CONTENTS

[1. PURPOSE 3](#_Toc486317023)

[2. BACKGROUND TO THE CONTRACTING aUTHORITY 3](#_Toc486317024)

[3. Background to requirement/OVERVIEW of requirement 3](#_Toc486317025)

[4. definitions 4](#_Toc486317026)

[5. scope of requirement 4](#_Toc486317027)

[6. The requirement 5](#_Toc486317028)

[7. key milestones 6](#_Toc486317029)

[8. authority’s responsibilities 6](#_Toc486317030)

[9. reporting 6](#_Toc486317031)

[10. volumes 6](#_Toc486317032)

[11. continuous improvement 7](#_Toc486317033)

[12. Sustainability 7](#_Toc486317034)

[13. quality 7](#_Toc486317035)

[14. PRICE 7](#_Toc486317036)

[15. STAFF AND CUSTOMER SERVICE 7](#_Toc486317037)

[16. service levels and performance 7](#_Toc486317038)

[17. Security requirements 8](#_Toc486317039)

[18. payment 9](#_Toc486317040)

[19. additional information 9](#_Toc486317041)

[20. Location 9](#_Toc486317042)

#

# PURPOSE

## The purpose of this study is to aid the Department for Transport understanding of the processes and decision making triggers for how software updates are managed in industries where there is a need to maintain the safety case/approval of the items that are updated.

## The report will then be used within the Department to inform policy development in this field.

# BACKGROUND TO THE CONTRACTING aUTHORITY

## The Department for Transport (DfT) is the lead Government Department for cyber security in the transport domain.

## Within the automotive sector the DfT are the lead Government Department. This includes the regulation of vehicles and assuring the type approval of vehicle components and systems.

# Background to requirement/OVERVIEW of requirement

## Vehicles and their safety functions normally have a safety certification, called type approval. This will have been obtained during the development of the vehicle and maintained for all systems or vehicles of that type (hence type approval). Traditionally type approvals do not need to be re-visited once awarded and will last for the lifetime of a system or its parent vehicle. The main exception to this is when a vehicle is recalled because a component has subsequently been found to be faulty. Current systems requiring type approval are defined by the United Nations Economic Commission for Europe (UNECE) (<http://www.unece.org/trans/main/wp29/presentation_regulations.html>).

## Most vehicle systems now include both hardware and software. It is possible that the software may be updated throughout a systems lifetime for a number of reasons. This may include performing security updates, changing the functionality, improving the performance or addressing software flaws. When software is updated it is possible that the updates may knowingly, or otherwise, affect safety critical parameters. This in turn may mean that the type approval of that system, and hence the vehicle, may be affected.

## With in-service updates there is a need to address how these updates are permitted with regards how any changes to the software may affect safety certification (type approval) and how any certification may be re-assessed. This is particularly pertinent when the hardware components are no longer in production.

## The automotive sector is not alone in facing this challenge. There are parallel industries, such as medicine, mining, oil, aviation, space, rail and more where safety approvals are provided for systems that comprise both hardware and software and where the software may be updated for components in the field. Relevant practices in other sectors, such as benchmarking updates in the mobile phone space, should also be considered.

## The project is to look at how this situation is addressed in other industries. It should review existing practices elsewhere and consider how applicable they may be to the automotive industry. It should also compare these with any existing practices or recommendations for the automotive industry (for example within the ISO 26262 series). This may include a review of academic, industry and legal reports, literature and standards. Within this it should describe the underpinning rationale for the decisions and processes identified and appraise whether the rationale would apply to the automotive industry.

# definitions

|  |  |
| --- | --- |
| Expression or Acronym | Definition |
| DfT | Department for Transport |
| UNECE | United Nations Economic Commission for Europe |

## The term ‘automotive industry’ is used within this document. The term is intended to be broad and cover many participants in the automotive sector. It will comprise existing and potential vehicle manufacturers (not just car manufacturers), their tier 1 and tier 2 automotive suppliers, insurance providers, subject matter experts and others integrally involved in the world of vehicles. The term is also intended to cover both light vehicles, such as cars and van, through to heavy vehicles, such as buses and heavy goods vehicles.

# scope of requirement

## The project should focus on software updates to equipment in the field, rather than updates to software before the component or system leaves a factory.

## The project shall include a review of legislative requirements, recommended practices academic papers and other relevant material. It can also include interviews with subject matter experts.

## The focus of the review shall be how the safety approval of an update is retained or re-applied within the update process. The actual process by which a vehicle is updated (be it physically or over the air) and the security of that process is secondary and should only be included in the findings where either forms part of the safety approval process.

## The project should not be limited to the industries identified above, as there may be other relevant industries not identified. The scope should look to include any other potentially relevant industry that would support the desired outcomes.

## The work will not aim to produce a government policy paper but to provide a report which could be used in the formation of such a paper.

# The requirement

## The Supplier shall deliver a report describing how parallel industries maintain safety cases (or equivalent certifications) for software updates that are provided to systems in the field, particularly with respect to the processes, requirements and evidence needed for the update approval in safety conscious industries. Within this the Supplier shall:

### Identify technical, physical or other measures that are used to evidence that safety requirements are met or maintained for a software update.

### Identify the processes and steps other industries use to manage how software updates are approved for use. This should include processes to approve the release of an update and processes used for assurance purposes. Assurance will include procedures to ensure that only approved software is used in the field and version control / audit traceability procedures and requirements.

### Identify how other industries differentiate between updates to safety critical and non-safety critical functions or systems and any procedures or evidence used to support such decisions.

### Identify the rationale behind the processes, measures and practices identified.

### Identify the bodies that are involved in the approval process and their roles.

### Identify how compliance with the requirements is verified.

### Compare how the practices and requirements differ between different industries and if possible identify why.

## Where a recommendation is made or a practice identified, the source should be quoted.

## The report shall assess how suitable the processes and practices identified might be applied to the automotive industry and any gaps or additional considerations that might be needed. This should include an assessment of the likely impact on industry in terms of cost and time.

## The report should consider the different bodies that might be involved in any software approval process and whether such a structure could be applied to the automotive industry.

## The report shall provide:

### A summary providing a high level overview of the findings and recommendations.

### A section describing the practices of other industries.

### A section describing how applicable the measures identified may be to the automotive sector, this shall include any recommendations on what could be most easily implemented.

### The report shall further highlight any gaps in what they have found and areas potentially requiring further work.

## A draft report shall be provided ahead of the project finish to the customer. This will allow the customer to provide feedback for the final report. The final report shall be accompanied by an oral presentation of the key findings of the review. This shall be conducted at DfT premises.

# key milestones

## The Potential Provider should note the following project milestones that the Authority will measure the quality of delivery against:

|  |  |  |
| --- | --- | --- |
| **Milestone** | **Description** | **Timeframe** |
| 1 | Inception meeting to clarify project deliverables and plan, above that provided in bid documentation.  | Will complete within the first week of launch of event.  |
| 2 | Draft report covering progress to date | Will complete by week 6 of contract |
| 3  | Final report delivery and presentation  | Will complete by the final week (week 8) of the contract |

#

## The Supplier shall perform its obligations so as to achieve each Milestone by the Milestone Date.

## Changes to the Milestones shall only be made in accordance with the variation procedure and provided that the Supplier shall not attempt to postpone any of the Milestones using the variation procedure or otherwise (except in the event of a Customer default which affects the Supplier’s ability to achieve a Milestone by the relevant Milestone Date).

# authority’s responsibilities

## DfT will need to ensure that sign-off and comments on the final report is provided as per the agreed timetable.

# reporting

## Please refer to the Suppliers’ key reporting responsibilities as mentioned in 7.1 and 7.2.

# volumes

## N/A

# continuous improvement

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

# Sustainability

## N/A

# quality

## The Potential Provider shall ensure they provide a product that is of a high quality and meets the needs of the requirements as described by the Authority in section six (6), both in terms of the information it provides and in the manner that the information is provided.

# PRICE

## The Potential Provider shall provide a capped cost price for this work. The maximum allocated budget for the contract is £60,000.00 excl. VAT. Bids submitted which are above this value will not be considered.

## Prices are to be submitted via the e-Sourcing Suite, Appendix E excluding VAT. Prices should not appear anywhere else in the bid documentation.

# STAFF AND CUSTOMER SERVICE

## The Authority requires the Potential Provider to provide a sufficient level of resource throughout the duration of Contract in order to consistently deliver a quality service to all Parties.

## Potential Provider’s staff assigned to Contract shall demonstrate relevant qualifications and experience in the field and how they will use this to deliver the Contract.

## The Potential Provider shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

# service levels and performance

## The Authority will measure the quality of the Supplier’s delivery through assessment of their progress alongside the agreed milestones set out in paragraph 7.1:

|  |  |  |  |
| --- | --- | --- | --- |
| KPI/SLA | Service Area | KPI/SLA description | Target |
| #1  | Progress Report  | Progress reports will be supplied to the DfT project manager by phone or email (to be confirmed). This will include a summary of progress against the delivery.  | Fortnightly |
| #2  | Risk monitoring  | The Supplier will raise any concerns about the possibility of failing to meet the overall deadline and lack of relevant information to meet the requirements. Key risks to be monitored should be identified and tracked to ensure the project delivers. | Within 24 hours |
| #3  | Communication  | The Supplier shall acknowledge any communications from the contract/project manager within 48 hours  | Within 48 hours  |
| #4  | Emergencies  | If there is an urgent issue, the Supplier shall make the contact with the project manager within 48 hours.  | Within 48 hours |

## In the event that the Provider is unable to meet a project milestone to the agreed specification and time the Authorities reserves the right to retain payment, either in whole or in part, until a satisfactory resolution has been achieved.

# Security requirements

## The Potential Provider must be able to handle and store classified material up to OFFICIAL level. The project report will be classified at OFFICIAL.

## The Potential Provider should demonstrate the measures in place to keep this information secure. Specifically, in the bid document the Potential Provider should provide detail on how they will meet the following requirements:

* The Supplier must ensure the security of the information in transit.
* Any electronic files should be stored on an IT system that has access controls that only allow approved personnel with a genuine ‘need to know’ to access them to read and copy. The IT system should be protected by an appropriate firewall.
* Once electronic files are no longer needed they should be deleted from the IT system in a way that makes recovery unlikely, either by overwriting the storage space or eventual dilution and deterioration on a busy shared storage system.
* Any electronic files or data should be stored within the UK.
* Paper copies (including drafts and notes) and any removable electronic storage must be locked away when not in use to prevent unauthorised access. Printed material should be marked OFFICIAL.
* Paper and printed material should be shredded when no longer needed.
* Access to all material generated by this project (not included source data unless supplied by DfT) must be on a limited and controlled basis, by persons notified to and approved by the DfT.
* The supplier should have or be seeking to have Cyber Essentials certification.

## Any personal information obtained under this contract must be controlled in compliance with the Data Protection Act.

## Further information on security classification is available on the Cabinet Office website at the following addresses:

* <http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-personnel-security-controls.pdf>

## <https://www.gov.uk/government/publications/security-policy-framework>

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

# payment

## Prices should be submitted in pounds sterling and be inclusive of expenses and exclusive of VAT.

## Invoices to be submitted to DfT on completion of each agreed milestone.

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

# additional information

## The Authority shall pay the Supplier within Thirty (30) calendar days of receipt of a valid invoice, paid against a valid Purchase Order issued by the Authority; the method of payment will be by BACS.

## The contractor shall agree not to publicise their involvement in this work without the express authorisation of the Department for Transport.

# Location

## The location of the Services will be carried out at the Suppliers premises. The base location will be Department for Transport offices in London. The Supplier shall travel to DfT premises, London for a maximum of 3 meetings. Travel to any other locations will only be permitted with prior permission of the authority and will be at Department for Transport T&S rates.