Specification for Incursion Alarm Warning and supporting systems.

INTRODUCTION

National Highways has a legal and moral obligation to meets its duty of care requirements to its workers, protecting employees from injury and harm across the entire network. Consequently we are looking for a Service Provider who can provide an Emergency Traffic Management Incursion Warning Radar System (ETMRS) that is an automated system and detects threats to Traffic Officers (TO) when they are undertaking their duties on the Strategic Road Network (SRN) within their Chapter 8 compliant Emergency Traffic Management (ETM).

A system that is designed to improve the safety of our workforce and reduce the likelihood of a fatal incident by providing a 'watchperson' function alerting Traffic Officer's a potential or actual strike into ETM or hard shoulder.

Previous trials have taken place and National Highways requires a Service Provider for the further development to finesse a prototype system based upon findings and feedback from on-road trials, in the form of firmware, software and hardware updates.

KEY OBJECTIVES

National Highways requires a Service Provider for the further development and production of a prototype ETMRS, the Service Provider is required to:

- Test and gather data on edge cases – this involves evaluating the devices' performance in challenging environments (e.g. tunnels) to ensure the device operates efficiently on all areas of the SRN;
- Gather data from 10 traffic officer vehicles from new trial regions, South-East and South-West, focusing on edge case environments (tunnels, toll plazas, areas of lack of infrastructure) and scenarios which need further research, i.e. low speed, poor driver behaviour and loss of control;
- Construct and ensure final product acceptance – this includes building a final version of the device and radar. The final device and radar will be built and verified to meet all safety and functionality requirements needed to be made compliant with UKCA marking, confirming it meets UK safety, health, and environmental standards.
- Additionally, the device, system, and processes will undergo pre-testing to prepare for ISO certification, ensuring compliance with international standards.
- Further development of the radar technology algorithm based upon above data gathering.
- Develop, produce and trial an updated version of a wearable device, incorporating feedback from previous trial phases and technical assessment.
- Provide ongoing project management support.

PRODUCTS AND SERVICES REQUIRED

The products and services of the successful Service Provider include:

- Development of a prototype radar;
- Development of a prototype user wearable alarm device;
- Live testing of equipment (vehicle & user) on the SRN (specifically in hard to access locations such as tunnels) to test signal strength and reliability;
- Provide enhancements to hardware units to update software, replace SIM cards and conduct operational stability testing
- Acquire data (from testing environment) to improve Incursion Radar System;
- Acquire user feedback (from Traffic Officers) to improve the development of prototypes to eventual 'final production stage' models;
- Use live data to develop and refine the required algorithm (to detect, predict vehicle movement and alert end-user via wearable device);
- Ensure compliance with cyber essentials as per Information Systems & Security requirements;
- Provision and access to technical experts and project manager for the duration of the contract;
- Regular meetings between National Highways and Service Provider to discuss project progress and findings;
- Production of a final evaluation report for National Highways.

SUCCESS CRITERIA

The service provider shall be responsible for the construction and final integration of the device and radar system, ensuring compliance with all specified safety and functional requirements. This includes verification processes in place to confirm that all defined success criteria are fully met.

Defined success criteria;

1. System Performance

1(a) False Negative Rate

- **Definition:** Situations where there is a significant danger of an incident, but no alarm was generated
- **Threshold:** ≤ 10% missed
- **Evidence:** Manual review of videos from the trial, and subsequent report

1(b) Nuisance Alarm Rate

- **Definition:** Situations where the alarm triggered without an identified and reasonable cause
- **Threshold:** ≤ 20% of total alarms

- **Evidence:** Manual review of videos from the trial, and subsequent report

2. Wearable Performance

2(a) Alarm Delivery Success Rate

- **Threshold:** ≥ 95% of alarms received at wearable within 1.0s, triggering both an audible and visual warning
- **Limitations:** Within a 500m range of the TOV, and for typical working scenarios of the TOS. Excludes laying face down on the ground, where wearable is completely shielded.
- **Evidence:** Off-highway test, and subsequent report

2(b) Wearable Operation

- **Operation:** Fully aligned with the supplied and agreed wearable v2 specification
- **Evidence:** Off-highway test, and subsequent report

3. Operational Availability

- **Threshold:** ≥ 95% uptime (excluding planned maintenance)
- **Limitations:** Any factors outside of the supplier's control including accidental damage
- **Evidence:** ≥ 90-day field trial

4. Integration & Interoperability

- **Chapter 8 ETM Compliance:** Verified during trials
- **Vehicle Compatibility:** Standard TOS vehicle types. BMW X5, Volvo XC90 and Tesla model X

5. Technical Specification documents

- **RRA600** system description and functional specification
- **Wearable** Alarm V2 specification
- RRA600's risk **algorithm specification**

LIVE TESTING AND EVALUATIONS

The Service Provider is required to set out in its evaluation plan how they will achieve the key objectives.

The Service Provider will:

- Work cooperatively with National Highways to ensure the efficient installation of base units into traffic officer vehicles prior to the start of the live testing trial;
- Provide knowledge sharing to traffic officers in the trial regions on the radar and wearable device;
- Produce an end of trial evaluation report than can support the full and final development of a working incursion alarm system, including a wearable device and its algorithm that provides safety critical information to National Highways.
- Identify any high risk alert scenarios and report to National Highways on weekly basis.

National Highways will

- Ensure that traffic officers are made available for the commencement of the live trial;
- Provide a location, to be agreed, for a knowledge sharing event;
- Ensure traffic officer vehicles are made available at the appropriate time and location;
- Collate any behavioural feedback and provide to the Service Provider at the end of the trial period and share with the Service Provider.

The evaluation report:

- Contains information at the level of detail necessary to manage the live testing period effectively.
- Takes account of all dependencies known to, or which should reasonably be known to, the Service Provider.
- The Service Provider keeps the evaluation plan under weekly review and updates on a regular basis.
- National Highways may instruct reasonable changes or provisions to ensure that milestones are met.

The Service Provider submits their evaluation report to National Highways within 20 working days of the end of trial period.

The Service Provider:

- Appoints an authorised representative who is responsible for the management of the contract and ensures the trial period is adequately resourced. Also the Service Provider appoints a representative who acts as a point of contact for National Highways.
- Manages and reports progress against the evaluation plan.
- Attends weekly or bi-weekly progress meetings, or as requested by National Highways.
- Ensures that all identified risks associated with the development period are minimised.
- Shall provide any additional support as necessary during the contract term, ensuring timely delivery within a reasonable timeframe.

ADDITIONAL CONDITIONS

Health and Safety

The Service Provider complies with and operates according to all relevant and prevailing health, safety and wellbeing legislation, considerations, guidance, industry best practice and National Highways requirements.

Information Systems & Security

This section sets out the requirements in respect of Information Systems that

- are developed, procured, provided and made available to National Highways by the Service Provider for the purposes of performing the information requirements under the contract,
- are developed, procured and provided by the Service Provider relating to its own corporate business and operations of performing the information requirements under the contract.

To the extent that the Service Provider is required to create or maintain any information under the contract in electronic format, the Service Provider ensures that, at all times

- a format is agreed with National Highways,
- information is maintained to allow fast and efficient electronic transfer of information to National Highways or Others
    - without additional costs National Highways or Others,
    - the need for complex, expensive procedures or processes and
    - in any event a format that complies with the specification for transfer,
- such information is backed up and copies are held in offsite storage in accordance with procedures agreed National Highways and it implements and complies with all procedures for information back-up and off-site storage referred to in this paragraph.

The Service Provider maintains all its Information Systems to enable its segregation from any other computer or electronic storage devices, systems, materials or information of the Service Provider and transfer to National Highways or an incoming Service Provider, efficiently and without additional expense or delay immediately on termination or expiry of the contract.

The Service Provider complies with the information management system (IMS) a platform outlining additional information for the processes of data and information requirements, which is available at https://nationalhighways.co.uk/ims.

A failure to comply with this section is treated as a substantial failure by the Service Provider to comply with its obligations under this agreement.

General security requirements

The Service Provider provides proof of compliance with the His Majesty's Government (HMG) Security Policy Framework (SPF) in respect of those Information Systems.

The Service Provider ensures that all persons who use National Highways Information Systems for or on behalf of the Service Provider comply with National Highways security requirements.

The Service Provider grants, or procures the grant of, licences required to allow National Highways to use the Information Systems developed, procured or otherwise provided by the Service Provider to the organisation.

The Service Provider implements IT and Information Security systems to protect the confidentiality, integrity, and availability of the information it handles, and have those systems independently audited. The Service Provider aligns these systems to meet requirement for the services provided.

A failure to comply with this section is treated as a substantial failure by the Service Provider to comply with its obligations under this agreement.

Information Security

Upon request the Service Provider prepares a robust information security plan complying with National Highways information security requirements and submits it to National Highways for acceptance. The Service Provider includes the security plan in its quality management system. The security plan complies with the requirements of ISO/IEC27001 and ISO/IEC27002 and includes procedures which

- ensure compliance with the Data Protection Legislation,
- protect information against accidental, unauthorised or unlawful processing, destruction, loss, damage or disclosure of Personal Data,
- ensure that unauthorised persons do not have access to Personal Data or to any equipment used to process Personal Data,
- protect IT systems from viruses and similar threats,
- provide for disaster recovery, and in particular ensure that the Personal Data is safely backed-up and
- provide for the vetting of its employees and sub-Service Providers' staff in accordance with National Highways staff vetting procedures.

The Service Provider does not use any confidential or proprietary information provided to or acquired by it for any purpose other than to provide the service. The Service Provider implements measures to prevent the disclosure of such information by its employees or sub-Service Providers.

On expiry of the contract, termination or if requested by National Highways, the Service Provider shall provide National Highways all Personal Data held by them in a format specified by National Highways (and destroys and procures any sub-Service Provider (at any stage of remoteness from National Highways) and any Sub-Processor destroys, any electronic and paper copies of such data in a secure manner.

Where the Service Provider obtains or collects Personal Data on behalf of National Highways, the Service Provider

- provides to Data Subjects a data protection notice in a form accepted by National Highways informing the Data Subject of the identity of National Highways, the identity of any data protection nominated lead it may have appointed, the purpose or purposes for which their Personal Data will be processed and any other information which is necessary having regard to the specific circumstances in which the Personal Data is, or is to be, processed to enable processing in respect of the Data Subject to be fair and
- where applicable, obtains all necessary consents for the processing of Personal Data.

The Service Provider complies with National Highways data handling policy when working on National Highway systems or handling National Highways data.

Prior to processing Personal Data on behalf of National Highways, the Service Provider submits a security plan to National Highways for acceptance that complies with the requirements of ISO/IEC27001 and ISO/IEC27002.

A system on which the Service Provider holds any National Highways data, including back-up data, is a secure system that complies with the security policy.

If National Highways minimum requirements for the Service Provider's data collection system are not met, the Service Provider is required to affect such modifications or enhancements to its own data collection system, or those of its supply chain, as are required, to meet National Highways requirements.

A system on which the Service Provider holds any Employer's data, including back-up data, is a secure system that complies with the security policy.

A failure to comply with this section is treated as a substantial failure by the Service Provider to comply with its obligations under this agreement.

Breech of security

Breach of security" is the occurrence of

- any unauthorised access to or use of the Information Systems, National Highways Premises, National Highways System (to the extent that it is under the control of the Service Provider) or any IT, information or data (including the confidential information and National Highways Data) used by National Highways or the Service Provider in connection with the contract and
- the loss (physical or otherwise), corruption, unauthorised disclosure of any information or data (including the confidential information and Employer Data), including any copies of such information or data, used by National Highways or the Service Provider in connection with the contract.

The Service Provider develops and maintain a Security Incident management and reporting policy in accordance with the Customer's 'Information Security Incident Management Requirements' and ISO27001. The Service Provider makes a full log of Security Incidents available to National Highways on request, and in any case on a quarterly basis. All Security Incidents defined as a Major Incident is reported to National Highways as soon as practicable (in any case within twenty four (24) hours of the *Service Provider* becoming aware of the Incident).

The Security Incident management process as a minimum, requires the Service Provider upon becoming aware of a breach of security or an attempted breach of security to

- immediately take all reasonable steps (which includes any action or changes reasonably required by National Highways which is completed within such timescales as National Highways may reasonably require) necessary to
    - minimise the extent of actual or potential harm caused by such breach of Security
    - remedy such breach of security to the extent possible and protect the integrity of the Information System against any such potential or future attempt of breach of security

- apply a tested mitigation against any such breach of Security or potential or attempted breach of security and, provided that reasonable testing has been undertaken by the *Service Provider*, if the mitigation adversely affects the *Service Provider* ability to deliver the Services so as to meet any Performance Indicator, the *Service Provider* is granted relief against the failure to meet such affected Performance Indicator for such period as National Highways, acting reasonably, may specify by written notice to the Service Provider; and
- prevent a further breach of security or attempted breach of security in the future exploiting the same root cause failure

as soon as reasonably practicable and, in any event, within 2 working days, following the breach of security or attempted breach of security, provide to National Highways full details of the breach of security or attempted breach of security, including a root cause analysis where required by National Highways.

In the event that any action is taken in response to a breach of security or attempted breach of security which occurred as a result of non-compliance of the information security management system (ISMS) outlined in ISO 27001 or the risk management with the Baseline Personnel Security standard outlined in the HMG SPF and the contract, then such action and any required change to the Information System or risk management is completed by the Service Provider.

A failure to comply with this section is treated as a substantial failure by the Service Provider to comply with its obligations under this agreement.

Cyber Essentials Scheme

National Highways and the Service Provider comply with the provisions of Cyber Essentials or Cyber Essentials + Scheme and holds a valid certificate confirming compliance for the entire duration of the contract.

Off-shoring of Data

In this section Risk Assessment is a full risk assessment and security review carried out by the Service Provider and submitted to National Highways in accordance with the HMG Security Policy Framework (SPF) and the "National Highways Information Security Policy".

The Service Provider does not engage in any Offshoring activity including storing data, providing services or solutions that is classified in the OFFICIAL tier or higher in accordance with the "HMG Government Security Classifications" and from 30th May 2024 Procurement Policy Note 7/23: Government Security Classifications Policy 2023.

The Service Provider does not

- keep any data offshore,
- allow in any way for data to be accessed from an offshore location,
- host National Highways project systems, services or information outside the UK,
- allow staff based outside the UK to have access to National Highways systems, services or information,

- develop system applications outside the UK or
- send diagnostic data to an organisation outside the UK as a result of break / fix activity

until the National Highways has confirmed to the Service Provider that

- National Highways has gained agreement for such action in accordance with the "NHPOL0079 Offshoring Policy" or
- such approval is not required.

The Service Provider ensures that no offshore premises are used in providing the services until

- such premises have passed a Risk Assessment or
- National Highways confirms to the Service Provider that no Risk Assessment is required

The Service Provider complies with a request from National Highways to provide any information required to allow National Highways to

- gain agreement for storing data or allowing access to data from an offshore location in accordance this section or
- conduct a Risk Assessment for any premises in accordance with this section.

The Service Provider ensures that any subcontract (at any stage of remoteness from National Highways) contains provisions to the same effect as this section.

A failure to comply with this section is treated as a substantial failure by the Service Provider to comply with its obligations under this agreement.

APPENDIX 1 – DATA PROTECTION

DATA PROTECTION (SCHEDULE [A])
Processing, Personal Data and Data Subjects
This schedule is completed by National Highways, who may take account of the view of the Service Provider, however the final decision as to the content of this schedule is National Highways and at its absolute discretion.
1. The contact details of National Highways' Data Protection Officer are obtainable from the Data Protection team available via dataprotectionadvice@highwaysengland.co.uk .
2. The contact details of the Service Provider Data Protection Officer or nominated lead are to be provided during the implementation period.
3. The Service Provider complies with any further instructions issued by National Highways with respect to the processing of Data.
Any such further instructions are to be incorporated into this table.

Description	Details
Identity of National Highways and Service Provider	The Parties acknowledge that for the purposes of the Data Protection Legislation, National Highways is the Data Controller and the Service Provider is the Processor in accordance with Data Protection in the specification of works.
Subject matter of the processing	The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide lone worker devices and phone application to National Highways.
Duration of the Processing	For the duration of the contract
Nature and purposes of the processing	The use of data for the purpose of provide the goods and services including storing of data to facilitate such processes. This includes structuring the data to facilitate efficient processes such as into geographical areas and maintaining the list of data to align with current employees.
Type of Personal Data	The types of personal data shall include: • Employee name • Employee gender

	• Employee work location(s) • Employee work email address and phone number • Employee personal address(es) (in rare and limited cases only)
	The following is classed as special category data and is especially sensitive: • Employee medical information
Categories of Data Subject	National Highways staff
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	All employee data shall be destroyed: • 3 months from the date of contract expiry or • once relevant data has been handed back to National Highways as part of any demobilisation process. Identifiable employee data shall be destroyed at regular intervals no more than 6 months from when the Service Provider is informed by National Highways. Any relevant data can continue to be held providing all identifiable information has been removed.

APPENDIX 2 – DEFINITIONS

REF.	DEFINED TERM	DEFINITION
1	Information Systems	Can be a combination of hardware, software, infrastructure and trained personnel organised to facilitate planning, control, coordination and decision making in an organisation.
2	Information Technology Infrastructure Library	A governance model for IT service management and best practices that defines an end-to-end life cycle and integrated set of practices and guidance in the areas of service strategy, service design, service transition, service operation, and continual service improvement.
3	Offshoring	Any arrangement where the performance of any part of the services or a solution under a contract may occur outside the UK for domestic (UK) consumption.
4	Security Incident	Is a breach of security that results, or may result in, leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data.

APPENDIX 3 - REFERENCE DOCUMENTS

REFERENCE	DOCUMENT TITLE	SOURCE
H&S	Health and safety policies, procedures, and guidance notes (generally)	http://www.highwayssafetyhub.com/ (general link to safety hub containing all our documents)
H&S	Home Safe and Well approach	https://assets.highwaysengland.co.uk/about-us/Home+Safe+and+Well+Strategy+2019.pdf
H&S	ISO45001:2018	https://www.iso.org/iso-45001-occupational-health-and-safety.html NB This is now cross referenced from the Quality Management section.
Information Security Offshoring	HMG Security Policy Framework (SPF)	https://www.gov.uk/government/publications/security-policy-framework .
Information Security	HMG Government Security Classifications	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1166697/Procurement_Policy_Note_-_Government_Security_Classifications_Policy.pdf
Information Security	HMG Government Security Classifications	Procurement Policy Note 7/23: Government Security Classifications Policy 2023
Information Security	Information management system	https://highwaysengland.co.uk/ims
Information Security	Public Records Act 1958	https://www.legislation.gov.uk/ukpga/Eliz2/6-7/51
Information Security	National Cyber Security Centre End user device (EUD) security guidance	https://www.ncsc.gov.uk/guidance/end-user-device-security
Information Systems	Commercial reporting and monitoring system	https://supplychainportal.highways.gov.uk/commperf/SitePages/Home.aspx
Information Systems and Security	National Cyber Security Centre End user device (EUD) security guidance	https://www.ncsc.gov.uk/guidance/end-user-device-security
Information Systems and Security	HMG Government Security Classifications	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file

		/715778/May-2018_Government-Security-Classifications-2.pdf
Information Systems and Security	Information Management System	https://highwaysengland.co.uk/ims.
Offshoring	HMG Government Security Classifications	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf
Offshoring of data	Statement of Highways England's IT Security Policy	