions	Period
dSeries Workload Automation for Hybrid Cloud	DSRCLD990	50,000 Executions per month across all environments. Unlimited agent installations Unlimited environment installations	01/09/25 – 31/08/26

DVLA have an associated Account Managers at Broadcom who will be able to assist suppliers in pricing this requirement. Details below:

Names: **REDACTED** and **REDACTED**

Email Addresses: **REDACTED** and **REDACTED**

6.1 Service Levels

Required service levels are detailed in the below table:

Severity Level	Incident Addressed	Response Time Objective	Severity Level Description
1	24/7	1 hour	System down or product in an inoperative condition that is having an impact on a production environment
2	During normal business hours	2 business hours	High impact business condition possibly endangering a production environment. The software may operate but is severely restricted.
3	During normal business hours	4 business hours	Low impact business conditions with a majority of software functions still usable. However some circumvention may be required to provide service.
4	During normal business hours	1 business day	Minor problem or question that does not affect the software's functionality

6.2 Social Value Considerations

The Social Value Act (2012) requires contracting authorities to consider social value when procuring services, by taking into account the additional social benefits that can be achieved in the delivery of its contracts. It has been identified that [Procurement Policy Note \(PPN\) \(Taking Account of Social Value in the Award of Central Government Contracts\)](#) PPN02 applies to this procurement.

Using policy outcomes aligned with Government's priorities, a weighting of **10%** of the overall score for this requirement is dedicated to social value criteria.

6.3 Modern Slavery Considerations

- **6.3.1 Modern Slavery Assessment Tool (MSAT)**

As part of an initial assessment of the risk of modern slavery, the Buyer has identified this requirement as Low risk. The Buyer may re-assess the risk during the period of the contract, depending on circumstances (e.g. contract variation, change of subcontractor or audit etc.). If a re-assessment results in a High or Medium risk of modern slavery, at any point during the contract, the successful tenderer will be required to complete the Modern Slavery Assessment Tool (MSAT) as outlined below.

The MSAT is a modern slavery risk identification and management tool. This tool has been designed to help public sector organisations work in partnership with suppliers to improve protections and reduce the risk of exploitation of workers in their supply chains. It also aims to help public sector organisations understand where there may be risks of modern slavery in the supply chains of Goods/Services they have procured.

Where the risk of modern slavery is assessed as High or Medium risk the successful tenderer, as part of the contract, may be requested to complete the MSAT and, where appropriate, work with the Buyer in resolving any issues identified. Suppliers who have previously completed the MSAT for another Government body may share their results with the Buyer.

When applicable, the requirement to complete and assess the MSAT at appropriate intervals throughout the lifecycle of the contract may also form part of the Contract Management process.

In addition to completing the MSAT, and depending on the outcome of this assessment, it may be necessary for the Buyer to work with the successful supplier to undertake a supply chain mapping exercise to have a more informed position of any modern slavery risks within the wider supply chain beyond first tier/prime supplier. Such an exercise may also cover wider compliance with all relevant social, ethical and legal requirements of first tier/prime Suppliers and their supply chain.

For further information on the MSAT and registration process, please visit:
<https://supplierregistration.cabinetoffice.gov.uk/msat>

7. Quality Assurance Requirements

Not Applicable.

8. Other Requirements

8.1 Information Assurance and Governance

IAG Security Schedule

Where the supplier processes Government data, including but not limited to, personal data on behalf of the DVLA the following requirements shall apply, unless otherwise specified or agreed in writing.

Use of Artificial Intelligence for delivery of the requirement

The Buyer wishes to understand and approve any proposed use of any Artificial Intelligence (AI) tools/solutions or machine learning technologies to carry out activities in delivery of this contract.

Suppliers must state any plans to use such tools/solutions in their proposals and describe in detail how they will be integrated into your service offerings and used in the delivery of the contract.

Any proposed AI tools/solutions or extensive processing of data would need to be discussed and agreed with the Buyer before delivery as part of the contracted work so that the department can carry out the necessary impact assessments to ensure that the proposal is compliant with relevant laws and government policy.

If the supplier has no plans to use AI tools/solutions/technologies in the delivery of the contract they should state so in their proposal.

Should the successful Supplier wish to introduce AI tools/solutions at any point throughout the life of the contract, then a proposal should be submitted to the Buyer's Contract Manager who will consider the proposal and either confirm or decline the usage of AI tools/solutions.

Certification

The supplier shall ensure they hold relevant certifications in the protection of personal data and/or evidencing the effectiveness of technical and organisational measures they have in place. These certifications must be maintained throughout the entirety of the contract, including any applicable extension periods. Evidence of valid certificates and corresponding documentation shall be provided upon request by the DVLA's representative or an agent acting on DVLA's behalf.

Supplier Devices

- **Removable Media**

The supplier shall not use removable media in the delivery of this contract without the prior written consent of the DVLA.

Governance

- **Organisational Structure**

The supplier shall have a senior individual responsible for DVLA assets within your custody.

- **Asset Management**

The supplier shall implement and maintain an asset register that identifies and records the value of sensitive DVLA assets which require protection. This includes both physical and information assets. Risk assessments should be managed to ensure that the security of the asset is proportionate to the risk depending on value and sensitivity.

- **Policies**

The supplier shall establish, or indicate that they have in place, policies which detail how DVLA assets should be processed, handled, copied, stored, transmitted, destroyed and/or returned. These shall be regularly maintained. The supplier shall provide evidence of relevant policies upon request.

- **Risk Assessment**

- **Technical**

The supplier shall perform a technical information risk assessment on the service/s supplied and be able to demonstrate what controls are in place to address any identified risks.

- **Security**

The supplier shall ensure an annual security risk assessment is performed at any sites used to process or store any DVLA data. This assessment must include perimeter security, access controls, manned guarding, incoming mail and delivery screening, secure areas and/or cabinets for the storage of sensitive assets, and have a demonstrable regime in place for testing controls against operational requirements.

- **Return of Data / Information to DVLA**

The supplier must be able to demonstrate they can supply a copy of all data or information on request or at termination of the service.

- **Destruction / Deletion of Data or Information**

The supplier must be able to securely erase or destroy all DVLA-related data or information that it has been stored and processed for the service, upon DVLA request.

- **Incident Management**

The supplier shall have policies in place which set out how information security incidents, and personal data breaches or data loss events (including breaches to the confidentiality, integrity, availability, and resilience of data) should be managed and who it should be escalated to, including notifying the DVLA immediately, or in any case within 24 hours, of becoming aware of the incident/s and/or breach/es.

This policy shall also include:

- a) individual responsibilities for identifying and reporting security incidents and information security breaches;
- b) a reporting matrix including escalation points;
- c) an up to date list of relevant internal and external contact points; and
- d) a timeline detailing at which point the policy should be implemented.

Personal Data

- **Processing Personal Data**

The supplier as part of the contract agrees to comply with all applicable UK law relating to the processing of personal data and privacy, including but not limited to the UK GDPR and the Data Protection Act 2018, and the EU GDPR where applicable to the processing.

- **DVLA Written Processing Instructions**

The supplier shall comply with DVLA's written instructions, as outlined **Joint Schedule 11 (Processing Data) Annex 1 Processing Personal Data**.

- **International Transfers (Offshoring) of Government Data**

When international transfers or offshoring is described, the focus is typically on the physical location where data is hosted (such as where the data centres are located).

However, whilst physical location of data is a critical part of the offshoring question, it is important to understand how and where data might be logically accessed. Administrators or technical support staff may be located anywhere in the world, with logical access to data.

The supplier (and any of its third party sub-contractors, sub-processors or suppliers) shall not, transfer, store, process, access or view DVLA data outside of the UK without the prior written approval of DVLA, which may be subject to conditions. Any changes to offshoring arrangements must also be approved by DVLA.

Any request to offshore DVLA data must receive formal approval from DVLA prior to the commencement of any data processing activity. This is requested through the completion of DVLA's offshoring questionnaire (**Appendix D**).

In the event that the supplier proposes to offshore any DVLA data as part of the contract, they would be required to provide details in the offshoring questionnaire about the processing to be carried out offshore, including:

- a) the privacy risks and the security controls in place to protect the data;
- b) how the offshoring arrangement is legitimised to comply with relevant data protection legislation (e.g. adequacy decision, appropriate safeguards, Standard Contractual Clauses/International Data Transfer Agreements); and
- c) where applicable details of any transfer risk assessment that has been conducted, along with any supplementary measures implemented.

Processing of Sensitive Information (not Personal Data)

- **Security Classification of Information**

If the provision of the services requires the supplier to process DVLA data which is classified as OFFICIAL:SENSITIVE or higher, the supplier shall implement such additional measures as agreed with the DVLA in order to enhance the safeguarding of such information. A copy of the Government Security Classification scheme can be found at: <https://www.gov.uk/government/publications/government-security-classifications>

Personnel

- **Security Clearance**

- **Level 1**

The supplier is required to acknowledge in their response that any supplier staff that will have access to the DVLA site for meetings and similar (but have no access to the DVLA systems), must be supervised at all times by DVLA staff.

- **Level 2**

The supplier is required to confirm that Baseline Personnel Security Standard clearance (BPSS) is held for any supplier staff that will have:

- access to or will process DVLA (customer or staff) data or information
 - access to the DVLA site to provide routine maintenance
 - access to the DVLA site and/or DVLA systems

The aim of the BPSS verification process is to provide an appropriate level of assurance as to the trustworthiness, integrity and proper reliability of prospective staff.

The BPSS comprises verification of the following four main elements:

1. Identity;
2. Employment History (past 3 years);
3. Right to Work (RTW) in the UK;
4. Criminal Record Check (unspent convictions only).

BPSS is a series of checks conducted once a provisional offer of employment is accepted by individuals. A formal offer shall only be made once BPSS is passed. BPSS is not a [national security vetting \(NSV\) clearance](#). It applies to all individuals working within and for the government, such as civil servants, contractors, members of the armed forces, temporary staff and suppliers.

The supplier is required to provide evidence that the relevant BPSS checks (as listed above) have been undertaken.

- **Employment Contracts**

The supplier shall confirm that organisational and individual responsibilities for information security are clearly defined in the terms and conditions of employment contracts, along with relevant non-disclosure agreements, where the individual with have access to any DVLA data, information and /or the DVLA site or systems.

- **Training**

The supplier shall maintain a mechanism to ensure employees and contractors receive appropriate information security awareness and data protection training upon appointment, and perform regular updates to organisational policies and procedures, as relevant for each job function. Evidence must be provided where reasonably requested by DVLA.

- **Access Rights**

The supplier shall ensure their staff are provided only the necessary level of access (using the principle of least privilege) to DVLA data or information, to deliver their job function within the contracted service(s).

Upon staff migration, or termination of employment, the supplier shall verify that there is a process in place to ensure assets are returned and rights to assets revoked without undue delay.

Evidence of the above must be provided where reasonably requested by DVLA.

Business Continuity and Disaster Recovery

The supplier shall have business continuity and disaster recovery plans in place to maintain or quickly resume any services provided to DVLA and shall maintain compliance with relevant legislation.

8.2 Cyber Security

The Government has developed Cyber Essentials, in consultation with industry, to mitigate the risk from common internet-based threats.

It will be mandatory for new Central Government contracts, which feature characteristics involving the handling of personal data and ICT systems designed to store or process data at the OFFICIAL level of the Government Security Classifications scheme (link below), to comply with Cyber Essentials.

<https://www.gov.uk/government/publications/government-security-classifications>

All potential tenderers for Central Government contracts, featuring the above characteristics, should make themselves aware of Cyber Essentials and the requirements for the appropriate level of certification. The link below to the Gov.uk website provides further information:

<https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>

As this requirement features the above characteristics, you are required to demonstrate in your response that:

- Your organisation has Cyber Essentials certification; **or**
- Your organisation will be able to secure Cyber Essentials certification prior to commencement of the required services/deliverables; **or**
- Your organisation has other evidence to support that you have appropriate technical and organisational measures to mitigate the risk from common internet-based threats in respect to the following five technical areas:
 - Boundary firewalls and internet gateways
 - Secure configuration
 - Access control
 - Malware protection
 - Security update management

The successful tenderer will be required to provide evidence of Cyber Essentials certification 'or equivalent' (i.e. demonstrate they meet the five technical areas the Cyber Essentials Scheme covers) at the point of contract award, and prior to personal data being sent to the Supplier for processing.

The Supplier will be required to secure and provide evidence of Cyber Essentials certification 'or equivalent' (i.e. demonstrate they meet the five technical areas) on an annual basis.

Further information regarding the certification process can be found here:

<https://www.ncsc.gov.uk/cyberessentials/overview>

8.3 Sustainability

The Buyer is committed to reducing any negative impacts produced by our activities, products and services. This aligns to the Government's Greening Commitment which

states we must: “Continue to buy more sustainable and efficient products and services with the aim of achieving the best long-term, overall value for money for society.”

The Buyer is certified to ISO 14001:2015 and more information is available in our Environmental Policy at:

<https://www.gov.uk/government/publications/dvlas-environmental-policy>

8.4 Health and Safety

The Buyer has an Occupational Health and Safety Management System that is certificated to ISO45001. Further information on our Health & Safety Policy, is available on request from the Buyer.

8.5 Diversity and Inclusion

The Public Sector Equality Duty (PSED) is a legal requirement under the Equality Act 2010. The Equality Duty ensures that all public bodies play their part in making society fairer by tackling discrimination and providing equality of opportunity for all. It ensures that public bodies consider the needs of all individuals in their day-to-day work – in shaping policy, in delivering services, and in relation to their own employees. The Buyer is committed to encouraging equality, diversity and inclusion within our workforce and against unlawful discrimination of employees, customers and the public. We promote dignity and respect for all and will not tolerate bullying, harassment or discrimination by staff, customers or partners we work with. Everyone working for us and with us, as partners in delivering our services, has a personal responsibility for implementing and promoting these policy principles in their day-to-day transactions with customers and our staff.

A full copy of our Equality, Diversity and Inclusion Policy is available on request from the Buyer.

8.6 Business Continuity

The Supplier shall have business continuity and disaster recovery plans in place to maintain or quickly resume any Goods/Services provided to the Buyer and shall maintain compliance with relevant legislation.

8.7 Procurement Fraud

The DVLA adopts a zero-tolerance approach to procurement fraud and bribery. Please read the DfT Counter Fraud, Bribery, Corruption and Ethical Procurement Statement in **Appendix B**.

8.8 Use of Buyer Brands, Logos and Trademarks

The Buyer does not grant the successful Supplier licence to use any of the Buyer's brands, logos or trademarks except for use in communications or official contract

documentation, which is exchanged between the Buyer and the successful Supplier as part of their fulfilment of the Contract.

Approval for any further specific use of the Buyer's brands, logos or trademarks must be requested and obtained in writing from the Buyer.

9. Management and Contract Administration

Invoicing Procedures

DVLA invoicing procedures are detailed in **Appendix C**. Invoice payments will be annually in advance

Subcontracting to Small and Medium Enterprises (SMEs):

The Buyer is committed to removing barriers to SME participation in its contracts, and would like to also actively encourage its larger Suppliers to make their subcontracts accessible to smaller companies and implement SME-friendly policies in their supply-chains (see the Gov.Uk [website](#) for further information).

If you tell us you are likely to subcontract to SMEs, and are awarded this contract, we may send you a short questionnaire asking for further information. This data will help us contribute towards Government targets on the use of SMEs. We may also publish success stories and examples of good practice.

10. Documentation

Pricing Schedule Appendix A

Suppliers **must** complete **Appendix A – Pricing Schedule** to provide a full and transparent breakdown of costs associated with this contract.

11. Arrangement for End of Contract

The Supplier shall fully cooperate with the DVLA to ensure a fair and transparent re-tendering process for this contract. This may require the Supplier to demonstrate separation between teams occupied on the existing Contract and those involved in tendering for the replacement contract to prevent actual (or perceived) conflicts of interest arising.

12. Response Evaluation

The evaluation will comprise of the following elements:

- 1) an evaluation of mandatory requirements. These will be assessed on a pass/fail basis. Responses that fail any of the mandatory requirements may be disqualified from further consideration
- 2) an evaluation of the response based on the social value criteria
- 3) an evaluation of the prices submitted

Your response will be evaluated using the weightings **and** criteria weightings set out in Annex 1.

Selection will be based on the evaluation criteria, which demonstrates a high degree of overall value for money, competence, credibility and ability to deliver.

Your response will be evaluated using the following weightings **and** the criteria weightings set out at Annex 1, to obtain the optimal balance of quality and cost.

Mandatory Requirements

Annex 1 provides details of any elements/criteria considered as critical to the requirement. These are criteria, which will be evaluated on a pass/fail basis. A fail may result in the response being excluded from further evaluation.

Social Value Criteria Scoring Methodology

The scoring methodology used to assess and allocate scores to each criteria are included in the table below.

Points awarded	Description
100	Fully meets/evidence provided that demonstrates the requirement can be met
60	Minor concerns/issues that the requirement can be met
30	Major concerns/issues that the requirement can be met
0	Does not meet the requirement, not addressed or no evidence provided

Based on the allocated score, a percentage will be calculated against each element using on the following calculation:

$$\frac{\text{(Allocated Score)}}{\text{Maximum Score}} \times \text{Weighting}$$

For example, “Social Value Element 1” can be allocated a score between 0 and 100 but carries a weighting of 10%. Supplier A is given a score of 60 for this element so receives a score of $(60/100 \times 10) = 6\%$. The scores for each element will then be added together to calculate the overall social value criteria score.

Financial / Price Criteria

Evaluation of the prices submitted will be performed separately by a Commercial Finance Accountant and details will not be made available to the Quality Evaluation Panel. This is to ensure fairness and avoid any subconscious influence of a lower price on the quality scoring. The overall percentage weighting allocated for the Financial/Price Criteria is outlined in the table “Overall Weighting Allocation”.

Financial / Price Criteria Scoring Methodology:

A Percentage Scoring Methodology will be used to evaluate all proposals for this requirement. This methodology is based on the following principles:
The lowest quoted price will be awarded the maximum score available. Each subsequent responses will be baselined to this score and will be awarded a percentage of the maximum score available. The calculation used is as follows:

$$\frac{(\text{Lowest Quoted Price})}{\text{Price Quoted per Supplier}} \times \text{Maximum Score Available (i.e. Weighting)}$$

For example, if the Financial/Price weighting allocation is 40%, the maximum score available is 40. Supplier A submits the lowest price of £100,000 and Supplier B submits a price of £180,000. Based on the above calculation Supplier A and B will receive the scores shown below:

Supplier A = $100\text{k}/100\text{k} \times 40 = 40\%$

Supplier B = $100\text{k}/180\text{k} \times 40 = 22.22\%$

Overall Weighting Allocation

Evaluation Criteria	Weighting
Quality Criteria and Social Value Criteria (if applicable)	10%
Financial / Price Criteria	90%
Total	100%

Calculation of Overall Score:

The allocated score for the quality and Social Value criteria (where applicable) will be added to the Financial/Price Factor score to calculate the overall score for each tender (out of a max available 100%). The tender with the highest overall score will be deemed as successful.

Annex 1

Evaluation Criteria

Mandatory Criteria

Mandatory Criteria	Mandatory Criteria Description	Pass/Fail
Framework Core Terms and Schedules	<p>The Crown Commercial Service (CCS) Public Sector Contract and it's associated Core Terms and Schedules will apply to any resultant contract awarded under this Invitation to Tender. Bidders are asked to review the Core Terms in addition to the Call Off and Joint Schedules identified as being applicable to this tender process. These are referenced in the draft Call Off Order Form (Schedule 6).</p> <p>The successful bidder will be expected to contract on the basis of the above terms. Therefore, with the exception of populating the highlighted areas in the published Call Off and Joint Schedules, the Authority will not accept any amendments, revisions, or additions to these schedules.</p> <p>Bidders who are unable to contract on the terms as drafted will deemed non-compliant and their bid will be rejected.</p> <p>Please provide a YES/NO response to this question</p>	

Scored Social Value Criteria

Primary Scored Criteria	Primary Scored Criteria Weighting (%)
Describe your organisation's contributions to support environmental protection and improvement. This may include net zero greenhouse gas emissions, energy efficiency, waste management etc.	10%
	Total = 100%

Financial/Pricing Criteria

Primary Financial/Pricing Criteria	Financial/Pricing Weighting (%)	Description
Pricing Requirements	90%	Refer to the Appendix A Pricing Schedule
	Total = 90%	