



One Box: Driver and Vehicle Data Management System Criteria

Publication No. 28/12

In association with



ACPO ITS Working Group
One Box Consortium



One Box

Driver and Vehicle Data Management System

Criteria

ACPO ITS Working Group
One Box Consortium

28/12

One Box

Driver and Vehicle Data Management System Criteria

Publication No. 28/12

1

ISBN: 978-1-78246-002-2

FIRST PUBLISHED SEPTEMBER 2012

© CROWN COPYRIGHT 2012

For information on copyright see: <http://www.opsi.gov.uk/advice/crown-copyright/copyright-guidance/>

Home Office Centre for Applied Science and Technology
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051

Fax: +44 (0)1727 816233

Email: cast@homeoffice.gsi.gov.uk

Website: <http://www.homeoffice.gov.uk/science-research/>

Foreword



The Emergency Services, along with other public sector organisations, are facing significant pressures to maintain core services with significantly reduced budgets. One way of achieving this is through efficiency savings on the purchase and use of all services, including vehicles, through standardisation and the use of technology. Traditionally, the Emergency Services operate a large number and range of vehicles. These are mostly normal production vehicles that have been retrofitted with a wide array of aftermarket equipment, according to their role.

This document outlines the standards relating to the Driver and Vehicle Data Management System (DVDMS), required by the Association of Chief Police Officers (ACPO) and the National Association of Police Fleet Managers (NAPFM), in relation to providing a data management system for vehicle and driver telematics. Its aim is to ensure commonality of approach to provision of telematics for the police, together with providing a management tool to underpin safe and efficient driving standards for organisations and staff. Furthermore, this approach is likely to deliver cost efficiencies across the police service as well improving driver behaviour and reducing collisions.

This work has been funded by the Home Office Centre for Applied Science and Technology (CAST). It was led by the ACPO Intelligent Transport Systems (ITS) Working Group that, with a large consortium including third-party suppliers, vehicle manufacturers and other Emergency Services, have developed these criteria, which will be assessed by one or more accredited test houses.

These criteria are a major step forward for the police service in producing a standardised telematics solution, which provides key management information to both managers and users which in turn leads to efficiency savings for the police service, with the ability to benchmark across forces in the future, thereby providing a platform for sharing best practice across forces.

The requirement to comply with the One Box Driver and Vehicle Data Management System (DVDMS) criteria will be included as part of the ACPO Fleet Procurement Technology Standardisation work for future police vehicle specification.

Suzette Davenport

Deputy Chief Constable
ACPO Lead for Roads Policing
Northamptonshire Police

Rob Coleman

Director
Home Office CAST

Management Summary

The aim of the One Box Driver and Vehicle Data Management System (DVDMS) criteria is to facilitate the development and installation of an effective, safe, proactive telematics system to positively influence driver behaviour with the aim of improving safety and saving money.

This document sets out the standards that DVDMS-compliant systems must meet in order to be approved. This includes the functionality that will be required in all DVDM Systems to be Listed¹ as compliant. It includes details of tests that equipment or systems will be subjected to.

The DVDMS criteria document is owned and maintained by the Home Office Centre for Applied Science and Technology (CAST). The criteria will be managed operationally by CAST, who will also manage the Compliance Testing of submitted systems against the criteria.

A periodically updated List of approved equipment, systems and components will be maintained by CAST.

These criteria will be subject to review in order to keep pace with technological developments in the field of DVDMS equipment or systems.

Operational Relevance

DVDMs meeting the criteria laid out in this document are likely to improve safety, as well as providing cashable efficiency savings for the Emergency Services.

It will support reductions in fuel consumption and servicing costs by logging and reporting detailed usage information on both vehicles and drivers. This will provide information to encourage drivers to improve and to support management interventions.

Anticipated changes in driver behaviour are expected to lead to reductions in the number and cost of collisions and associated third party costs.

Conclusions and Recommendations

It is recommended, when choosing fleet management or event data recording systems, that emergency service fleet managers and procurement personnel should procure systems that comply with these criteria. Only then will realisation of the benefits on offer be maximised.

¹ 'Listed' is capitalised where it refers specifically to inclusion of a system, a component or a device in the List of those that have been approved by the Home Office Centre for Applied Science and Technology (CAST)

Contents

1	One Box Driver and Vehicle Management System (DVDMS) Concept.....	1
1.1	Introduction.....	1
1.2	Objective of DVDMS	2
1.3	Effective and Fair Supervision	4
1.4	DVDMS Criteria.....	5
2	General Requirements	7
2.1	Introduction.....	7
2.2	Coverage.....	7
2.3	Bundled Services	7
2.4	Upgradeable and Reusable	8
2.5	Open Standards	8
2.6	Quality Assurance	8
2.7	National Procedures for Operation of DVDMS	8
2.8	Audit	9
2.9	Human-Machine Interface within the DVDMS	10
2.10	Legislative Requirements.....	10
3	In-Vehicle Components and Use Requirements.....	13
3.1	General.....	13
3.2	Controls	13
3.3	One Box esCAN	13
3.4	One Box DVDMS Operation	14
3.4.1	Safety and Reliability	15
3.4.2	User Cannot Deactivate.....	15
3.5	In-Vehicle Device	16
3.5.1	Device Dimensions	16
3.5.2	DVDMS Marking	16
3.5.3	Device and System Security	16
3.5.4	DVDMS Operating Conditions	17
3.5.5	Compatibility with Vehicle and Emergency Service or Other Specialist On-Board Equipment.....	17
3.5.6	Electrical Requirements	18
3.5.7	Electrical Backup	18
3.5.8	Standalone Power Supply.....	19
3.5.9	Power Feedback	19
3.5.10	Antenna.....	19
3.5.11	Vehicle Tracking and Immobilisation	19
3.5.12	System Health Checks.....	20
3.6	General Documentation Requirements.....	20
3.6.1	User Instructions	20
3.6.2	Installation Instructions	21
3.6.3	Certificate of Installation for Permanently Installed Original Equipment Manufacturer or Aftermarket One Box DVDMS	22

3.7	General Installation and System Commissioning Requirements.....	22
3.7.1	Introduction to Installation Requirements	22
3.7.2	Installation of Hardware and Software.....	23
3.7.3	Installation Technical Requirements.....	24
3.7.4	Procedures for Aftermarket Systems.....	24
3.7.5	Procedures for OEM Systems	24
3.7.6	Installer Security	24
3.7.7	Storage Security	24
3.7.8	Training	24
3.7.9	Activation of System	25
4	DVDMS Operation	27
4.1	DVDMS Identification	27
4.2	Location.....	27
4.2.1	Location Accuracy.....	27
4.2.2	Location Update Rate	27
4.3	Communications	28
4.3.1	Coverage	28
4.3.2	Communication Performance	28
4.3.3	Communication Update – Emergency Light Activation	29
4.3.4	Communication of Driver Profile.....	29
4.4	Geo-fences.....	29
4.5	Diagnostics.....	29
4.6	Vehicle Data.....	30
4.6.1	Emergency Service Equipment Data.....	33
4.6.2	Voice Warnings – Text to Speech	34
4.7	Cameras and Audio	34
4.8	Virtual Log Book.....	36
4.9	Alert Function	37
4.9.1	Resistance to False Alerts	37
4.9.2	Unauthorised Driver	37
4.9.3	Speed Alert	37
4.10	Incident or Event Detection.....	38
4.10.1	Collision or Incident Alert.....	38
4.10.2	Process for Accessing Event/Collision Data.....	39
4.10.3	False Incident Alert	39
4.11	Incident or Event Data Recording Additional Requirements.....	40
4.11.1	Data Recording Frequency.....	40
4.11.2	Driver Notification.....	40
5	Data Requirements	41
5.1	Data Categories	41
5.2	In-Vehicle Data Storage and Retention	41
5.3	In-Vehicle Data Security.....	42
5.4	Data Capture.....	42
5.5	Benchmarking	42
5.6	DVDMS Data Communication.....	42
5.7	Communication In-Vehicle	43

6	Driver	45
6.1	Driver Interaction	45
6.2	DVDMS Driver Identity	45
6.2.1	Driver Identification	46
6.2.2	Wireless Driver Identification	47
6.2.3	Driver Identification Methods	47
6.2.4	Mechanical Driver Identification	48
6.2.5	Multi-driver Vehicles	48
7	Back Office	49
7.1	General	49
7.2	Link to other Databases	50
7.3	Updates and House Keeping	50
7.4	Back Office Sizing	50
7.5	Disaster Recovery	50
7.6	Back Office Database	51
7.7	Freedom of Information Act Requests	51
7.8	Data Access Security	51
7.8.1	Data Security	51
7.8.2	Back Office Audit Data	52
7.9	Back Office Drive Events	52
7.10	Driver Performance	54
7.10.1	Performance Grading	55
7.10.2	Variance from User Defined Figures	55
7.10.3	Excess Threshold Events	56
7.11	Informing or Warning the Driver	56
7.11.1	Driver Feedback	56
7.11.2	Warning of Outside Safety Thresholds	57
7.12	Driver Categories	58
7.12.1	Unauthorised Driver	58
7.12.2	Removal of a Driver Category	59
7.12.3	Driver Profile and Vehicle Profile	59
7.12.4	Normal and Emergency Driving	59
7.13	Vehicle Profile	60
7.14	Driver Profile	60
7.15	Fleet Management Requirements	61
7.15.1	Workshops	61
7.15.2	Servicing	62
7.15.3	Management Information	62
7.16	DVDMS Back Office Reports	62
7.16.1	Costing	63
7.16.2	Driver Reports	64
7.16.3	Level 1 Supervisor Reports	67
7.16.4	Level 2 Supervisors Reports	68
7.16.5	Level 3 Supervisors Report	69
7.16.6	Level 4 Supervisors Report	70
7.16.7	Command/Force Level Report	71
7.16.8	High Priority: Safety Issue Report – Control Room	72

7.16.9	Fleet Managers Overview	72
7.17	Workshop Managers Report	73
7.17.1	Vehicle Profile	75
7.17.2	Technicians Report	76
7.18	Searches	77
7.18.1	Vehicle Usage	77
7.18.2	Vehicle Speed Search	79
8	DVDMS Compliance Procedure and Evaluation.....	81
8.1	Introduction.....	81
8.2	One Box Driver and Vehicle Data Management System.....	82
8.3	DVDMS Accreditation	82
8.3.1	Publication	82
8.3.2	One Box DVDMS Criteria List.....	83
8.4	Period of Application of the Compliance Procedure	83
8.5	Partial Compliance	83
8.6	Compliance Procedures and Administrative Requirements	84
8.6.1	Conditions of Evaluation	84
8.6.2	One Box DVDMS Already Accredited to Relevant Standards.....	84
8.6.3	Application Procedure.....	85
8.6.4	Evaluation	85
8.7	Phases of Evaluation	86
8.7.1	Phase 1: Questionnaire	86
8.7.2	For Vehicle Original Equipment Manufacturer Systems.....	86
8.7.3	Phase 2a: Vehicle Test Programme	87
8.7.4	Phase 2b: Functional Test Programme for Aftermarket Systems	88
8.7.5	Original Equipment Manufacturer System Component Certification Programme.....	89
8.7.6	Phase 3: Review and Notification	89
8.7.7	Compliance Procedure Summary.....	90
8.8	Management of Failures	91
8.8.1	Minimisation of Failures	91
8.8.2	Timings	92
8.9	Administrative and Technical Documentation to be Submitted at Each Test Phase	92
8.9.1	Phase 1	92
8.9.2	Phase 2a.....	92
8.9.3	Phase 2b.....	92
8.10	Aftermarket Systems to be Submitted	94
8.11	Name Changes or Additions	95
8.12	Branding of Systems by Vehicle Manufacturers or Adding Additional Vehicle Models (Original Equipment Manufacturer Only)	95
8.13	System Derivatives	96
8.14	Documentation Available to Applicants.....	97
8.15	Documentation Available from Test Houses.....	97
8.16	Schedule of Evaluation Rates	97
8.17	Reporting.....	98
8.17.1	Evaluation Progress Reports	98
8.17.2	Period for the Notification of Compliance	98

8.18 Use of the Names – Centre for Applied Science and Technology, Accredited Test Houses and Association of Chief Police Officers.....	99
8.19 Compliance Verification and Term of Validity	99
8.19.1 Quality Assurance	99
8.19.2 System Quality Audit.....	100
8.19.3 Audit Process	100
8.19.4 Random Audit	102
8.20 System Changes	102
8.21 Warranty, Notification Incidents and Performance Information	103
8.21.1 Misrepresentation of Listed System Name	103
8.21.2 Discontinuation of Production	103
8.21.3 Withdrawal of the Notification of Compliance	103
8.21.4 Renewal of the Notification of Compliance	104
8.22 Audit and Annual Listing Fee	104
8.23 System Specification and Classification.....	104
8.24 Liability	104
8.25 Performance and Environmental Test Regime	104
8.25.1 In-Vehicle Testing	105
8.25.2 Additional/optional Equipment to be Tested	106
8.25.3 Changes of State and Failure Modes	106
8.25.4 Performance and Environmental Testing Failure	106
8.25.5 Tracking/Field Trials.....	107
8.26 Acknowledgements	108

List of Figures

Figure 1 – Schematic representation of DVDMS concept.....	3
Figure 2 – Difference between raw data and useful information.....	4
Figure 3 – Bands showing fuel consumption performance for specific vehicle types.....	55
Figure 4 – Example of a driver performance profile.....	65
Figure 5 – Various different types of Driver Report that can be made available	66
Figure 6 – Driver report, highlighting areas for improvement.....	66
Figure 7 – Individual driver profile report	68
Figure 8 – Driving behaviour profile by team.....	69
Figure 9 – Driving behaviour profile by Police Station	70
Figure 10 – Driving behaviour profile by District	71
Figure 11 – Driving behaviour profile by Division.....	72
Figure 12 – Prioritised driving behaviour profile report with details and suggested action	72
Figure 13 – Fleet Manager’s report.....	73
Figure 14 – Workshop Manager’s report	74
Figure 15 – Police Station detail for Workshop Manager.....	74
Figure 16 – Vehicle report for Workshop Manager	75
Figure 17 – Vehicle maintenance profile	76
Figure 18 – Vehicle technician’s report	77
Figure 19 – Vehicle usage search criteria	78
Figure 20 – Vehicle utilisation report by Division, Department or Station	79
Figure 21 – Specific vehicle utilisation report	79
Figure 22 – Vehicle speed report by District	80
Figure 23 – Speed report for a single vehicle.....	80

List of Tables

Table 1 – Performance grading colour scheme to enable performance to be assessed at a glance	55
Table 2 – Driver and permit categories	59
Table 3 – Summary of compliance procedure	90

Normative References

This document incorporates provisions from other publications. These Normative References are cited at appropriate places in the text. For undated references, the latest edition of the publication referred shall apply – including any amendments. For dated references, subsequent amendments or revisions shall apply.

- BS EN 60068-2-1: 1993, Environmental testing. Test methods. Tests A. Cold, December 1990
- BS EN 60068-2-2: 1993, Environmental testing. Test methods. Tests B. Dry heat, August 1993
- BS EN 60068-2-78, Environmental testing - Part 2-78: Tests - Test Cab: Damp heat, steady state
- BS EN 60529: 1992, Specification for degrees of protection provided by enclosures (IP code), January 1992
- CiA (CAN in Automation) 447, ‘Application profile for special-purpose car add-on devices,’ May 2008, as amended
- FCS1362, UK Code of Practice for the installation of mobile radio and related ancillary equipment in land-based vehicles (previously known as MPT 1362), May 2008 (‘FCS’ is the ‘Federation of Communication Services’)
- MPT 1372, Code of Practice for field maintenance and repair of civil land mobile radio, Revised & Reprinted November 1996
- EN 61000-4-20: 2010, Electromagnetic compatibility (EMC) – Part 4-20: Testing and measurement techniques – Emission and immunity testing in transverse electromagnetic (TEM) waveguides, 2003, as amended and updated
- ISO 11429: 1996, Ergonomics – System of auditory and visual danger and information signals
- European Statement of Principles on the Design of Human Machine Interaction (HMI), 2008
- Home Office Centre for Applied Science and Technology (CAST), 2007, *Digital Imaging Procedure (58/07)*. London: Home Office
- ISO/IEC 11801: 2002 Category 7/Class F, Information technology – Generic cabling for customer premises
- Interior layout, 74/60, amended by 78/632/EEC
- Council Directive 74/60/EEC, on the approximation of the laws of the Member States relating to the interior fittings of motor vehicles (interior parts of the passenger compartment other than the interior rear-view mirrors, layout of controls, the roof or sliding roof, the backrest and rear part of the seats), December 1973, amended by 78/632/EEC
- AES Automotive Conformance Specification 5, ‘A specification relating to the electromagnetic compatibility (EMC) performance of vehicle mounted,

electrically powered equipment, designed for use by the Police & Fire Services of England and Wales’

- AES Automotive Conformance Specification 6, ‘A specification relating to the electromagnetic compatibility (EMC) performance of motor vehicles for use by the Police Services of England and Wales’
- AES Automotive EMC Assessment and Installation Evaluation Specification 13, ‘A specification relating to the electromagnetic compatibility (EMC) assessment and installation evaluation of electrical, electronic and radio equipment in Police & Fire Service vehicles’
- Home Office One Box Single Vehicle Architecture criteria
- ISO 9001, ISO 9000, ISO 9004 Quality Management
- Radio signalling legislation (European Telecommunications Standards Institute – ETSI)
- RJ45, registered jack, standardised as the IEC 60603-7 8P8C modular connector, physical dimensions of the connectors are specified in ANSI/TIA-1096-A and ISO 8877 standards
- ISO 11898, Road vehicles – Controller area network (CAN)
- ISO 4040, Road vehicles – Location of hand controls, indicators and tell-tales in motor vehicles
- ISO 3958, Passenger cars – Driver hand-control reach
- ISO 2575: 2010, Road vehicles – Symbols for controls, indicators and tell-tales
- ISO/FDIS 15006, Road vehicles – Ergonomic aspects of transport information and control systems – Specifications for in-vehicle auditory presentation
- ISO 15005: 2002, Road vehicles – Ergonomic aspects of transport information and control systems – Dialogue management principles and compliance procedures
- ISO 15008: 2009, Road vehicles – Ergonomic aspects of transport information and control systems – Specifications and test procedures for in-vehicle visual presentation
- ISO 4513: 2010, Road vehicles – Visibility – Method for establishment of eyellipses for driver's eye location
- RS-232, recommended standard 232
- RS-485, recommended standard 485, also known as TIA/EIA-485
- SAE J1113, Electromagnetic Compatibility Measurement Procedure for Vehicle Components – Immunity to AC Power Line Electric Fields
- IEC/EN 60950, Information technology equipment – Safety, 2005
- Council Directive 2005/83/EC, amending, for the purposes of their adaptation to technical progress, Annexes I, VI, VII, VIII, IX and X to

Council Directive 72/245/EEC relating to the radio interference (electromagnetic compatibility) of vehicles, November 2005

- Council Directive 2006/28/EC, amending, for the purposes of their adaptation to technical progress, Council Directive 72/245/EEC of 20 June 1972 relating to the radio interference (electromagnetic compatibility) of vehicles and Council Directive 70/156/EEC on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers, March 2006
- Council Directive 2009/19/EC, amending, for the purposes of its adaptation to technical progress, Council Directive 72/245/EEC relating to the radio interference (electromagnetic compatibility) of vehicles, March 2009
- ISO 17025 (Competency of Test Houses) Test and Calibration criteria
- ETSI EN 300 220-1 v1 3.1 (2000-9)
- ISO 15007-1: 2002 Measurement of driver visual behaviour with respect to transport information and control systems – Part 1: Definitions and parameters
- ISO/TS 15007-2: 2001 Measurement of driver visual behaviour with respect to transport information and control systems – Part 2: Equipment and procedures
- ISO 17287: 2002 Ergonomic aspects of transport information and control systems -- Procedure for assessing suitability for use while driving
- ISO/TS 16951: 2004 Ergonomic aspects of transport information and control systems (TICS) - Procedures for determining priority of on-board messages presented to drivers
- ISO/TR 16352: 2005 Ergonomic aspects of in-vehicle presentation for transport information and control systems – Warning systems
- ISO 16673: 2007 Ergonomic aspects of transport information and control systems -- Occlusion method to assess visual demand due to the use of in-vehicle systems
- TRL Project Report PA3721/01 Design Guidelines for Safety of In-Vehicle Information Systems

Other references may be included by way of addendum or in future releases.

Note: ISO standards are available through the ISO website at:
<http://www.iso.org>.

Definitions and Abbreviations

For the purposes of this standard, the following definitions and abbreviations shall apply:

Note: Definitions relate to the terms used in this document and are not intended to define or exclude existing or alternative technologies.

ACPO – Association of Chief Police Officers

AES – the Automotive and Equipment Section

Aftermarket equipment (AM) – vehicle equipment installed at any stage following vehicle production

ANPR – Automatic Number Plate Recognition

Authorised agent – person or persons authorised to act on behalf of the registered owner or keeper of a motor vehicle

Back Office – office-based remote logging and data processing capability for DVDMS

CAN – Controller Area Network

CAST – [Home Office] Centre for Applied Science and Technology

Commissioning – method of ensuring newly installed DVDMS is functioning correctly

Control equipment – component or components of the DVDMS that process the setting and un-setting commands

DVDM – (One Box) Driver and Vehicle Data Management

DVDMS – (One Box) Driver and Vehicle Data Management System

EMC – Electromagnetic compatibility

esCAN – emergency service Controller Area Network

Evaluation Number – reference number issued by CAST to a type of DVDMS for identification purposes

GNSS – Global Navigation Satellite System

GPRS – General Packet Radio Service

GPS – Global Positioning System

GSM – Global System for Mobile Communications

HMI – Human-machine interface

ISO – International Organisation for Standardisation worldwide

ITS – Intelligent Transport Systems

LAN – Local Area Network

LED – Light Emitting Diode

MDT – Mobile Data Terminal

NAPFM – National Association of Police Fleet Managers

OBDVDM – One Box Driver and Vehicle Data Management

OE – Original Equipment, meaning vehicle equipment installed during original vehicle production and fully validated by the engineering division of the vehicle manufacturer

OEM – Original Equipment Manufacturer (vehicle manufacturer)

Public authority – a publicly-funded or part-funded organisation, for example, the Emergency Services

Public Authority Standards – minimum standards that are required to satisfy both private industry and public authority organisations, and that are approved by an independent public authority

RFID – Radio Frequency Identification Device designed to emit and receive a radio signal as part of an electronic identification system

Rx – Received data

SLA – Service Level Agreement

SMS – Short Message Service

SVA – Single Vehicle Architecture

TETRA – Terrestrial Trunked Radio

Tx – Transmit data

Upgrade system – DVDMS installed on to a vehicle fitted with an existing recognised system in order to enhance the overall functions

Vendor – company that sells DVDM Systems

VSWR – Voltage Standing Wave Ratio

1 One Box Driver and Vehicle Management System (DVDMS) Concept

1.1 Introduction

The DVDMS criteria define a concept (in this chapter) and the functional and performance requirements (in subsequent chapters) for an advanced driver and vehicle fleet management system, designed specifically by and for the emergency services.

The DVDMS concept includes:

- Capture of real-time data, from both the vehicle and emergency service aftermarket equipment via connection to the One Box SVA esCAN;
- Safe storage and processing of data on the vehicle:
 - This may include providing in-vehicle information and/or feedback to the driver;
- Secure communication of data to an authorised Back Office;
- Automatic secure storage and processing of data into information² relevant to different users accessing the Back Office;
- Automatic communication of information to different categories of user in order to:
 - Improve safety by the prevention of incidents or reducing the number of incidents occurring;
 - Provide information to drivers and supervisors to positively influence driver behaviour;
 - Provide information on fleet utilisation to those to whom it would be useful;
 - Save money by changing the way emergency service vehicles are driven and used;
- The capability for secure access to the data and information held in the:
 - Vehicle; or
 - Back Office;
- A provision for further analysis of information for use in:
 - Fleet Management;
 - Training; and
 - Incident investigation.

² A description of the distinction between ‘data’ and ‘information’ can be found in Figure 2 on page 4

1.2 Objective of DVDMS

The aim of the DVDMS criteria is to facilitate the development, installation and operation of an effective, safe and advanced driver and vehicle data management system, designed specifically by and for the emergency services.

The DVDMS criteria, when implemented in the real-world as an end-to-end system, builds on the processes, practices and public-private partnerships already formed as part of One Box SVA consortium. This includes existing event data recorder and fleet management stakeholders, allied to asset tracking technologies.

DVDMS priorities are:

- To identify and, where possible, intervene to prevent drivers of emergency service vehicles from being involved in safety-related incidents or being misused;
- To improve driver behaviour;
- To improve vehicle usage patterns; and
- To reduce the associated running costs involved with managing a vehicle fleet.

The DVDMS criteria are intended to apply to police vehicles in the UK but are also available to be used by other emergency services, both in the UK and in Europe.

The DVDMS criteria build on those of the One Box SVA criteria and significantly extend the functionality, security and performance requirements of SVA.

This chapter sets out the Concept for DVDMS, which includes:

- The capture of real-time data, from both the vehicle and emergency service aftermarket equipment via connection to the One Box SVA esCAN;
- The safe storage and processing of data on the vehicle;
- This may include, providing information and/or feedback to the driver;
- The secure communication of data to an authorised Back Office;
- The automatic secure storage and processing of data into information relevant to different categories of authorised user accessing the Back Office;
- The automatic communication of information to respective users, in order to:
 - Improve safety by preventing or reducing incidents from occurring;
 - Provide information to drivers and supervisors to change driver behaviour;
 - Provide information on fleet usage;

- Save money, by influencing the way emergency service vehicles are driven and utilised;
- The capability for secure access to data and information held in the:
 - Vehicle;
 - Back Office;
- The provision for further analysis to include:
 - Fleet Management;
 - Training; and
 - Incident investigation.

The DVDMS concept is depicted diagrammatically in Figure 1 below.

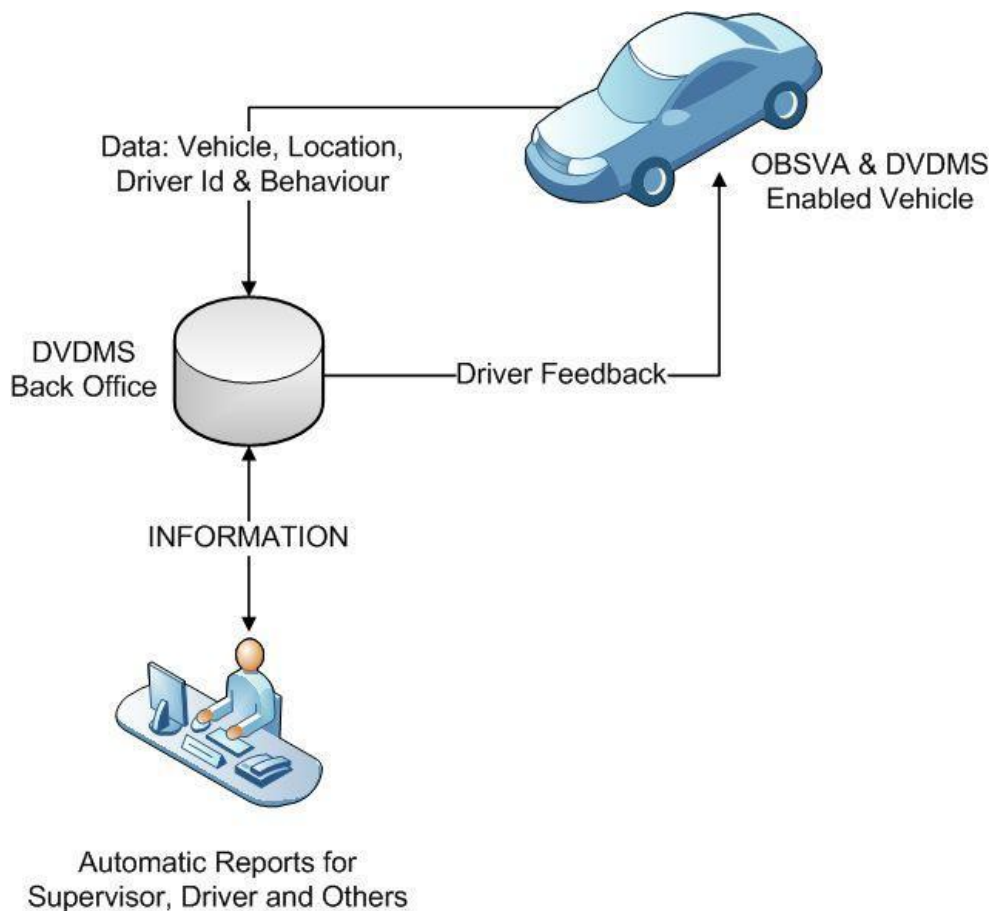


Figure 1 – Schematic representation of DVDMS concept

The scope of the DVDMS concept as set out in this document includes:

- General and specific requirements for an end-to-end DVDMS;
- A requirement for DVDMS-compliant systems to be designed, installed and operated to work with and where appropriate and possible, integrate with the original equipment installed by the vehicle manufacturers, via the OBSVA esCAN;

- The requirement for bespoke information reports to be automatically generated and communicated by the Back Office for each different level of user with relevant access controls to protect those reports and information so only those authorised can view and access, negating the need for additional analytical capability within the host organisation; and
- Reports that will be able to be configured and presented to users so that they are simple and easy to understand and need little or no analytical effort from the end user.

Reports generated by the DVDMS as shown in Figure 2 below need to be simple to understand by the end user. It is also required that reports be underpinned by detailed data, which can be drilled down into but only when required.

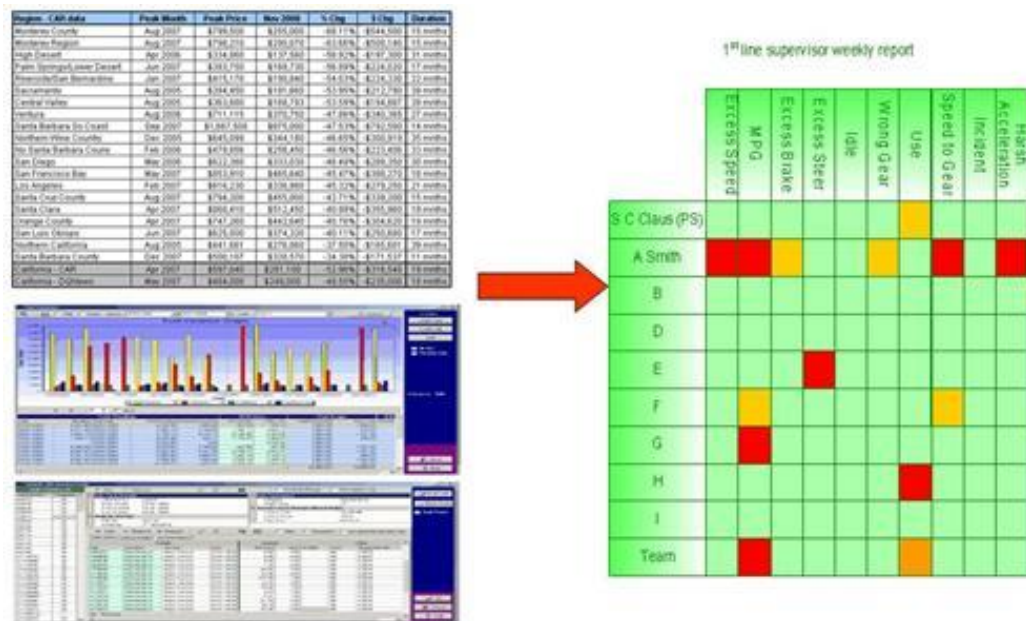


Figure 2 – Difference between raw data and useful information

The DVDMS will generate incident and event notifications and alerts from equipped vehicles, which may indicate an event or misuse that could have the potential for serious consequences for safety and security. All such safety-related alerts and alarms from DVDMS-equipped vehicles will be treated as a high priority by the on-board device and Back Office for evaluation and onward communication to the nominated person(s) in that organisation.

For DVDMS to succeed, it is essential that emergency service control rooms only receives DVDMS notifications to genuine events and compliance with these criteria will go some way to ensure that the system is well designed and installed so as to minimise such false activations.

1.3 Effective and Fair Supervision

The DVDMS will provide a wealth of information on how drivers and vehicles are performing, about vehicle usage and a wide range of other parameters. When properly used, DVDMS can provide the information necessary to allow supervisors to better manage their resources. It is important to recognise that the DVDMS is not a substitute for effective supervision but a tool to provide the information to allow effective supervision. Influencing driver behaviour and vehicle usage will require supervisory intervention.

This includes:

- Recognising good behaviour;
- Challenging driver behaviour or vehicle usage when it falls outside acceptable parameters; and
- Providing guidance, encouragement and training to improve driving behaviour or vehicle usage.

This will need new procedures to be developed, helping to ensure that such interventions are fair and balanced, that the information is used consistently and appropriately and that a worker's right to privacy is appropriately protected.

Whilst it is not possible to check how each supervisor uses the information, ensuring systems have appropriate checks and balances designed into them will form part of the independent testing and verification, as outlined below and in the test and evaluation documents.

1.4 DVDMS Criteria

The DVDMS criteria define the functions, connections, outputs and operating systems for all parts of the system, both in-vehicle and Back Office. The criteria also require rigorous and independent testing for compliance before systems can be Listed (see Chapter 8).

This document provides the functional and performance requirements of the DVDMS, including installation, commissioning, operation and procedures for an end-to-end system that need to be implemented by companies manufacturing, installing, commissioning and operating both OEM and aftermarket DVDMS.

These specifications shall be subject to amendments or extensions from time to time, in order to recognise advances in technology, changes to and consolidation of standards, legislation and best practice.

The objective of validation in accordance with these criteria is to ensure a minimum high level of performance with regard to safety, security, reliability and functionality of the evaluated DVDMS.

The DVDMS criteria also define the requirements for documentation, quality of installation and operation of the proposed system. It specifies the minimum performance requirements, tests and processes to which the DVDMS shall be subjected, ensuring the safe and effective deployment of the system and protection for vehicle occupants and motor vehicles.

These specifications are applicable both to new vehicle OEM fitment and systems professionally installed after the sale of the vehicle. However, it is recognised in the DVDMS criteria that, while there must be commonality of functions, connectors and performance, the design and installation for OEM equipment, compared with aftermarket equipment may be different and this document identifies where this applies.

The criteria set out requirements for both the in-vehicle device and the Back Office functions that monitor the DVDMS. Systems Listed as compliant shall be required to meet or exceed the requirements of the normative references referred to in this document.

2 General Requirements

2.1 Introduction

The following chapters detail the functional and performance requirements that DVDM Systems are required to meet in order to be Listed as compliant.

Systems that meet the DVDMS criteria for emergency service vehicles will be required to work effectively and reliably in all real-world operating conditions faced by equipped vehicles – as a minimum in the UK and Europe.

When required to be activated, the entire end-to-end system, which includes the in-vehicle equipment and the Back Office, must operate effectively in order to deliver the safety and security benefits that are made possible by compliance with these criteria.

They will have been tested to verify they work effectively in the emergency services operating environment and meet all of the quality, security and performance criteria required.

2.2 Coverage

The DVDMS shall be capable of effective operation across the UK and should be capable of covering Europe, with the potential for being expanded to worldwide operation. This includes the in-vehicle device, communication and Back Office, which shall be designed, operated and maintained to ensure that it is capable of operating at all times.

2.3 Bundled Services

The DVDMS criteria describe the core functionality of the system that must be provided. However, it also recognises the real-world imperatives of providing an effective business case, to ensure the widest deployment of DVDMS technologies. Therefore, DVDM systems may include additional facilities or functionalities as part of the system seeking compliance with these criteria, providing they have been accredited as per the procedures laid down in this document and have been found to be safe, secure and not to interfere with the core functionality.

Such additional facilities or functionalities must also be agreed by CAST, as part of an application for accreditation. In particular, this includes linkage with Project RESTORE technologies that enable the remote immobilisation of high risk vehicles. Reference should be made to the appropriate Home Office RESTORE criteria.

As part of this assessment all parties submitting a DVDMS for testing against the criteria shall, where bundled services are to be included, conduct a thorough assessment to determine the safety of their system using a recognised methodology with a full classification of risks to the DVDMS, prior to submission. This analysis shall as fully as possible define the potential risks posed by such bundled services and the measures taken to militate against those risks. The assessment shall then be verified and extended as required by the accredited test house to ensure that the bundled services represent either no risk or no unacceptable risk to the DVDMS.

Aftermarket or general upgrade systems shall not be permitted to connect into, or interact with, any existing installed DVDMS, unless tested in such a mode, accredited as part of the formal process by an accredited test house and certificated by CAST. This would be managed as a change application from the system manufacturer to CAST.

2.4 Upgradeable and Reusable

The DVDMS, both software and hardware, installed in the vehicle and Back Office, shall have a long operating life of at least 8 years. It is recognised over this life span that there will be changes and upgrades to the system and or its components.

The DVDMS shall be designed to be upgradeable, to enable future functionality, with redundant or expandable communication, data storage and power capability to allow for expansion and through standardised connections, operating systems and data dictionary, to include the Back Office.

The in-vehicle components shall be capable of being removed and re-fitted into other vehicles as requirements change or vehicles are replaced.

The supplier and the user shall be required to keep a secure record of all changes and upgrades to the system.

2.5 Open Standards

DVDMS shall be based on open data standards; this will include and facilitate connection to esCAN and utilisation of the CiA 447 data protocols. The Back Office shall log data and produce information in the formats set out in this document, which will allow comparison and benchmarking with other users, operating the same or different compliant DVDM systems. This will include compliance with existing or emerging UK and EU standards, as defined in the Normative References and elsewhere in this document or as it is amended.

2.6 Quality Assurance

The DVDMS shall have security and quality control built in from the inception, including where the DVDM device or Back Office is connected to other vehicle component or other systems.

Back Offices operating in conjunction with DVDMS shall comply with the requirements of this document and the provisions in this document and as a minimum include BS EN ISO 9001: 2000.

2.7 National Procedures for Operation of DVDMS

Where possible, there shall be nationally agreed operating procedures and practices for the DVDMS, with clear guidance, where local customisation (based on best practise) is acceptable. From this, each organisation (e.g. Police Force) will develop their own detailed operational procedures for all aspects of the system including:

- Use/Repair;
- Replacement;
- Maintenance;

- Failures/ Faults;
- Complaints;
- Access control;
- Security;
- Authorities for Access-use;
- Data Handling;
- Evidence and Handling;
- Back Office Reports;
- Data Storage;
- Accuracy testing and data extraction;
- Quality Control; and
- Audit.

2.8 Audit

As part of the operation of the DVDMS, it is essential to have full accountability for the use, operation and access to all parts of the system. This shall be required for legal purposes, as part of the evidential process and to ensure and evidence the proper use of the system.

The audit trail, where possible, requires identifying the person undertaking each action, the date, time and location of the action, together with the action or process carried out. This shall include a log of driver identity associated with the vehicle together with any actions that they take, for example, removal of data from the in-vehicle device or any operation or action in the Back Office system. The audit trail shall also be required to capture access to any part of the system, use, maintenance, inspection, breaches and sanctions.

It is essential that where control messages from aftermarket equipment are sent via the esCAN, that they are also received and stored by the DVDMS as part of the audit process and for analysis of driving and equipment operation. The esCAN will also carry the data from the vehicle OEM CAN, as part of the emergency service data set.

The system shall be designed to identify where possible all of the occupants in a vehicle and shall be capable of assigning events, actions or inputs to individual persons. This audit trail shall be kept, as required for legal processes for evidence, which is currently 7 years.

A full audit trail of all actions and commands sent to a DVDMS in-vehicle device shall be stored within the DVDM device securely for at least 7 days before being overwritten. It can additionally be stored in the Back Office. This shall be time stamped and digitally certified to evidential standards or best practice. These can be found in the following publications:

- CAST publication – Digital Imaging Procedure – 09/05;
- CAST publication – Digital Data Standards for Handling – 58/07;

- CAST publication – Retrieval of Evidence and production for evidence – 66/08; and
- NPIA – Advice on Police Use of Digital Images 2007.

2.9 Human-Machine Interface within the DVDMS

The scope of the HMI requirements in the DVDMS criteria is limited to the location, installation and operation of the hardware and software provided as part of emergency service electronic equipment fitted to the DVDMS in that vehicle. Specifically, this includes:

- Use of DVDMS alerts or data sent to a mobile data or other screen in a vehicle, with particular emphasis on a moving vehicle; and
- DVDMS alerts, be they visual, audible or haptic.

The European Statement of Principles on HMI (2008) will be one of the definitive documents in this area. System suppliers shall use this in conjunction with the TRL checklist to assess whether their systems comply with HMI requirements.

2.10 Legislative Requirements

The DVDMS shall comply with all current legislative requirements to the extent that they are applicable. This includes but is not limited to:

- The Road Vehicles (Construction and Use) Regulations 1986
- The Road Vehicle Lighting Regulations 1989
- The Road Traffic Act 1988
- Data Protection Act 1998
- United Nations Economic Commission for Europe (ECE) Regulation TRANS/WP 29/425, Uniform provisions concerning the approval of vehicle alarm systems (VAS) and of motor vehicles with regard to their alarm systems (AS), 1 January 1996
- Human Rights Act 1988
- Radio signalling legislation – including European Telecommunications Standards Institute – ETSI
- Road Traffic Act 1991
- Council Directive 72/245/EEC, Automotive Electromagnetic (EMC) Requirements, June 1972
- United Nations Regulation 116, Uniform technical prescriptions concerning the protection of motor vehicles against unauthorized use, April 2005
- The Control of Noise at Work Regulations 2005
- Council Directive 2004/104/EC, adapting to technical progress Council Directive 72/245/EEC relating to the radio interference (electromagnetic compatibility) of vehicles and amending Directive 70/156/EEC on the approximation of the laws of the Member States relating to the type-approval

of motor vehicles and their trailers, October 2004, as amended by 2005/83/EC, 2006/28/EC, 2009/19/EC and other applicable Directives

- Council Directive 74/61/EEC, on the approximation of the laws of the Member States relating to devices to prevent the unauthorized use of motor vehicles, December 1973, as amended and corrected, amended by 95/56/EC
- Council Directive 2006/95/EC, on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits, December 2006 (known as ‘Low Voltage Directive’)
- Council Directive 90/630/EEC, adapting to technical progress Council Directive 77/649/EEC on the approximation of the laws of the Member States relating to the field of vision of motor vehicle drivers, October 1990
- Council Directive 78/316/EEC, on the approximation of the laws of the Member States relating to the interior fittings of motor vehicles (identification of controls, tell-tales and indicators), December 1977, amended by 93/91/EEC and 94/53/EC
- Other relevant best practice
- Other CEN or ISO standards that may be applicable

Compliance with all legislation is the responsibility of the compliant DVDMS manufacturer, importer and installer.

Compliance with these criteria does not confer immunity from legal obligations. If a conflict exists between these criteria and those of legislation, the requirements of the legislation shall take precedence.

3 In-Vehicle Components and Use Requirements

3.1 General

The DVDMS shall be capable of being fitted to all powered vehicles.

The DVDMS shall be simple to operate, both by the user and in the Back Office function. Examples are referred to throughout the document and include activation, driver identification, setting of geo-fences, use of searches, reports and so on.

The DVDMS supplier and/or installer shall agree with the vehicle manufacturer on the location for the installation of the DVDM device in the vehicle and the secure, safe routing of cables, power and control capability, to ensure that the resulting system is safe, effective and does not interfere with other vehicle or emergency service equipment, including the emergency service radio system.

Any DVDM in-vehicle device shall follow emergency service guidelines and specifications, in order to ensure it is safe, most effective and compliant with electromagnetic compatibility (EMC), HMI, relevant legislation and European Directives. These include AES Specification 5, NAPFM Installation Guidelines and FCS 1362.

The DVDMS and the components attached to it shall where possible comply with all relevant new vehicle legislation for all fitments, both new and aftermarket. Where a DVDMS fitment is unable to comply with new vehicle legislation, this must be brought to the attention of CAST, who will decide whether or not this is acceptable. CAST may require the supplier to agree to additional conditions prior to Listing, such as notifying customers of this derivation.

3.2 Controls

All adjustable controls and pre-set adjustments, as may be fitted within the DVDMS shall be accessible only by the removal of a normal access panel or existing vehicle trim panel. It is preferable that adjustments to the DVDMS be made using a physical connection with a computer or similar device, in order to promote system security.

3.3 One Box esCAN

The One Box esCAN is a CAN bus compliant with ISO 11898 specification, for communication and control of the emergency service electronic equipment within the vehicle. This shall use the open (published) CiA 447 data dictionary, to enable all suppliers to the market to use it and allow for the interchange of equipment.

The esCAN network shall physically consist of industry standard CAN shielded twisted pair wire. The esCAN shall operate at a minimum of 125 kbit/s in order to provide the requisite functionality.

Each relevant component of emergency service equipment systems shall be connected to the esCAN bus via a standard CAN bus controller.

The provision of technology in emergency service vehicles shall require CAN bus controllers to broadcast a status onto the CAN so that the DVDMS can record that signal for any subsequent processing, analysis or investigation.

The DVDM device shall be capable of being connected to and communicating with the vehicle esCAN, where this is fitted, including receiving, processing and storing data from the esCAN.

Note: Where esCAN is not available, the DVDM device can be connected to the OEM CAN, where this is permitted and supported by the vehicle manufacturer, or to other emergency service aftermarket equipment data outputs to deliver some or all of the functionality listed below.

CiA 447 defines the standard messages that shall be used on the esCAN bus. It also defines connections to and communication with the internal vehicle CAN. The esCAN data dictionary will be maintained and extended by the CiA as part of their ongoing development of relevant CiA standards.

The esCAN data dictionary CiA 447 has been published as an open standard. Organisations wishing to obtain copies of the publication should contact CiA directly.

The information that the esCAN bus carries shall include, but is not limited to, the following:

- Emergency warning lights –controls;
- Sirens –controls;
- Power management system –related to the above functions;
- Automatic Number Plate Recognition (ANPR) – controls/status;
- Evidential or other camera – controls/status;
- Speed or other enforcement equipment;
- Matrix signs;
- GNSS (satellite navigation);
- One Box Driver and Vehicle Data Management System (DVDMS);
- Defined subset of vehicle CAN data (see One Box SVA); and
- Other non-safety-critical functions.

All messages on the esCAN must be capable of being received and utilised by the DVDM device regardless of whether they originate from emergency service equipment installed on the vehicle or are messages from the base vehicle CAN that have been broadcast on the esCAN via the firewall.

3.4 One Box DVDMS Operation

The DVDMS shall be designed to work with:

- All vehicles
- All fuel types;

- All transmission types.

However, where a DVDMS cannot operate with a particular vehicle type (for example, if it were not compatible with electric vehicles), then subject to the agreement of CAST, a DVDMS may be Listed as compliant with the criteria, subject to agreed exceptions in this area of operation, namely limits to vehicle, fuel and transmission type.

Where this exception is requested, it shall be required to be clearly identified as part of the application process and if agreed, shall be explicitly included in any DVDMS criteria summary report produced by the accredited test house. Furthermore, exceptions shall be stated clearly in any commercial or marketing information.

3.4.1 Safety and Reliability

The DVDMS and its installation shall be safe, reliable and durable, as defined by compliance with relevant sections of these criteria.

The DVDMS shall as a minimum be as reliable as existing safety-related vehicle control systems.

The DVDMS shall be subject to a minimum warranty of 12 months, although a minimum of 24 months is normally expected, covering system and installation.

The DVDMS shall have an automated service and function checking capability, operating during the normal lifetime of the DVDMS.

The mechanical and physical properties of the DVDMS shall be such that it presents no unacceptable risk of danger or hazard to any person.

The risk of vehicle malfunction attributable to the DVDMS and its installation shall be minimised through attention to quality of design, manufacturing and installation, as defined by compliance with relevant sections of these criteria, including audit and random inspection.

The manufacturer of the DVDMS shall conduct a thorough assessment to determine the safety of their system using a recognised methodology to all possible failure modes of the DVDMS, so that it minimises the risk of danger or hazard to any person.

The DVDMS shall, in the event of a system or component failure, not affect the performance or the safe operation of the vehicle or its components, especially with regard to brakes or steering. This is critical where the esCAN connects to the internal vehicle CAN and to enable command inputs and/or processing.

Additional or auxiliary equipment interfacing with the DVDMS shall not adversely affect the normal operation of OEM systems.

3.4.2 User Cannot Deactivate

The user of the DVDMS shall have no facility to deactivate directly, change or override the functionality or performance of the system, unless specifically authorised to do so by the user organisation.

3.5 In-Vehicle Device

3.5.1 Device Dimensions

The DVDM device shall be small in size and weight and is a self-contained robust box that can be mounted safely into a range of locations within a vehicle to include: the boot/storage/passenger compartment of any vehicle, including commercial vehicles.

- Vehicle other than motorcycles maximum dimensions:
 - 150 mm by 150 mm by 70 mm; and
 - Max weight 1 kg.
- Motorcycles maximum dimensions:
 - 100 mm by 70 mm by 50 mm; and
 - Max weight 500 g.

The DVDM device shall be designed so that it can be easily and securely fitted to the vehicle in any of a wide range of locations, to include a single connection to the esCAN, where fitted.

3.5.2 DVDMS Marking

The DVDM main control unit shall be marked with the following information:

- The compliant DVDMS manufacturer's name or trade mark;
- The model number or name;
- Component part number; and
- The serial number or batch number or date of manufacture of the compliant DVDMS.

All large component parts shall be visibly identified by a part number.

3.5.3 Device and System Security

The DVDM in-vehicle device requires mechanical protection in order to be fully effective. This can often include the normal physical structure of the vehicle to which the DVDMS is fitted.

The DVDM in-vehicle device and Back Office shall also be designed to prevent cyber attack, unauthorised access or download or disruption, corruption, loss or damage to data.

The DVDMS, components shall be designed, manufactured and installed in such a way as to minimise the risk of a person de-activating or destroying it by:

- Intentional damage;
- Accidental damage;
- Damage as a result of a collision;
- Loss or corruption of data by electromagnetic means;

- Cyber attack (for example, an attempt by an unauthorised user to gain access to the in-vehicle device or Back Office by connecting to the device and attempting to access or corrupt data or information, or seeking to prevent its capture); and/or
- Unauthorised access/download.

The DVDMS shall be designed and installed and maintained in order to resist being de-activated by deliberate electrical, electronic and mechanical attack.

The DVDMS in-vehicle device shall have security to ensure that if the device is lost or unauthorised access to area where the device is located is gained, that access to the data and controls within the device and/or access to the DVDMS is prevented or the data is protected so that it cannot be used.

3.5.4 DVDMS Operating Conditions

The on-board equipment must be reliable and be capable of effective operation, as defined by compliance with relevant sections of these criteria, at all times.

For a system to meet the DVDMS criteria it must be designed with a minimum operational life span of 8 years.

The DVDMS shall function correctly in all relevant environmental conditions where it is required to be operated, to include:

- All weather types, including lightning strikes;
- Temperatures ranging from -20 to +85C;
- Vibration;
- Fluid resistance, including resistance to human fluids, to at least IP54;
- Impact resistance;
- EMC;
- Fire;
- Data or power interruption;
- Atmospheric conditions; and
- Water and dust.

Note: Specific references with regards to test standards can be found in section 8.25.

3.5.5 Compatibility with Vehicle and Emergency Service or Other Specialist On-Board Equipment

The installed DVDMS shall not adversely affect the safety or normal performance of the vehicle during the normal vehicle lifetime.

All the components of the DVDMS shall be correctly rated and technically compatible and not interfere with other OEM, aftermarket system components or other vehicle systems, other than as outlined as part of these criteria. (This includes EMC and mechanical interference.)

This requirement also applies to specialist equipment that may be fitted to this type of vehicle, including emergency service equipment, enforcement equipment and TETRA radio.

This will be tested through compliance with:

- EMC regulations: must meet 2004/104/EC;
- AES Automotive Conformance Specification 5, latest version;
- One Box Single Vehicle Architecture (SVA); and
- Other mandatory standards.

3.5.6 Electrical Requirements

The main source of power for the DVDMS, as for OBSVA, shall be taken from a location specified by the vehicle manufacturer and will be required to operate within the power management capabilities of the vehicle, without compromising other components through power drain.

The normal voltage for the DVDMS, as for OBSVA, will be 12 volts and must also be able to operate with an external trickle feed power supply when used.

The DVDMS shall require no more than 20 milliamperes (mA) quiescent current consumption when the equipment is not in use and the vehicle engine is not running, to reduce the risk of flattening the vehicle battery.

The current consumption of the DVDMS in the set state (vehicle ignition switched off, system set and able to respond immediately to Rx/Tx from the Back Office or obtaining their GPS location) shall not exceed 10 mA when supplied with a 12 volt nominal supply voltage (or the equivalent power consumption at an alternative supply voltage), subject to current legislative requirements.

The DVDMS shall continue to function correctly under conditions of supply voltage variation, specifically within the range of 9–18 volts.

The DVDMS shall be able to resume normal operation after repeated low, flat or no power events.

Power supply disconnection for up to 28 days without loss of data and return to normal use when power supply is reconnected.

The wiring of the DVDMS shall be of a standard suitable for the automotive environment.

The circuits and wiring of the DVDMS shall be adequately electrically rated for all states and conditions of operation.

The internal power supply shall be protected from discharge due to short-circuiting of the connections to the power supply.

3.5.7 Electrical Backup

The DVDMS shall contain and be operated in the event of loss of the vehicle battery supply by either:

- A rechargeable electrical power source and a charger charging from the vehicle electrical system; or

- A stand alone electrical power source.

The electrical backup provision shall comply with sections below.

3.5.8 Standalone Power Supply

The internal supply capacity shall be sufficient to support the device, such that it will remain operational for a period of not less than 2 hours (Unless this is a combined Restore box when it will be 8 hours) and suitable to preserve the data for a period of at least 28 days, following loss of power.

The electrical power source life shall be sufficient to support the device for a minimum of 4 years.

An automatic electrical power source test shall be carried out every 6 months.

Low electrical power source condition shall be signalled to the Back Office as soon as it is detected.

The electrical power source pack shall be replaced:

- When low electrical power source voltage signal is received;
- After a period of not more than 3 years; and/or
- If it is believed to have been compromised for any reason.

3.5.9 Power Feedback

It shall not be possible for power from the internal DVDMS power supply to feed back to the vehicle electrical system.

3.5.10 Antenna

All antennae, regardless of system technology, shall normally be mounted in covert locations but in such a way that satisfactory performance can be demonstrated in areas of good network coverage. All antennae, to include GSM, 3 or 4G or GPS should, wherever possible be combined with or make use of those provided as part of One Box SVA.

Antennae shall be discretely located, in such a way as to minimise their recognisability as a part of the Telemetric system and to guard against deliberate attack or damage.

Care shall be taken to ensure that the vehicle manufacturers and AES guidelines regarding the installation of aftermarket equipment are not compromised in any way.

3.5.11 Vehicle Tracking and Immobilisation

The DVDMS has many common components and functions to a wide range of tracking and remote vehicle immobilisation capabilities.

Where the DVDMS is fitted to a vehicle to which the Home Office RESTORE criteria applies, the DVDMS and RESTORE functionality may be combined on the same device, increasing functionality and reducing cost to the end user.

Where this occurs, the DVDM/Restore system must be approved, so as to comply with the requirements of both sets of criteria. Subject to the agreement of CAST, such testing may, where appropriate, be combined.

The DVDMS may include other vehicle immobilisation capabilities, such as preventing engine start by an unauthorised user. Where this is provided, the test house must satisfy themselves that the system is legal and complies with the Home Office CAST document 14/02 and in particular appendix E. The device or any other linked system or bundled service must be tested to ensure that it does not compromise the operation of the DVDMS.

3.5.12 System Health Checks

From the date of going live, the DVDM device shall be successfully polled by the Back Office or the system host, or the in-vehicle device shall send a 'health check'/signal to the Back Office or system host.

This polling shall occur within at least a 7 day period of the last communication of the system, and at least every 7 days thereafter, for the duration of the active lifetime of the in-vehicle device.

3.6 General Documentation Requirements

Clear and comprehensive Installation Instructions and User Instructions shall support the DVDMS. The user shall be provided with clear instructions as to the use and operation of the system. This will include connection to the system, fault analysis and correct operation and maintenance, operation of the Back Office, reports and searches.

3.6.1 User Instructions

The DVDMS manufacturer, supplier or importer shall supply for each system User Instructions detailing a clear and comprehensive description of:

- System components;
- Operation of the DVDMS functions;
- Action to be taken in the event of a malfunction or failure;
- Prevention of false alerts conditions;
- Action to be taken in the event of driver identification device loss including secure driver identification replacement; and
- Inspection and maintenance.

The User Instructions shall contain a general warning regarding the risk of making any alterations or additions to the compliant DVDMS; such alterations or additions can invalidate the Certificate of Installation and compliance to the DVDMS criteria.

The general User Instructions shall contain no information on how to unset or bypass the DVDMS, other than by the normal un-setting control or controls or alternative (emergency) un-setting procedure. (Specific guidance may be provided to an authorised user where required by that organisation).

The user instructions shall contain a clear warning that in no circumstances should the DVDMS driver identification device be attached to or kept with the ignition key.

The consequences of failing to adhere to this should be highlighted.

The users should also be made aware of their liabilities in the use and operation of the DVDMS and should be required to sign that they have been made aware.

3.6.2 Installation Instructions

The DVDMS manufacturer, supplier or importer shall supply to each installer, after appropriate training, DVDMS-specific Installation Instructions, detailing a clear and comprehensive description of:

- A list of the vehicles for which the DVDMS is applicable. The list may be specific or generic; for example, ‘all cars with petrol engines and 12V negative earth electrical systems;’
- System components;
- Wiring diagrams;
- A schedule of routing for all wiring for that model of vehicle, as agreed with the vehicle manufacturer and in accordance with the principles of AES Specification 5;
- Power supply, voltage range and system current consumption;
- The electrical characteristics of inputs and outputs;
- Installation directions, illustrated by photographs or clear drawings;
- Component installation directions – locations and orientations;
- Wiring installation directions;
- Recommended methods of wiring interconnection;
- Specific fixing instructions for components and wiring;
- Correct and incorrect vehicle circuits or systems to interface;
- Earthing and fusing directions;
- Specific detail of any adjustments and recommended adjustment procedure;
- The effects of adjustable controls on DVDMS performance;
- Any special tools required;
- Connection to the esCAN;
- Testing of the DVDMS;
- Fault finding;
- Maintenance directions;
- Requirement to conduct end-to-end system test of all functionality before final commissioning; and
- Back Office:
 - Installation;

- Security;
- Connection;
- Reports;
- Searches;
- Data Storage;
- Software/ Software updates; and
- Database operating system.

3.6.3 Certificate of Installation for Permanently Installed Original Equipment Manufacturer or Aftermarket One Box DVDMS

The installer shall supply to the system user or their representative for each installed DVDM in-vehicle device, a Certificate of Installation specifying, as a minimum the following information:

- Vehicle make;
- Vehicle model;
- Vehicle registration number;
- Vehicle identification number (VIN);
- DVDMS name;
- DVDMS model or part number;
- DVDM device serial number, batch number and batch code;
- Accredited test house name and evaluation reference number;
- Date of installation;
- Name of installation technician;
- Certificate serial number;
- Back Office installation; and
- Confirmation of commissioning tests and calibration.

The Certificate of Installation is required only for permanently installed aftermarket DVDMS. It is not applicable to temporarily installed DVDMS.

3.7 General Installation and System Commissioning Requirements

3.7.1 Introduction to Installation Requirements

The DVDM device may be installed at any of the following locations:

- Vehicle production line;
- Vehicle import or distribution centre;

- Vehicle dealership;
- Independent DVDMS installer; or
- User organisation premises.

The installer shall maintain a consistently high level of DVDMS installation quality and security.

The Manufacturer/Importer and Installer shall ensure that the release of all sensitive security related technical details of the DVDMS is securely controlled; this shall include driver identity codes.

The supplier and installer of a DVDMS shall agree with the user organisation an installation plan, taking account of the fleet size, type etc. This will include a plan for:

- Full or partial fit of the fleet;
- New or aftermarket fit;
- Connection to esCAN or existing CAN or other data outputs where esCAN is not available;
- Installation of the Back Office;
- Connection of the devices to the Back Office;
- Population of drivers onto the database;
- Distribution of driver identities; and
- Others may be defined by the user.

The test house will be required to assess an example installation plan to ensure it is realistic and comprehensive.

3.7.2 Installation of Hardware and Software

The manufacturer or importer shall provide to the installer a kit of components for each DVDMS installation as specified in this criterion and compliant with the testing procedure in section 8.25.1, and the installer shall ensure that all components of the kit are fitted when a DVDMS is installed. No other components may be substituted.

All aftermarket DVDMS shall be installed in accordance with the specifications laid down in this document.

Installation companies shall adhere to OEM new vehicle legislation and regulations when installing compliant DVDMS fitted after vehicle production.

The DVDMS will not be finally commissioned following installation, upgrade or repair until all or the relevant part of the functionality has been tested, as part of an end-to-end system check.

Note: The installation of the Back Office, where installed as part of the system on emergency services premises, would be managed and governed by the procedures and processes for installing hardware and software for that emergency service. This would include connections to other emergency services systems, where that is deemed appropriate.

3.7.3 Installation Technical Requirements

The following technical installation requirements are specified in order to provide a minimum acceptable level of security:

- All components and wiring of the DVDMS shall be installed in the vehicle in locations and via routes agreed with the vehicle manufacturer and in accordance with the principles of AES Specification 5 as safe, effective and compliant with all EMC and legislative requirements, together with the requirements of other standards listed under Normative References in these criteria;
- Where practical, all components and wiring of the DVDMS shall be concealed from view when installed, excepting visible indicators; and
- All components and wiring of the DVDMS shall be securely fixed to the vehicle.

3.7.4 Procedures for Aftermarket Systems

DVDMS permanently installed as aftermarket equipment by import or distribution centres, vehicle dealers, or by independent DVDMS installers, shall be installed by companies and technicians, in accordance with the administrative and technical standards of FCS 1362 and the NAPFM Guidelines. Where the DVDMS is installed by an emergency service workshop facility staff, they shall be trained to an equivalent level.

3.7.5 Procedures for OEM Systems

Installation of the in-vehicle system shall be carried out by OEM trained personnel, with all installation checks carried out either with the use of the client Back Office where this is permitted, or by use of an OEM recommended control system.

Note: This may require additional commissioning and calibration checks when supplied to the customer.

3.7.6 Installer Security

All installers, repairers and operators of the DVDMS shall be appropriately security checked, to ensure the security and integrity of the DVDMS. This includes in-vehicle and Back Office.

3.7.7 Storage Security

All components of the DVDMS, including devices should be held securely throughout their life, with a full audit trail maintained of their use to include end of life disposal.

3.7.8 Training

The supplier of the DVDMS in conjunction with the user organisations shall ensure training procedures that comply with training best practice, standards or policies for that organisation, are in place for the installation, repair, operation and validation of the DVDMS, to include in-vehicle, Back Office and associated functions, reports and searches. The training should be based on a achieving a minimum standard of competency, before access to DVDMS is granted, which should be held as part of an audit process.

The supplier of the DVDMS shall provide each user organisation a training manual and training package that complies with training best practice, standards or policies for that organisation, suitable for:

- Installers;
- Maintenance;
- Workshop staff;
- Fleet Staff;
- Drivers;
- Supervisors of all grades;
- Analysts;
- Investigators; and
- Others to be defined.

3.7.9 Activation of System

The installer shall be satisfied that every type of DVDM device being monitored meets the requirements of the Back Office criteria.

This includes, not connecting the device to the Back Office until they are satisfied that a full in-vehicle system test has been completed correctly.

Upon auditable confirmation that the tests have been performed successfully, the connection to the Back Office can be made and the device activated for Back Office monitoring. This includes:

- Communication with the vehicle installed system;
- GPS co-ordinates / other signalling method / signal strength / remote location test;
- Health check;
- Alerts (all fitted to that system); and
- Driver identification function.

Other additional checks may be included, if agreed with the user organisation and laid down in their SLA.

All alerts, live tracking information, data capture and any ignition status, and esCAN data shall be recorded and stored either in the in-vehicle device or at the Back Office as set out in the contract or SLA.

4 DVDMS Operation

4.1 DVDMS Identification

The DVDMS shall link vehicle and driver usage, activity, alerts and data to the location, date, time, device and driver identity.

The Back Office shall be able to remotely and uniquely identify each One Box DVDM device that is operated as part of a DVDMS. The DVDM device should authenticate as part of each communication with the Back Office as part of the audit trail.

4.2 Location

Accurately identifying the location of emergency service vehicles in a wide range of conditions, from rural to 'urban canyon' and other to hard reach areas, will be critical to the success of the system.

The DVDMS shall, when requested by an authorised user display:

- A single vehicle
- Multiple vehicles
- Vehicles by user defined group

On a user defined map or other display device in real-time or within a time period defined by the user.

4.2.1 Location Accuracy

The location system shall operate with a:

- Minimum location accuracy for vehicle tracking (fleet management/JDR) of 5metres for 95% of the time; and
- Minimum location accuracy for collision/event management (EDR) of 1 metre for 95% of the time in the horizontal field.

Where vertical location information is provided, it shall be accurate to 10 metres.

The DVDM device should also record GNSS signal strength where this is available.

4.2.2 Location Update Rate

The location update rate in the device shall be variable from 1 Hz to 1 update per 8 hours. This shall be configurable by an authorised user and remotely variable by communication from the Back Office.

The frequency of communication of the location information from the DVDMS to the Back Office shall be remotely variable by an authorised user, from every second up to 8 hour intervals.

The location rate of the DVDM device will automatically update to a minimum of 1 Hz, when the emergency warning lights of the vehicle are activated. The

update rate will automatically return to the previous setting, when the emergency warning lights of the vehicle are deactivated.

4.3 Communications

The communication between the DVDMS and the Back Office shall be secure to prevent unauthorised access to the DVDMS or device and/or unauthorised commands being input into the system.

The security for the communication system provided shall be compliant with the current highest standard of commercially available communication security encryption.

4.3.1 Coverage

The communication shall be reliable with a very high coverage across the UK and Europe. Target minimum 98% coverage. The communication system coverage and reliability shall be stated by the DVDMS manufacturer/supplier prior to submitting the system for testing.

The communication methods can include:

- GSM/3G/4G;
- Wi-Fi;
- TETRA; and
- Secure physical connection to the device.

Note: The inclusion of any specific communication method is subject to demonstrating and agreeing suitable security standards with the user community.

The supplier and user should agree the most appropriate and cost effective method for communicating each data type:

- High Priority;
- Low priority; and
- Administration.

The DVDMS shall be capable of automatically sending data via that route.

4.3.2 Communication Performance

Communication between the DVDM device and the Back Office shall be fast, efficient and cost effective for the data or commands it is required to communicate.

The maximum time for communication of a priority message, from the time sent by the DVDM device to being received via the Back Office and forwarded to the appropriate person is 10 seconds.

Where audio/video is fitted as part of the system, the maximum time for transmission of audio-visual signals from the DVDM Device to the Back Office shall be no longer than 20 seconds after being sent from the device to being received and ready to view in the Back Office.

These communication and performance targets shall be achievable whilst the vehicle is travelling at all speeds possible by that type of vehicle.

4.3.3 Communication Update – Emergency Light Activation

Where required by the user organisation, the communication update rate with the Back Office of the DVDM device will automatically update to a minimum of 1 time per second, or other rate as defined by the user organisation, when the emergency warning lights of the vehicle are activated. The update rate will automatically return to the previous setting, when the emergency warning lights of the vehicle are deactivated.

4.3.4 Communication of Driver Profile

The DVDM in-vehicle device, following driver identification, shall be able to receive the relevant driver profile within 10 seconds from communication being established with the Back Office. The communication will normally be established within 10 seconds of the driver identity being confirmed.

4.4 Geo-fences

As part of the normal operation of the DVDMS, the Back Office shall remotely be able to easily create and remove geo-fences.

There shall be simple and quick system to produce geofences which are and variable by location size and form that is in order to follow roads and features such as may be available within mapping systems. They should be capable of being generated for a single vehicle, group of vehicles or all vehicles monitored by the Back Office.

The DVDMS shall require capability to store at least 40 geo-fences per vehicle for normal operation.

4.5 Diagnostics

The DVDMS in-vehicle device shall, when the vehicle is switched on by a new user or within a user defined period from the last check, conduct a pre-vehicle diagnostic check on the in-vehicle device and where it is connected to the vehicle CAN system and the information is available, to report back to the Back Office in real-time, any faults or incorrect levels for:

- Electrical power source capacity;
- Coolant water level;
- Fuel level;
- Brake fluid level;
- Windscreen washer level;
- Tyre pressures;
- Emissions (Exhaust);
- Other vehicle warning lights:
 - Engine management/emissions;

- Brakes; and
- Oil;
- Vehicle overweight – if measured;
- Incident events – not already notified; and
- Faults with Emergency service equipment:
 - MDT;
 - Emergency warning lights; and
 - Emergency Sirens.

These faults shall be prioritised on the basis of safety to drive the vehicle or damage that may be caused.

Where a safety alert is identified, this shall be brought to the driver's attention as a high priority and this information shall automatically be passed as a high priority to the Back Office and then to the person designated by the user organisation to receive such alerts. A lower priority alert may be raised to the driver and then communicated to the Back Office.

The results of this diagnostic check shall be recorded in the DVDM device and transmitted to the Back Office, so that it is able to be viewed by workshops as part of a vehicle report.

4.6 Vehicle Data

The DVDM shall capture, via the esCAN where fitted or from another vehicle OEM approved means all the following data from the vehicle, where this is available or supported by the vehicle manufacturer or other third party.

- Vehicle identity;
- Vehicle fault codes;
- Brakes and percentage braking :
 - Foot;
 - Parking;
- Brake pad sensor warning;
- Pre load braking activated;
- ABS activation and fault;
- ABS switched off;
- Gear selection – manual or automatic:
 - Forward Gear 1 to X;
 - Reverse;
 - Park (Automatic);

- Neutral;
- Driving mode selected Sport or other mode;
- Engine revs, actual and excessive;
- Engine rev limiter activated;
- Engine efficiency;
- Clutch – percentage depressed;
- Accelerator percentage depressed and duration;
- Fuel usage per trip or driving event (Instantaneous and average);
- Steering percentage applied/rotational speed;
- Yaw in degrees;
- Excessive yaw;
- Activation of vehicle horn;
- Road speed (Road speed pulses road/wheel speed);
- Visual road speed displayed;
- Door open by door location (e.g. Right hand front door);
- Tailgate or boot open;
- Bonnet open;
- Ignition position where provided on/off;
- Auxiliary ignition position where provided;
- Engine run times at idle;
- Seat belt (By Position);
- Seatbelt warning light;
- Seatbelt pre-tensioners activated;
- Windscreen wipers (By position);
- Windscreen washers;
- Headlamp washers activated;
- Lights activation;
- Headlight:
 - Main;
 - Dipped;
 - Flash;

- Side lights by Position;
- Daytime running lights;
- Headlight load sensor;
- Fog lights – front/rear;
- Brake lights;
- Turn indicators – by position front rear side. Left right;
- Hazard warning lights;
- Reversing lights;
- Reversing audible warning;
- Interior light by position;
- GPS location information where provided;
- Heading;
- Air conditioning on/off;
- Service warning indicator;
- Vehicle warning lights on/off:
 - Coolant overheating;
 - Engine warning light (engine management);
 - Oil;
 - Brakes;
 - Battery/alternator;
 - Tyre pressure;
 - Fuel;
 - Airbag;
 - Passenger airbag disabled;
 - Stability control or other active safety device/Deactivation;
 - Active braking;
 - Adaptive cruise control activated;
 - Lane departure warning;
 - Collision avoidance activated;
 - Traction control/Deactivation;
 - 4x4 activated;
 - Gearbox warning;

- Vehicle mileage (trip);
- Change of vehicle settings:
 - Suspension;
 - Sport mode;
 - Cruise control on/off set;
- Temperature control;
- Heated screen front/rear;
- Vent air direction;
- Steering wheel controls used by function;
- Vehicle on board computer used by function;
- Mobile phone-blue tooth used by function;
- Vehicle radio/iPod used by function; and
- Others, to be defined.

Each activation shall be linked to a date, time and location. Where fitted, these shall comply with industry best practice and relevant legislation.

4.6.1 Emergency Service Equipment Data

The DVDMS shall capture via the esCAN where fitted or from another vehicle OEM approved means all the following data from the vehicle, where this is available or supported by the vehicle manufacturer or other third party.

- Activation of emergency lights:
 - 360 lights;
 - Rear Protect;
 - Low Power;
 - Cancel all lights;
 - Front blue lights grill/repeaters/dash mount;
 - Rear red lights vehicle/boot/tailgate;
 - Alley lights left and right;
 - Front “take down” lights;
 - Sign or matrix on/off message displayed;
 - Others to be defined;
 - Front blues light bar;
 - Front whites vehicle;
 - Rear reds light bar;

- Rear blues light bar;
- Headlamp flash;
- Amber lights where fitted (Airports);
- Emergency siren By setting:
 - Yelp;
 - Wail;
 - Bull horn;
 - White noise;
 - PA;
 - Other;
- Airwave radio – where linked all functions;
- Police MDT where linked all functions;
- Cameras where linked to esCAN all functions;
- ANPR, where linked to esCAN;
- Digital recorder all functions;
- Run Lock;
- Gun cabinet open;
- Dog cage open by door;
- Prison cell open by door;
- Laptop docked;
- PDA or other device docked;
- Microphone active; and
- Head up display active.
- Others may be defined in future releases of the criteria or by user organisations.

Each activation shall be linked to a date, time and location.

4.6.2 Voice Warnings – Text to Speech

Where voice warnings or text to speech functionality is provided, this shall be tested by a competent organisation to ensure that it is not distracting and complies with European Statement of Principles for HMI and relevant regulations and other best practice in this area.

4.7 Cameras and Audio

One Box DVDMS may include camera and audio to assess the situation inside or around the vehicle. These shall be digital and shall communicate via the installed

One Box SVA system wired LAN, where this is fitted (exceptions may include legacy equipment). Where the data is used for incident investigation or evidential purposes, it should be securely stored on the vehicle until it is no longer required or until it has been confirmed as being successfully transferred to another authorised storage capability.

To that end, the camera installations, wherever about the vehicle they are fitted and utilised as part of the DVDMS, shall meet the following requirements:

- Cameras shall be capable of capturing still or moving images;
- Forward-facing and rear- or side-facing cameras shall be permitted to have different characteristics (e.g. resolution, etc.), appropriate to their intended viewing area;
- Cameras shall operate, without making an audible sound;
- Cameras shall be robust – suitable for use in the vehicle environment (i.e. car);
- Cameras should be capable of remote activation or deactivation only by the Back Office;
- A digital date and time stamp data obtained from DVDM device, including the DVDM device identification shall be placed on all images. As detailed in the following CAST and NPIA publications:
 - CAST publication - Digital Imaging Procedure – HOSDB publication 09/05;
 - CAST publication - Digital Data Standards for Handling – HOSDB publication 58/07;
 - CAST publication - Retrieval of Evidence and production for evidence – HOSDB publication 66/08; and
 - NPIA - Advice on Police Use of Digital Images 2007;
- Cameras shall be capable of operating with the vehicle ignition switched off;
- Cameras should be capable of communicating images and streaming video in real-time to the Back Office or other appropriate viewing location (e.g. police force control room, etc.);
- Where communications have been lost (e.g. poor cellular network coverage, etc.), the system should be capable of storing camera images and video on-board for up to 7 days;
- Where the transmission of data is interrupted, it shall be stored locally and re-transmitted when communications are re-established. Receipt of the data shall be confirmed to the DVDMS;
- Cameras shall be capable of providing images of lawfully and reasonably sufficient quality adequate quality in all light and weather conditions, day and night;
- Cameras should provide images of sufficient clarity to enable the identification of all persons in the field of view to evidential standards;

- Camera image capture rate should be capable of being changed remotely by the Back Office;
- The Back Office should be able to switch remotely between cameras or to view feeds from multiple cameras simultaneously;
- The Back Office should be able to switch between camera operating modes (e.g. still to video, etc.);
- The DVDMS should possess sufficient communication capability to send the images to the Back Office;
- For any installation to police or other Emergency Services vehicles operating with Tetra Airwave radio, cameras shall additionally comply with AES Specification 5;
- Audio shall be capable of capturing all speech in the passenger area;
- The audio shall not be able to be turned off; and
- Audio shall be capable of being captured and stored to evidential standard.

Note: The use of cameras in DVDMS is seen as a significant enhancement to security. In order to maintain public support, it will be essential that One Box DVDMS are operated ethically – that is, within the frameworks of and taking full account of all relevant Privacy, RIPA, Human Rights and Data Protection legislation.

4.8 Virtual Log Book

The DVDMS shall provide a virtual log book capability to provide an automated record of the vehicles use, drivers and drive or other events captured on the DVDMS.

This will include:

- Driver identity;
- Driver identity, where this changes;
- Result of diagnostic checks;
- Bonnet open;
- Date, time, location of driver identity;
- Vehicle start;
- Miles and route driven;
- Date, time and location of end of use of the vehicle by that driver:
 - Journey;
 - End of use;
- Fuel added;
- Faults;

- Collisions or events; and
- Servicing.

4.9 Alert Function

The DVDMS shall be capable of providing a wide range of alerts, when a vehicle or driver exceeds a range of thresholds set by the user. The alerts may be sent to the Back Office to be associated with a vehicle or driver record. They may also be communicated to the driver or where they are a high priority, provide a warning signal, via the Back Office to a user nominated contact point (normally the control room) of a defined high priority alert e.g. crash – over speed – or other high priority alert.

Upon cancellation of the alert by the Back Office, the DVDMS shall automatically return to the monitoring set condition.

4.9.1 Resistance to False Alerts

The components of the DVDMS shall be designed, manufactured, and installed, in such a way as to minimise the possibility of false alerts.

4.9.2 Unauthorised Driver

The DVDMS shall recognise when an unauthorised driver is attempting to start and/or driving a vehicle. This will be recorded as an event and a high priority communication will be sent, via the Back Office to a nominated user for investigation.

4.9.3 Speed Alert

The DVDMS shall be able to determine the accurate speed of the vehicle and where required, shall provide an alert to the Back Office when a preset speed threshold has been reached.

The speed alerts shall include:

- Exceeding a defined threshold speed, no emergency warning equipment activated; and
- Exceeding a defined threshold speed, emergency warning equipment activated.

The speed alert should include:

- Exceeding a posted speed limited by a user defined amount no emergency warning equipment activated; and
- Exceeding a posted speed limited by a user defined amount emergency warning equipment activated.

The system shall be able to easily set variable thresholds above the user defined amount to automatically initiate warnings to the:

- Driver (e.g. Posted speed + 10mph inform driver);
- Supervisor (e.g. Posted speed + 20mph inform supervisor); and
- User nominated emergency contact point e.g. Force Control room (e.g. posted speed +30mph inform control room).

The speed alerts will also be communicated to the driver's profile.

The speed and alert thresholds shall be capable of being changed remotely by an authorised user via the Back Office either on a single, group or all vehicles.

4.10 Incident or Event Detection

All DVDMS shall provide the capability to capture, store, process and where required immediately, communicate to the Back Office data that can be used to investigate an incident or event involving that driver or drivers and that vehicle or vehicles.

This incident or event data may include data as a result of a collision and shall be capable of being stored securely and or separately to other driving events, either in the device or the Back Office, to ensure that it can be preserved and accessed.

The DVDMS in-vehicle device shall note the exact time, date and location where an incident or event began and concluded and this shall be stored with the data.

Note: It is a fundamental requirement of DVDMS that this process shall not be capable of being able to be deactivated by the driver or passenger.

The event or incident data shall have a specific event or incident flag, within the system and when presented to the user designated person(s) to clearly identify that it is a high priority incident or event.

Once an event has been captured, there shall be no means for the driver or passenger to deactivate, unfreeze or alter any incident or event alert or data. (Where the driver or passenger is an authorised person to release or unfreeze data, there shall be a clear separation of access rights to and audit procedures are put in place to prevent misuse of this capability).

The incident or event data including those captured and stored as a result of collisions shall meet requirements set out in this document, so as to be suitable to meet the needs of collision or other investigators, now and in the future.

This includes the requirement for constant monitoring and storing of data, albeit on a time limited basis of data able to be captured as part of the DVDMS. (This requires the ability to capture and store all data on the esCAN and from other data sources that the DVDMS is connected to.

At the conclusion of the event, when the event or incident data has been downloaded, either from the device or to the Back Office, this shall flag as an event or exception report to both the driver and vehicle profile.

The DVDMS shall have a method for a driver or vehicle occupant to identify or bookmark an event and where this is required by the user organisation, a method to do so manually.

4.10.1 Collision or Incident Alert

The DVDMS shall have a capability to monitor and provide an alert where the vehicle:

- Experiences sudden deceleration (suggestion of an impact);
- Roll over; and/or
- Other alert, such as air bag deployment.

Where these alerts are received by the Back Office, they shall be assessed. The subsequent status of an alert shall be decided by the Back Office, according to their operating guidelines and priorities.

The DVDMS will provide an immediate alert to the user organisation designated person(s) of an event or incident that is likely to be a collision. This shall be by an automated process and may allow a manual activation, if required by the user organisation. This will normally be sent to the control room supervisor. Where the user organisation is not an emergency service, this function must comply with the 999 Liaison Committee data handling protocols and existing procedures for handling eCall.

4.10.2 Process for Accessing Event/Collision Data

The DVDMS data shall be made available to authorised personnel for use in an investigation in the event of an incident such as, a crime or road traffic incident, involving an equipped vehicle.

There shall be a clear and easy process for an authorised person, to access or download data relating to an event, incident, vehicle or driver, either from the in-vehicle device or Back Office.

This access shall be able to be securely performed both remotely, via the Back Office and/or from a secure connection to the in-vehicle device.

There shall be a secure physical access point on each in-vehicle device or system to enable an authorised user to securely download or upload data direct from or to that device. The secure connection point should be via a standard hardware and software interface

There shall be a specific access level for collision and other authorised investigators to access all data held on the DVDMS, system, which has an audit trail that covers all access and functions granted and used. This access level will include any incident or event data that is stored or secured separately to other data.

The incident or event data shall be capable of being interrogated, analysed, viewed and compared with other relevant data held on the DVDMS regarding the driver, vehicle, event or incident or location or other relevant parameter. The event or incident data must include and be able to analyse the full list vehicle and emergency service data available to the system.

The data obtained as a result of an incident or event shall be based on open standards or have an open standards output to enable the data to be investigated without the need for specialist software or equipment. This will allow the data to be obtained and analysed anywhere in the country. (This will require the standard to be defined in the future).

The data recorded and stored as a result of the incident or event should be capable of being exported to a nationally and user organisation approved collision or event reconstruction software, to allow the automated re-construction of the event or incident, where this feature is not provided within the DVDMS.

4.10.3 False Incident Alert

Where the event notification is a false alert, this shall be capable of being rescinded by an authorised user remotely, it shall also be possible to do so from/via the in-vehicle device.

4.11 Incident or Event Data Recording Additional Requirements

Where data relating to an incident or an event is captured, this data shall be capable of being secured, to enable it to be used for evidential or investigation purposes. The secured data, which can be in the in-vehicle device or when downloaded to the Back Office, shall not be overwritten until it has been released or extracted by an authorised person.

Where the system is able to secure data by manual activation of a book marking/ flagging capability from an in-vehicle device, this will secure a user organisation a time defined set of data before and after the activation. (Current best practice is to store at least 45 seconds before and 15 seconds after the activation of the device, to a non volatile memory).

In the event of an incident or collision involving the equipped DVDMS vehicle, the data held on the DVDM device within that vehicle shall be protected and preserved before, during and after that incident or collision, so that it is available for post event investigation or analysis or until it has been securely downloaded to the Back Office.

The DVDMS shall have a simple and auditable process for an authorised user to release/change the status of secured (data held specifically relating to that incident by a manual or automatic process) data following an incident or event to a non secure data, so that it can be managed as per any other DVDMS data. This would normally be used to remove the requirement to keep data e.g. where an incident is false or minor.

4.11.1 Data Recording Frequency

The DVDM device shall be able to record data from the esCAN and other linked devices at 80Hz, where it is available at this speed for event data recording and 1HZ for journey data recording, where the data is provided by the host system to this speed.

4.11.2 Driver Notification

Where an event or incident is recorded, the DVDMS shall immediately notify that driver and subsequent drivers that an event or incident has been recorded, until that alert notification is cancelled by an authorised person. (Subject to compliance with the European Statement of Principles for HMI 2008)

The DVDMS shall have a way of notifying the current or subsequent driver that an event has occurred with that vehicle that has not been cleared by an authorised person.

This may be way of a signal:

- Light; and/or
- Audio

Other means may be agreed with the user organisation.

5 Data Requirements

The DVDMS in-vehicle device shall store all of the data it is capable of receiving on the device for a period of 14 days of continuous use at all times. This period may be reduced only where the data has been sent to the authorised Back Office and the Back Office has confirmed to the device that the data has been received correctly.

All data captured, stored, used or accessed by the DVDMS or its users, shall be appropriately stored, managed and utilised to comply with the relevant legislation, policies, procedures or best practice relating to that data or information.

5.1 Data Categories

The DVDM in-vehicle device shall be able to automatically recognise different data categories when they are received, captured and store them according to that data category in the device. The categories and quantity stored in the device shall be configurable by an authorised user.

For and within each data category, either the category of data or data within a given category shall be given a priority for action and communication.

- High priority – immediate action and or communication
- Medium priority – action and/or communication by the most appropriate means, at the most appropriate time
- Low priority – action and/or communication at the most appropriate time or by the most cost effective means
- Not to be actioned or communicated but stored until overwritten.

The DVDM in-vehicle device shall be able to automatically communicate defined categories of data to the Back Office, as required by the user, given the relevant priority and type of data in each category.

5.2 In-Vehicle Data Storage and Retention

Data categories that are not required to be downloaded by the DVDMS and are not subject to being secured event or incident data as defined in section 4.11 may be overwritten after minimum of 14 days or other longer authorised, user defined period when the available storage capacity has been reached. (NB: the requirement is for the system to be sized to store the data for the minimum period. The capacity reached allows data to be stored for longer on a device, before over writing.)

The data collected and stored by the DVDMS must be captured, stored and communicated to evidential standards and quality.

On-board data storage should conform to ACID rules (Atomicity, Consistency, Isolation and Durability). That means that each transaction must be:

- Atomic – it is one unit of work and does not depend on previous and following transactions;

- Consistent – data are either committed or rolled back with no possibility of an “in-between” case where something has been updated and something has not;
- Isolated – no transaction sees the intermediate results of the current transaction; and
- Durable – values persist if the data had been committed even if the system crashes right after.

5.3 In-Vehicle Data Security

Data should be encrypted, particularly if it is stored on removable storage (memory cards). A number of encryption standards exist, some of the most common being Data Encryption Standard (DES) and its more secure successor DES3.

5.4 Data Capture

The DVDMS shall be able to capture, record, store and communicate to the Back Office, all data associated with the beginning and end of a drive event. A drive event begins with an engine start and concludes with the engine being switched off for more than 30 seconds, unless fitted with an automated engine start/stop system.

The DVDMS shall automatically communicate the agreed categories of data associated with a driver or vehicles use of a vehicle and or drive event to the Back Office, where it will update the relevant vehicle and driver records and profiles.

5.5 Benchmarking

All data and information shall be able to be used for comparison and benchmarking with other systems.

5.6 DVDMS Data Communication

The DVDMS shall be able to communicate information to:

- The driver;
- Supervisor;
- Emergency service control room; and
- Other person or systems nominated – e.g. fleet staff, other computer based system or Back Office.

Communication with each shall be according to the priority of the data/information and the route and time for communication agreed with the user organisation.

The data shall be communicated by the most effective and efficient means, to achieve the required outcome, according to:

- Priority;
- Category; and

- Volume.

This will include using a range of communication bearers:

- GSM, 3G, 4G, GPRS;
- TETRA;
- Wi-Fi, where permitted;
- Direct download; and
- Others to be defined by the user organisation

These may be provided individually or in combination, as agreed with the user organisation.

Where the data is communicated via one or more of the means above, the DVDMS shall confirm receipt of the full data content and integrity. Where this does not occur, the data communication will be repeated until confirmation of receipt of the data is provided.

Where local infrastructure or geological surroundings cause loss of communications, vehicle and data shall be stored and transmitted when communications are re-established.

5.7 Communication In-Vehicle

Where the data is communicated to persons in that vehicle, it shall be capable of being communicated via one or more of the following:

- A dedicated DVDMS device or screen;
- An OEM or aftermarket device or screen (e.g. MDT);
- By audible or visible alert; and/or
- Haptic alert – e.g. vibration.

6 Driver

6.1 Driver Interaction

Where the driver is required to interact with the DVDMS in a moving vehicle, all such interactions shall ideally be hands free, comply with best practice in Human Machine Interface and comply with the guidance in the European Statement of Principles for Human Machine Interface 2008 or later versions, as this document is amended.

Where the driver fails to act on the information provided, the DVDMS will repeat the information, until the reason for communicating the data/ information has concluded. This will be logged as part of the audit trail

The HMI requirement also applies to all other communication between the DVDMS Back Office and users, to include:

- Text;
- Voice;
- Audio;
- Visual;
- Screen display; and
- Other communication.

The HMI requirement shall apply to the following categories of communication:

- In-vehicle;
- Mobile device; and
- Office-based system.

6.2 DVDMS Driver Identity

The DVDMS shall uniquely identify and recognise (authenticate) the driver of the vehicle, before and during that vehicles use and link all activity to that driver and vehicle identity, in both the vehicle and Back Office. The DVDMS may also identify the passengers and link this to the vehicle.

The action required for the driver to identify themselves to the DVDMS shall be simple and easy to use.

The action may be either a passive or active operation.

The driver/passenger shall be identified by either, a coded signal or a coded key to the system or other approved system for vehicles, used by multiple drivers that achieve the criteria requirements.

The DVDMS shall confirm to the driver the acceptance of their driver identity. This can be visual, audible, or haptic.

6.2.1 Driver Identification

The DVDMS driver identification token shall be separate from the ignition key.

The DVDMS driver identification token shall be made in such a way as to:

- Make it difficult to attach the driver identification token to a key ring holding the vehicle ignition key, or
- Enable the automatic setting of the functions of the DVDMS, without the need for additional conscious or deliberate actions by the user

It shall not be possible to identify the driver to the DVDMS, without the acceptance of the specific valid coded signal, key or other approved system for vehicles used by multiple drivers.

Each individual driver shall be identified to the DVDMS only in response to a specific coded signal or identification token meeting these requirements. All other codes or identities shall have no effect. There shall be no universal or generic code or identity for a specific type of DVDMS.

There shall be no security override or low security un-setting function for the DVDMS.

There shall be no permanent external visible indication of any driver identity code on any component of the DVDMS.

The range of combinations of the driver identity code shall be evenly or randomly distributed throughout a normal serial production run of the DVDMS.

The programming of the DVDMS to accept additional or different driver identities, driver identity codes or control units, shall be carried out by a secure programming procedure by:

- The input of a combinational action,
- Personal identification number (PIN) specific to the vehicle controlled by the user;
- The manufacturer on a secure database;
- Providing secure user details to the manufacturer;
- The use of a special master driver identity programming procedure; or
- A combination of the above meeting the normal un-setting security requirements.

It shall be possible to exclude existing valid identities [including alternative (emergency) driver identity codes] from the DVDMS by a procedure which can be executed at low cost to the user. This may be a programming procedure or may require the changing of the DVDMS components.

Programmed driver identity code information shall not be erased in the event of a supply voltage interruption of the DVDMS or the driver identity.

Automatic reprogramming of the DVDMS to accept additional driver identities upon the reinstatement of supply voltage to the DVDMS shall not be permitted.

It shall not be possible to damage the DVDMS by shorting together any terminals on a normally accessible socket or lock. It shall not be possible to

damage the driver identification token by shorting together any normally accessible terminals on the token.

Note: The driver identification token must in no way interfere with the operational use of that vehicle or immobilise the vehicle unless specifically required to do so by the user organisation.

6.2.2 Wireless Driver Identification

The DVDMS driver identity code protocol shall provide for the following:

- Resistance to code copying followed by trial of codes, by providing changing codes.
- Resistance to interrogation of changing code algorithms with a personal computer, followed by trial of probable codes.
- Resistance to sequential trial of codes by providing an adequate number of code combinations and code acceptance rates.
- There shall be a minimum of 50,000 code combinations.
- The minimum duration to sequentially scan through 5000 codes shall be 24h. All codes shall be repeated no more frequently than every 5000 key operations.
- It shall not be possible for the driver identification token to identify to the DVDMS by retransmitting in any sequence the previous 5 codes generated by a legitimate key.

6.2.3 Driver Identification Methods

The following methods of driver identification are permitted:

- Electronic or electrical direct connection;
- Proximity sensor;
- Combinational action (PIN); or
- Keypad.

There shall be a minimum of 10,000 code combinations.

The minimum duration to scan through 5000 codes shall be 24 hours.

Additional requirements for keypad and combinational action (PIN) controls are set out below.

The PIN controls shall:

- Have buttons or controls which shall not mark readily, such that unauthorised identification of a current code is prevented;
- Be operated only by a deliberately entered code of a minimum of four decimal digits or equivalent;
- Have codes freely assignable by the user (excepting any alternative (emergency) unsetting control code which may be fixed or freely assignable); and

- Incorporate an automatic alarm function following the input of 3 incorrect codes (or equivalent security level) prior to accepting further codes.

6.2.4 Mechanical Driver Identification

The use of mechanical driver identification is not permitted.

6.2.5 Multi-driver Vehicles

Where a vehicle is used by multiple drivers and it can be demonstrated that the above methods would significantly reduce the functionality of the vehicle or where, through deliberate evasion or work rounds, the users circumvent the intended security, alternative methods of set/unset will be considered that provide the desired security and functionality is maintained. Before such a method is approved, it must demonstrate and be independently tested to show that it meets at least the same or ideally higher levels of physical and/or electronic/communication security as the above methods and approved by the accredited test house and CAST.

7 Back Office

7.1 General

The main role for the DVDMS Back Office is to securely and accurately receive data from all of the equipped vehicles, relating to that vehicle and its use and/or data relating to the driver of that vehicle, associated with their unique driver identification. This data will then be automatically processed into information, to enable the user organisation to better manage the use of its vehicles and to manage and improve driver behaviour, through:

- A series of automatically generated reports, a number of which are listed in these criteria;
- The capability to run generic or bespoke searches against the data held, a number of which are listed in these criteria;
- The capability to develop new reports or searches, as required by the user organisation; and
- The capability to produce detailed reports relating to incidents or events, to include the ability to drill down to very low levels of data where required.

The reports shall be automatically generated and the appropriate reports forwarded, automatically to the correct driver, supervisor or other relevant person at the time and frequency agreed by the user organisation. This is fundamental to delivery of the benefits of the DVDMS, namely:

- Improving driver safety;
- Improving driver behaviour; and
- Reducing costs.

The information and data held on the system will also need to be made available to supervisors and other authorised personnel to allow them to make better informed decisions or to assist discussions with a driver as to:

- A drivers suitability to drive or continue to drive a particular type of vehicle;
- Their driving behaviour;
- To support an investigation of an incident or an event;
- A requirement for additional or remedial training; and
- Their suitability for more advanced driver training.

To achieve this, the Back Office system will be required to automatically process and analyse all driving, vehicle and driver and other relevant data held in that Back Office related to:

- A driving event;
- Trends;

- Vehicle usage; and
- Driver behaviour.

7.2 Link to other Databases

The DVDMS Back Office shall be able to link to other user organisation systems, e.g. personnel, command and control, GIS, crime etc, where required by that user organisation and where it is feasible to do so.

The DVDMS Back Office should be able to link to external live or historic information sources, where required by the user organisation, e.g. weather, traffic conditions etc.

The DVDMS Back Office shall be capable of being linked to and operated on the Police National Network (PNN) or its replacement, which includes the requirement to comply with all the security requirements and operating procedures to do so.

7.3 Updates and House Keeping

The Back Office software shall be able to be easily and cost effectively modified to take account of new driving legislation, procedures or best practice or other changes relevant to the operation of the DVDMS.

All maintenance and housekeeping functions for the Back Office shall comply with relevant legislation, best practice and be consistent with the user organisations procedures for other systems.

7.4 Back Office Sizing

The DVDMS Back Office shall when introduced be appropriately sized, to include:

- Processing capability;
- Data storage;
- User access; and
- Number of vehicle or driver profiles held.

This is so as to ensure all reasonable future use is met over the expected life of the system.

7.5 Disaster Recovery

The Back Office shall have full disaster recovery procedures to include independent power supplies, such that following an incident full operation can continue or be taken over by another competent body within 15 minutes. This handover should be tested according to the requirements of the user organisation. This facility is required to provide system operation at all times.

Where a DVDMS is combined with a vehicle immobilisation capability which requires the correct driver identification token to start the vehicle, this shall be achieved in a way that is not impacted by any disaster recovery procedures.

Note: It is not acceptable for police vehicles not to be able to start due to issues with the Back Office.

7.6 Back Office Database

Each Back Office will be required to keep an accurate database of all the DVDMS devices and drivers, vehicles other stake holders relevant to the operation of that system. Any changes to information on this database must be updated within 30 minutes of being received by the Back Office.

There shall be a process for an authorised user to either, manually or automatically add, update, amend or delete any record (driver or vehicle) held on the live system, subject to audit, legal and storage requirements. (See audit and retention requirements section 7.8.2.)

The DVDMS shall have a means for a suitably authorised user to remove or restrict access by another user to all or part of the DVDMS.

The Back Office shall have a system for deleting driver and vehicle related data, when it is no longer required to be retained by the user organisation, subject to the legal and audit requirements. This process should be an automated process but may have a manual process to enable deletion and correction of errors from a vehicle or driver profile.

Note: Where this correction occurs, a full audit trail will be kept and the deleted data will be retained in a file linked to the driver or vehicle profile, which will be capable of being accessed by an authorised person if required, until the legal or audit retention periods are met.

7.7 Freedom of Information Act Requests

The DVDMS Back Office shall have a search and report capability to support the administration of freedom of information requests, which may require specific searches of data held on the system.

7.8 Data Access Security

The DVDMS Back Office shall only be able to be accessed by authorised person(s), nominated by the user organisation. The DVDMS Back Office shall uniquely identify and authenticate each authorised person.

The DVDMS Back Office shall be a secure system and have a range of secure access levels, which controls access to data and search functionality to ensure access to any data, information and reports, are appropriately protected and secured in accordance with the relevant legislation and practices and policies of the user organisation.

The access levels will only allow authorised users to access the data, reports information that they are entitled to access. This applies to the in-vehicle device and the Back Office.

7.8.1 Data Security

The DVDM device and Back Office must be appropriately protected and secured for the level of data held by that part of the system. This will be defined in agreement with the user organisation and governing legislation and best practice.

The DVDMS user organisation must have in place practices, policies and procedures that properly control access and use of the data, reports and information held on or produced by the DVDMS, to include:

- Access;
- Printing;
- Down loading;
- Copying; and
- Version control.

The test house shall ensure that the supplier instructions clearly include this guidance.

7.8.2 Back Office Audit Data

The Back Office is required to capture and securely store for a period of 7 years an audit of:

- All log transactions with time date and identities to include Back Office operator;
- All data transmitted to or from Back Office;
- All alerts;
- All actions or commands;
- All faults;
- All alarms; and
- All service requests.

The Back Office will be required to produce this information and data as evidence, when lawfully required by the emergency services.

7.9 Back Office Drive Events

The Back Office shall be able to capture all drive and/or journey event data communicated to it by the DVDM device in the vehicle, from start to finish of that drive event, to include, where a vehicle's engine is stopped and started with a time resolution of no more than 30 seconds, on one or more occasions during that drive or journey and store the relevant parts of that data in:

- A unique record for that specific and identified vehicle; and
- A unique record for that specific and identified driver.

This will include:

- Vehicle identity;
- Start and end location;
- Time and date;
- Driver identity;

- Diagnostics checks for that vehicle, where available;
- Journey details with location updated at the user defined frequency;
- All alerts notified/identified with location, data and time information;
- All events notified/identified with location, data and time information;
- Speed information, at user defined periods or at user defined change thresholds;
- Average fuel consumption for that journey;
- Fuel used;
- Mileage;
- Harsh Braking;
- Harsh Acceleration;
- Activation of Active safety systems;
- Excessive G force – indicating collision or yaw;
- Harsh steering;
- Excess Revs;
- Idling time:
 - Per event; and
 - Total for journey; and
- Other data, as defined by the user.

The DVDMS will be able to link driver and vehicle records to allow analysis, comparison and reporting by:

- User defined groups of vehicles; and
- User defined groups of drivers.

This will allow association of vehicles and drivers by:

- Specific driving parameter (e.g. grade of driver);
- Individual driver;
- Driver hours;
- Team or group of drivers from section – force;
- Geographic location (station, division, etc.);
- Individual vehicle (make and model);
- Vehicle type (e.g. Traffic or Response vehicle);
- Vehicles by team or location;

- Vehicles by organisation;
- Vehicles compared across several organisations;
- Specific vehicle related parameters:
 - Fuel usage;
 - Mileage;
 - Vehicle usage;
 - Fault code(s);
 - Location;
 - Speed – (max/min/average);
 - Collisions;
 - Utilisation;
 - Servicing;
 - Emergency v normal patrol driving;
 - Activation rates for emergency warning equipment; and
 - Other to be defined.

7.10 Driver Performance

Categorising a driver's performance is another key feature of the DVDMS. Whilst it is relatively easy to define a scale for categorising performance, the conditions that sit behind this category can be complex. The following section will provide, as far as is possible, the grading system, method for assessing performance and guidance on the conditions to grade performance.

The DVDMS shall continually compare driving performance, behaviour and vehicle usage against the performance measures, for both normal and emergency driving thresholds and communicate that information according to the priorities set out early in the document; emergency – slow time and these shall automatically update the driver and vehicle profiles, records and reports.

For each of the categories below, there will be two thresholds set:

- Normal driving; and
- Emergency driving.

The parameters measured will be the same; however the user organisation shall be able to set different thresholds for each, driving or vehicle parameter for each driving type (e.g. higher for emergency driving).

For example a user organisation may expect to achieve 40 MPG during normal driving but only 35MPG during emergency driving.

When calculating driver performance each for each type of driving, the target figure above would be used as the basis of calculating that driver's performance.

7.10.1 Performance Grading

The grading of performance will be based on the following scale. The following grades and colour definitions will be used in all reports:

Silver	top 10% performance
Green	55 – 89% performance
Amber	16 – 54% performance
Red	0 – 15% performance

Table 1 – Performance grading colour scheme to enable performance to be assessed at a glance

Other values may be used, as defined by the user organisation.

7.10.2 Variance from User Defined Figures

Performance against each DVDMS data parameter measured will be defined as variance + or – from a user defined figure. An example is shown in the picture below for Miles per Gallon (MPG) for a range of vehicles.

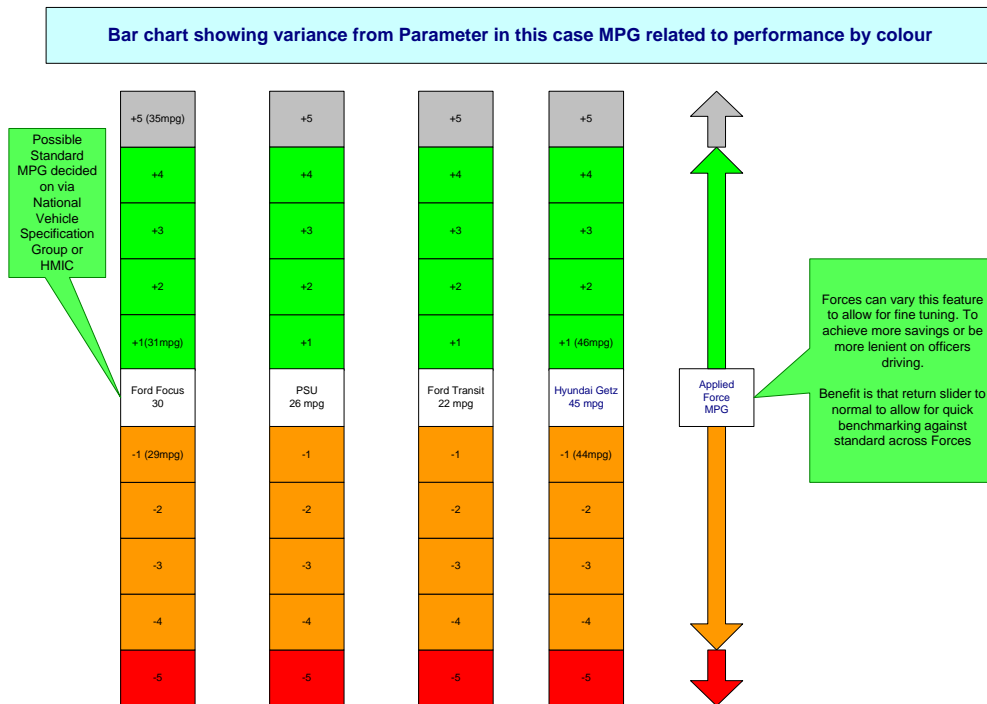


Figure 3 – Bands showing fuel consumption performance for specific vehicle types

This method allows the user organisation to define, in this case MPG for each vehicle type for both normal driving and emergency use. The user organisation may, for example accept a lower MPG figure or harsher steering when on an emergency response than would be acceptable in normal driving.

The same would apply parameters such as maximum speed, braking etc. The user defined figure would allow a driver’s use of different vehicle types for the same parameter e.g. fuel usage (MPG), to be compared on the basis of variance.

This will also require the DVDMS to allow the setting of parameters for each vehicle type for normal and emergency use and the capability to allow an authorised user to change the value in these parameters, subject to an audit trail.

7.10.3 Excess Threshold Events

The Back Office will analyse the available data in the Back Office, together with each new driving event or record communicated to it from a DVDM device and update both the vehicle and driver record and profile. This will be then used to automatically categorise and update performance, using the above categories for all related reports and profiles.

The One Box consortium and or CAST may produce additional guidance to define what constitutes an event and how multiple events shall be handled. This will be published, once completed.

7.11 Informing or Warning the Driver

The DVDMS shall warn the driver when their performance is at or below an acceptable standard.

This warning shall be in real-time through an in-vehicle device, subject to compliance with HMI requirements (European Statement of Principles and other best practice).

Other than for those that are safety critical, these warnings shall be able to be switched off by an authorised user if required.

Priority communication to a control room or supervisor shall be possible for communication to the driver where this is a safety issue.

Note: Neither the driver nor any unauthorised person shall be able to switch off the DVDM device in the vehicle or so configure it that it cannot communicate with the Back Office.

Less urgent warnings shall be communicated in slower time to the driver via the following means:

- Reports;
- Email;
- Text; and/or
- Or other feedback mechanism.

The DVDMS shall also automatically notify the driver and where previously notified, the control room or supervisor, when their driving has returned to an acceptable level. This will all be recorded in the Back Office, as part of the audit trail and driver records.

7.11.1 Driver Feedback

Where a driver is driving below the required standard, the DVDMS shall automatically identify which areas are below that standard and provide advice, guidance, tips and hints as to how the driver can improve. The driver's progress should then be monitored over the next user defined period to review progress.

This driver feedback shall also be available to supervisors and driver training as they may wish to provide additional guidance or training input.

The DVDMS will require the user to acknowledge the receipt of this feedback, which will form part of the audit trail.

7.11.2 **Warning of Outside Safety Thresholds**

One of the aims of the DVDMS is to provide the capability for the user organisation to change driver behaviour, manage vehicle usage and create the capability; where possible to intervene before an incident or collision occurs.

Whilst it is recognised that it will not be possible to recognise all characteristics or behaviours that would indicate a higher probability of an incident, there are a number of parameters that indicate a higher or significant risk.

These may include:

- Exceeding a maximum speed threshold (e.g. 100mph);
- Exceeding a maximum speed threshold in a given location (e.g. 50mph in a 30mph limit);
- Exceeding a maximum speed threshold without the use of warning instruments (e.g. 90mph no blue light);
- Multiple incidents of harsh braking within a single journey or per user defined time;
- Multiple incidents of harsh steering within a single journey or per user defined time;
- Activations of ABS within a single journey or within a user defined time;
- A combination of ABS, traction control and stability system simultaneously;
- Outside of user organisation defined area;
- Activation of emergency equipment outside user organisation defined area;
- Exceeding the speed limit by more than 10% + 2mph (or as specified by ACPO) outside of the user organisation defined area;
- Others to be defined.

(This may be subject to an additional report developed by the One Box consortium and CAST.)

The user organisation shall also be able to set maximum thresholds for parameters that are defined as indicative of potential safety issues.

Where these thresholds are exceeded, they will be recognised by the in-vehicle DVDM device, prioritised as a high priority and communicated as a high priority message to the Back Office for immediate communication to a user defined person. (Normally the Emergency Service Control Room but this may also include the driver's nominated supervisor).

7.12 Driver Categories

The DVDMS shall place each vehicle and driver into a user organisation defined driving category. This driving category will define those vehicles a given driver is entitled to drive.

When a driver identifies themselves to the DVDMS in the vehicle, the DVDMS will automatically compare the driver category with the vehicle category. Where this is within a permitted category, this will be logged.

7.12.1 Unauthorised Driver

Where the driver does not have a driving authorisation to drive that vehicle, this shall be:

- Raised as a high priority alert to a user organisation nominated person, normally the emergency control room or drivers supervisor.
- Flagged as an alert on the driver's profile

OR

- Where the user organisation has required the functionality to be activated, the vehicle may be prevented from starting or activating the emergency equipment.

Where the driver is regarded as a Basic driver or has restrictions placed upon them by the user organisation in the use of that vehicle, for example, a Basic driver may not be permitted to switch on emergency warning equipment, whilst moving or exceeding any speed limit. The DVDMS shall monitor the use of the vehicle and its equipment, in accordance with the conditions of the driver's authorisation. Where the conditions are breached or a threshold exceeded they shall be:

- Where this is a safety issue, raised as a high priority alert to a user organisation nominated person, normally the emergency control room or drivers supervisor;
- Where it is not a safety issue raised as an alert to the driver's supervisor; and/or
- Flagged as an alert on the driver's profile.

Table 2 gives an example of driver permit and vehicle categories, which would need to be customised for each Force or user group. This may be different in each user organisation.

Another option for the categorisation of vehicles, where the user organisation requires it, is to use the National Association of Police Fleet Managers, vehicle categories.

Group	Vehicle type
1	Traffic car
2	Traffic motorcycle
3	Incident car
4	Plain car high performance vehicle
5	High performance motorcycle
6	PSU/Personnel carrier
7	Personnel carrier/small vans non PSU
8	All terrain vehicles
9	Section vehicles (beat or marked cars)
10	Motorcycles (other)
11	Trial motorcycles
12	Cell/Command vehicles
13	Any other vehicle

Table 2 – Driver and permit categories

7.12.2 Removal of a Driver Category

The DVDMS shall allow a suitably authorised person to add, remove, delete or suspend a driver or vehicles category. Where this occurs, any use by a driver of a vehicle category they are no longer authorised to use, will be dealt as for any other breach of this condition.

7.12.3 Driver Profile and Vehicle Profile

The DVDMS shall create a unique driver and vehicle profile for each driver and vehicle. The driver and vehicle profile are a set of vehicle or driver related parameters that have been defined by the DVDMS to be updated by each drive or vehicle usage event.

7.12.4 Normal and Emergency Driving

The definition of normal and emergency driving will always be subjective. There will always be examples of where a member of staff is required to lawfully make use of exemptions to Road Traffic law in order to carry out an emergency service purpose, where emergency service warning equipment (Blue or Red Lights and/or Siren) are not activated.

However, for the purposes of the DVDMS criteria, Emergency use of a vehicle shall be defined as the operation of a vehicle with the emergency warning equipment (Blue or red lights and/or siren) activated.

The DVDM device shall recognise when the vehicle is being used in emergency mode, by the emergency warning instruments being activated, and automatically record this as an event in both the driver and vehicle profile.

7.13 Vehicle Profile

The vehicle profile will include the following information:

- Vehicle usage;
- Vehicle category (driving permit);
- Vehicle fuel consumption;
- Fuel used by user defined period;
- Vehicle mileage;
- Performance parameters;
- Harsh braking;
- Activation of emergency warning equipment;
- Time driven when emergency warning equipment activated;
- Drivers who have driven a vehicle within a user defined period via activation of driver identification token;
- Vehicle faults:
 - Servicing;
 - Engine management lights; and
 - Not available for operational use;
- Time on high demand driving when not on emergency warning equipment (defined as over 80mph);
- Times for normal driving; and
- Others to be defined by the user organisation.

7.14 Driver Profile

The driver profile will include the following information:

- Unique identity;
- Driver training;
- Vehicle categories permitted to drive;
- Driver history:
 - Sanctions;
 - Events; and
 - Driver performance;
- Harsh Braking/Steering;
- MPG variance – performance;

- Incidents/events;
- Alerts;
- Safety related incidents by type as listed at section 7.11.2;
- Hours driving;
- Vehicle usage by:
 - Vehicle identity and type;
 - Day date time duration;
 - Locations;
 - Mileage;
 - Emergency usage; and
 - Other factors as defined in section 7.13 above.

7.15 Fleet Management Requirements

Meeting the requirements of the fleet management stake holders is a key part of delivering DVDMS.

In addition to any reports elsewhere in this chapter, the DVDMS shall be able to produce when required by an authorised user the current status of:

- All vehicles; or
- User defined groups of vehicles from the user fleet showing their current location, on a:
 - Map; and/or
 - Report.

This map and/or report shall show any outstanding or current alerts, as defined by the user.

The DVDMS shall also be able to provide a report, when required by an authorised user, showing the current status of:

- All drivers; or
- A user defined group of drivers listed on the DVDMS with as a minimum the list of drivers with:
 - warnings;
 - events; and/or
 - poor performance.

7.15.1 Workshops

An authorised workshop user, shall be able to download all data or user-identified categories of data from the in-vehicle device and/or the Back Office

and have the capability within the DVDMS or Back Office to generate vehicle or other user defined reports as required by these criteria.

7.15.2 Servicing

The DVDMS shall provide a means of identifying and displaying a vehicles service schedule, by date or mileage and or time from last service and when the next service is due.

The DVDMS should be able to automatically inform the relevant driver/user that a vehicle is due for service. This should be by a user nominated communication method, which may include text or e mail.

The DVDMS shall identify when a vehicle is not available for operational use, to include its location, date and time when taken out of availability for operational use (e.g. within a service centre), all subsequent movements and events and the date, time and location of when it was available for operational use. This status and times shall be added to all relevant reports and the vehicle profile.

The DVDMS shall also be able to identify how long a vehicle is in workshops for service or other repairs and be able to report on this, when required. The DVDMS should warn a nominated person from the user organisation, when a vehicle has been out of service for user defined and user configurable period. This notification should be by way of an alert and through a report (see section 7.17).

7.15.3 Management Information

The DVDMS Back Office shall, where possible, be capable of being linked to other authorised DVDMS Back Offices, to allow comparison, exchange, or benchmarking of data. Where this is not possible or required by the user organisation, the DVDMS data/information/reports shall be capable of being produced in a format that allows direct comparison, analysis and benchmarking with other DVDMS users to include, both paper and data outputs.

The Back Office shall be appropriately registered under the Data Protection Act.

7.16 DVDMS Back Office Reports

The DVDMS standardised generic reports have been developed by the ACPO ITS team, following extensive research and discussion with a wide range of stake holders. The standardised generic reports have been subject to extensive feedback from the users and reports from suppliers that are compliant with DVDMS are expected to be closely similar across the country, to ensure and facilitate benchmarking and fair and equal treatment.

Whilst it is acknowledged that the reports will change over time, this section of the document sets out the broad style, content and user interface for these standardised reports that is expected from all DVDMS.

Minor derivations to the reports may be permitted but accredited test houses will be required to assess compliance with these reports. All derivations will have to be evidenced to show added value. Where this added value is proved to be significant, this may result in changes to the report style in the criteria, which require all future reports for all DVDMS to be of a similar style. This process is essential, to ensure that there is consistency of approach across the country and that the criteria do not become redundant through mission creep.

Note: All suppliers submitting DVDMS for testing that are producing new reports or derivations to standardised reports, before they are accepted for use on the system, must agree to the use of their reports style, content and user interface by the Test Authority to develop future standardised generic DVDMS reports as part of a revised criteria document.

The DVDMS reports will include information displayed as:

- Charts;
- Graphs;
- Tabular;
- Icons;
- Comparisons;
- Written reports; and
- Recommendations.

They shall be capable of being produced automatically. They shall also be capable of being generated manually by an authorised user.

The reports shall be capable of being sent to the relevant authorised user by:

- Text message;
- Email;
- Print out;
- Direct access to the Back Office;
- Web access to the Back Office; and/or
- Other method as required.

The reports shall be capable of being sent automatically to the defined recipients at a time, communication method and frequency as defined by the user organisation, according to the priority of that information, where applicable or where permitted by the user organisation at a time or frequency set by an authorised user.

These reports shall be sufficiently detailed to allow the driver or supervisor to easily and quickly identify driving or certain aspects of driving are above or below the expected standard and will also provide advice and guidance as to how compliance with the expected standard can be achieved.

7.16.1 Costing

The vehicle and driver reports shall be able to have data added to them to provide data on:

- Costs;
- Fuel;
- Servicing;

- Mileage;
- Emissions/ CO2;
- Damage;
- Third party costs; and
- Other parameters to be defined by the user organisation.

7.16.2 Driver Reports

The aim of the driver report is to provide the driver with a clear and easy to understand report that describes their driving performance over time. An example of a driver report is produced below.

The report contains the driving parameters on the vertical axis and time on the horizontal axis. The report shown below is in months, the actual time periods shall be user organisation configurable to include:

- Days;
- Weeks;
- Months; and
- Years.

The number of time periods shown in the report is 5. This should be regarded as the minimum for this type of report. Each parameter is scored by colour as defined in section 7.10.1.

This report shall be sent to the driver automatically, at a frequency set by the user organisation and by a means agreed by the user organisation. This is normally expected to be by email.

The report shall only be sent to the driver and can only be accessed by other authorised users, normally the driver's supervisor or other person in the command chain.

Driver Profile – PC Adrian Smith 101111					
	October 2010	November 2010	December 2010	January 2011	February 2011
Excess Speed	3	4	20	25	10
MPG	0	0.5	5	8	1.5
Excess Brake	0	0	6	4	2
Excess steer	0	0	0	0	0
Idle	0	0	3	0	1
Wrong Gear	4	0	7	8	2
Use	0	0	0	0	0
Speed to gear	3	1	7	7	0
Incident	0	0	0	0	0
Harsh accel	4	2	20	25	6
Over rev	4	1	20	20	6
Warning light	0	0	3	3	0
Mileage	0	-10	-3	-6	-8
Blue Light	0	0	10	15	2

Figure 4 – Example of a driver performance profile

This report will clearly identify at a high level how the driver is performing and how that trend is changing over time.

Sitting beneath this high level report, the driver/authorised user will be able to access more detailed information about their driving behaviour over a range of time periods. This should be achieved by a simple means, ideally by clicking on an information item to drill down to the next level. It shall also be possible to reach this next level, via a simple series of search requests or pre-prepared reports.

The reports below are examples as to how these reports should be prepared. They include additional detail of the vehicles driven, identify where driving falls below the acceptable standard. This will allow further drilling down to an individual vehicle for a particularly time period and identified parameters to enable the driver or supervisor to identify where the driving behaviour is good or needs improving. Both the vehicles, time periods and parameters shall be customisable by the user.



Figure 5 – Various different types of Driver Report that can be made available

The final report shown above details tips and hints to improve the driving behaviour. The content of this shall be agreed with the user organisation to ensure it is applicable to local practice. The report shall define the target improvement required and should provide guidance as to the economic or other impact of the behaviour. At the driver level it is preferred that this is described in non monetary value, for example converted to a number of people that could be saved if the behaviour improved.

This information shall also be provided on a map detailing a specific drive or event, showing the time, date location and route of the driving event and where the driving exceptions, incidents or events occurred.

The final report in these examples is a monitoring report that monitors the driver’s performance over time against the specific parameters that require improvement.

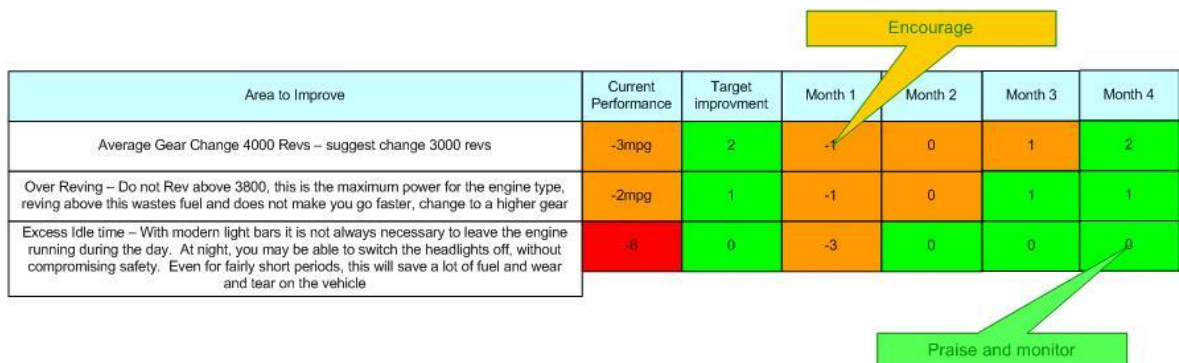


Figure 6 – Driver report, highlighting areas for improvement

Again all fields for times and parameters are customisable. These reports are intended to support drivers and supervisors to monitor improvements.

7.16.3 Level 1 Supervisor Reports

This report is intended to provide first line supervisors an overview of the driving performance of the team or staff they are responsible for. The team or staff group is shown on the vertical axis.

The driving parameters are shown on the horizontal axis and the fields are automatically completed with the driving performance for that parameter for that individual for that time period.

The report shown below shall be user organisation configurable to include:

- Days;
- Weeks;
- Months; and
- Years.

This report shall be sent to the supervisor automatically, at a frequency set by the user organisation and by the means agreed by the user organisation. This is normally expected to be by email. This report is only available to the supervisor for that team or staff and those at a higher level who are authorised to see this report for those staff.

On the right hand side of this report, the drivers are rated by user organisation configurable categories. In the report below this is shown by team, increasing in size to force level. The driver shall be colour coded and placed by number in teams, thereafter colour coded only, to show their performance compared to that category, for example station or force.

The final column shall be provided to show supervisor action. This will indicate where a supervisor fails to address a driver's behaviour. This will be based on driving behaviour over time. The user organisation shall define time periods where, if a driver's behaviour is below a certain level of performance and remains so for a number of time periods, then the supervisor action will be deemed to be a higher priority and this figure will change from green to red.

	Excess Speed	MPG	Excess Brake	Excess Steer	Idle	Wrong Gear	Use	Speed to Gear	Incident	Acceleration	Harsh	Over Rev	Warning Light	Mileage	Blue Light	Team	District	Division	Force	Sup Action
S C Claus (PS)																3				
A Smith	Red	Red	Yellow			Yellow		Red		Red					Red	5	Red	Red	Orange	Red
B																1	1	1	3	
D													Red			7	Orange			
E				Red												5	Orange			
F		Yellow						Yellow								4	Orange			
G		Red										Yellow				6	Orange			
H							Red									3	Orange			
I														Yellow		2	Orange			
Team		Red					Orange									Orange	Orange	Orange		Orange

Figure 7 – Individual driver profile report

Where the supervisor requires more detail regarding a particular driver, they shall be able to access this via the driver report. This should be available by simply clicking on the relevant section of the report but may require access to the live system.

7.16.4 Level 2 Supervisors Reports

This report follows all of the principles of the first line supervisors report, but aggregates the data into the teams the level 2 supervisor is responsible for. This provides a simple report for the supervisor to assess team performance over time. The report has less detail than earlier reports as at this level overall performance is being assessed. The final column again has the supervisor action field, so that the performance of the level 1 supervisors in improving the driver behaviour of their teams can be assessed.

	MPG	Incident	Warning Light	Excess speed	Blue Light	Mileage	Team average	Division Average	Force average	1 st Line Supervisor actions
Team 1	Orange	Green	Green	Green	Green	Green	4	12	24	Green
Team 2	Orange	Orange	Green	Orange	Green	Green	5	14	25	Orange
Team 3	Green	Green	Green	Green	Green	Green	1	1	3	Green
Team 4	Red	Orange	Red	Red	Orange	Red	10	20	55	Red
Team 5	Green	Green	Green	Green	Green	Orange	2	7	16	Green
Team 6	Green	Green	Green	Orange	Green	Green	3	8	20	Green
Team 7	Green	Orange	Green	Red	Orange	Green	6	15	28	Green
Team 8	Red	Orange	Green	Red	Orange	Green	9	18	48	Orange
Team 9	Orange	Red	Green	Orange	Green	Green	7	16	29	Green
Team 10	Orange	Orange	Green	Orange	Orange	Red	8	17	46	Green

Figure 8 – Driving behaviour profile by team

7.16.5 Level 3 Supervisors Report

This report follows all of the principles of the level 2 line supervisors report but aggregates the data at a higher level into geographic areas. In this example stations that the level 3 supervisor is responsible for. This provides a simple report for the supervisor to assess station performance over time. The report has less detail than earlier reports, as at this level overall performance is being assessed. The final column again has the supervisor action field, so that the performance of the level 1 supervisors in improving the driver behaviour of their teams can be assessed.

As per previous reports, the level 3 supervisor is able to drill down into more detail, if required.

	MPG	Incident	Warning Light	Excess speed	Blue Light	Mileage	Team average	Division Average	Force average	Supervisor actions
Station A team 1	Orange	Green	Green	Green	Green	Orange	4	12	24	Green
Station A team 2	Orange	Orange	Green	Orange	Green	Green	5	14	25	Orange
Station A Team 3	Green	Green	Green	Green	Green	Green	1	1	3	Green
Station A Team 4	Red	Orange	Red	Red	Orange	Red	10	20	56	Red
Station B Team 1	Green	Green	Green	Green	Green	Orange	2	7	16	Green
Station B team 2	Green	Green	Green	Orange	Green	Green	3	8	20	Green
Station B Team 3	Green	Orange	Green	Red	Orange	Green	6	15	28	Green
Station B Team 4	Red	Orange	Green	Red	Orange	Orange	9	18	48	Orange
Station A PCSO	Orange	Red	Green	Orange	Green	Orange	7	16	29	Green
Station B PCSO	Orange	Orange	Green	Orange	Orange	Red	8	17	46	Green

Figure 9 – Driving behaviour profile by Police Station

7.16.6 Level 4 Supervisors Report

This report follows all of the principles of the level 3 line supervisors report, but aggregates the data at a higher level into geographic areas, in this example the report is for a Divisional or Borough Commander. The reports show the districts and other teams or units that the level 4 supervisor is responsible for. This provides a simple report for the supervisor to assess divisional performance over time. The report has less detail than earlier reports as at this level overall performance is being assessed. The final column no longer contains supervisor action. This would be expected to be resolved at a lower level. At this level, an additional field has been added which details the additional cost or potential cost saving for the driver behaviour or improving driver behaviour.

As per previous reports the level 4 supervisor is able to drill down into more detail if required.

	MPG	Incident	Warning Light	Excess speed	Blue Light	Mileage	District/Borough Average	Division Average	Force average	Cost/Savings £ 000
District A							4	12	24	1
District B							5	14	25	-2
District C							1	1	3	5
District D							10	20	55	-10
District E							2	7	16	2
District F							3	8	20	1
CID							6	15	28	-3
Intelligence							9	18	48	-3
Operations							7	16	29	-4
Admin							8	17	46	-3

Figure 10 – Driving behaviour profile by District

7.16.7 Command/Force Level Report

This report follows all of the principles of the level 4 line supervisors report, but aggregates the data at a higher level geographic area. In this example, the report is for the force area. The report shows the Divisions (Boroughs), Departments, that the Force level supervisor is responsible for. This provides a simple report for the supervisor to assess force performance over time. The report has less detail than earlier reports as at this level overall performance is being assessed. The final column details the additional cost or potential cost saving for the driver behaviour or improving driver behaviour.

As per previous reports the force level supervisor is able to drill down into more detail if required.

	MPG	Incident	Availability	Excess speed	Usage	Mileage	Division/ Department	Force average	Cost savings
Division A	Orange	Green	Green	Green	Green	Orange	2	3	8
Division B	Orange	Orange	Green	Orange	Green	Green	3	5	7
Division C	Green	Green	Green	Green	Green	Green	1	1	15
Division D	Red	Orange	Red	Red	Orange	Red	4	10	-12
Uniform Operations	Green	Green	Green	Green	Orange	Green	2	4	9
Road Policing	Green	Green	Green	Orange	Green	Green	1	2	10
Facilities	Green	Orange	Green	Red	Orange	Green	3	6	2
Investigation	Red	Orange	Green	Red	Orange	Green	6	9	-10
Training	Orange	Red	Green	Orange	Green	Green	4	7	-1
Other	Orange	Orange	Green	Orange	Orange	Red	5	8	-3

Figure 11 – Driving behaviour profile by Division

7.16.8 High Priority: Safety Issue Report – Control Room

This report is an example of a safety issue report that would be sent as a high priority message to a control room or supervisor. Given that it may/will require urgent action, this report needs to be clear, concise and suggest the action that needs to be taken.

The report should show the driver or vehicle, the contact details, where applicable. The precise nature of the alert or alerts, in the example below, they are shown in a graph and suggestions as to the expected action.

	Incident	Speed	Warning Light	Out of Force	Team	District	Division	Force	Sup Action	Detail	Suggested Action
Driver a	Red	Green	Green	Green	Red	Orange	Green	Green	Orange	Sudden deceleration - = airbag deployment potential crash	Confirm - send assistance contact local supervisor
Driver b	Green	Green	Green	Red	Red	Red	Red	Red	Red	Unauthorised movement of vehicle outside Force Area high risk vehicle	Establish circumstances - contact driver
Driver c	Green	Green	Red	Green	Red	Orange	Green	Green	Green	ABS, and ESC control activated beyond threshold	Check vehicle speed, consider contact driver. Flag for supervisor
Driver d	Green	Red	Green	Green	Red	Orange	Green	Green	Green	Speed threshold breached 80mph in 30mph area	Contact driver - justify consider flag for supervisor
Driver e	Green	Green	Green	Orange	Orange	Orange	Green	Green	Green	Unauthorised movement outside force area low risk vehicle	Contact driver

Figure 12 – Prioritised driving behaviour profile report with details and suggested action

7.16.9 Fleet Managers Overview

This is the first in a range of reports to allow a Fleet Manager or a person responsible for fleet in a given area of the organisation to gain a quick overview of the vehicles that they are responsible for and where there may be problems or issues. The report will identify the main vehicle groups or areas and identify by colour any problems identified through a number of user defined parameters.

The report is an example of the style that is expected. User organisations will require different variants depending on the area and fleet operated.

	Area / District 1	Area / District 2	Area / District 3	Area / District 4	Branch / Region	Annual Disposal	Police Order	CD	Abused	Damage	Underwater	Adapt	Notes / Advice
Excessive MPG	10	11	50	9	62	54	10	30	0	10	0	0	For further information check Station, Team and individual records to ascertain if this is caused by individuals or groups.
Exceeds 100 MPH	4	10	25	5	20	25	5	10	0	5	0	0	Why is this vehicle travelling at an excess of 100 MPH. Link this with location search to ascertain where these speeds were performed.
Vehicles not used for 7 days	5	13	25	7	24	22	3	25	0	3	3	0	Why are these vehicles not being used? Are these vehicles cost money, check details or find which vehicles are not being used.
Excessive Mileage / month	2	1	5	4	30	5	8	2	2	8	2	4	Check vehicles against service schedule, possible consideration to move fleet to even out mileage.
Excessive idling Time	2	1	5	4	30	5	8	2	4	8	2	3	Check types against what duty were these vehicles engaged at levels of prolonged idling.
Incident recorded	0	8	15	0	0	1	0	0	0	0	0	0	If an incident has been recorded the vehicle must be subjected to a safety check to ensure the vehicle is roadworthy on return from vehicle servicing.
in Workshop for more than 3 days	0	5	10	2	0	1	0	2	0	0	2	0	Why has it taken the vehicle more than 3 days to be repaired? (Changeable selection to suit different areas)

This area is second on the cost list to Area / District 3	This shows that Area / District 3 vehicles are not performing very well and are being the most damaged one and also the most abused.
---	--

Figure 13 – Fleet Manager’s report

This report may also be used in combination with an overall fleet summary or dashboard, providing a highlight of the information. This style of report would lend itself to indicators similar to a vehicle dashboard using dials and charts to provide a simple to read format. This dashboard style of report is not prescribed in this document.

7.17 Workshop Managers Report

The Workshop Managers report is based on vehicles in a given geographical area. This may also be useful for managing the vehicle fleet in that area. This report identifies vehicles that may have been driven excessively or are overdue for service or which have a fault. This report will provide information on which a Workshop Manager can make more informed decisions on servicing and the operation of the fleet for which they are responsible.

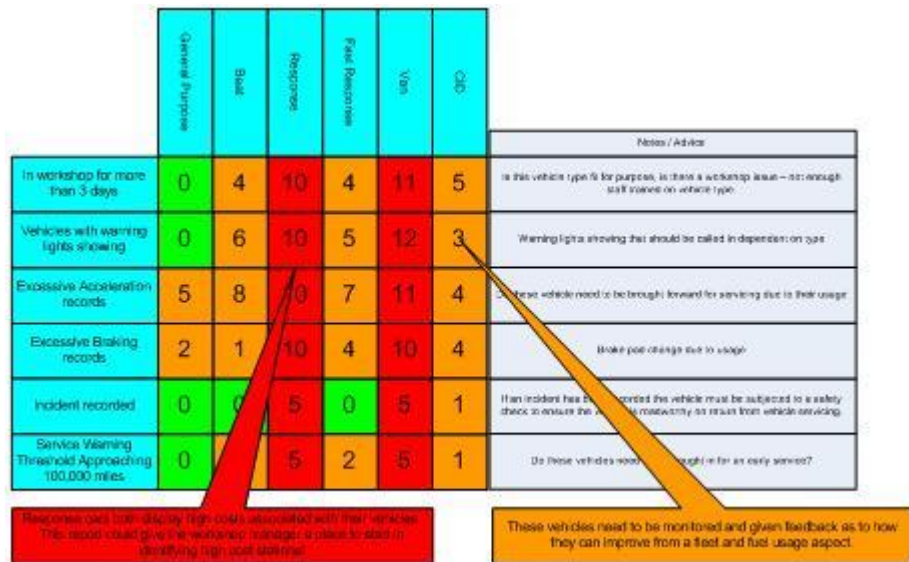


Figure 14 – Workshop Manager's report

These second and third level reports provide a more detailed response as to how teams operate vehicles at different levels: station or area. This, not only identifies where a team may be responsible for a defect or excess servicing but may assist in understanding where vehicles may need to be used differently or where a different type of vehicle is required.

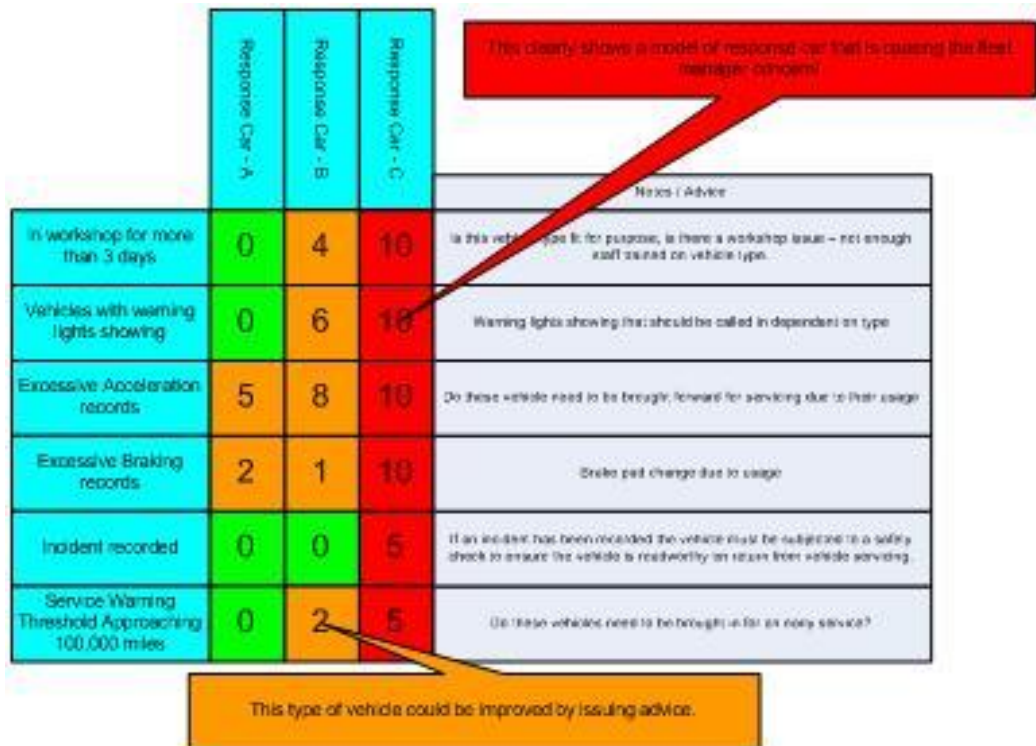


Figure 15 – Police Station detail for Workshop Manager

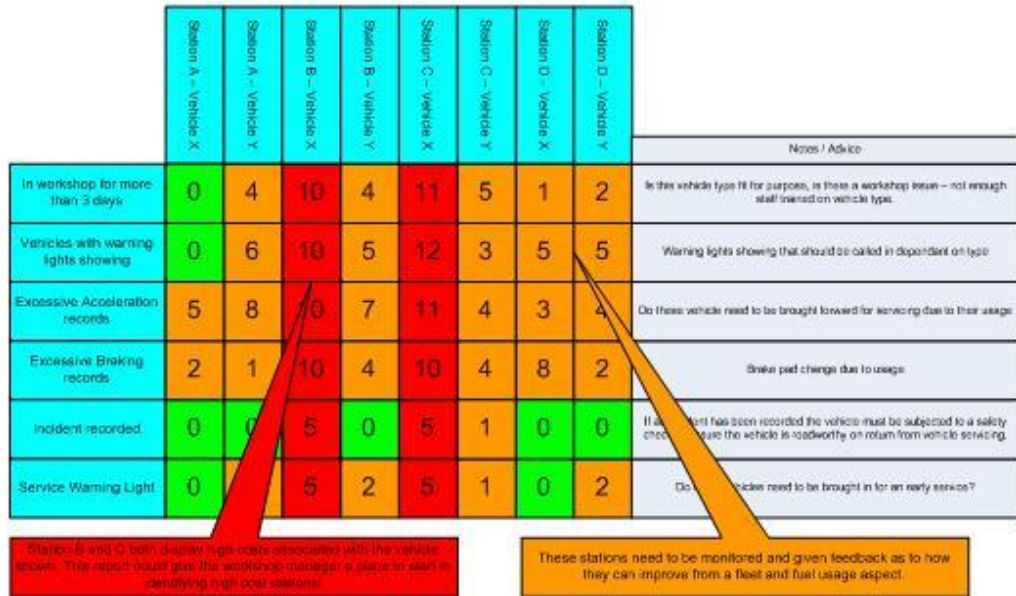


Figure 16 – Vehicle report for Workshop Manager

7.17.1 Vehicle Profile

The vehicle profile report is analogous to the driver report and details how the vehicle has been driven, within a given period and the activation of any warning equipment. This again may be used to identify specific servicing or maintenance needs or where a vehicle is being used excessively and needs rotating to prolong its operational life.

Vehicle Profile – AB03CDY - 100875					
	October 2010	November 2010	December 2010	January 2011	February 2011
Excess Speed	10	10	20	25	10
MPG	0	0.5	6	6	1.5
Brake pad wear light	0	0	0	0	0
Engine Management Light	0	0	0	0	0
Airbag Warning Light	0	0	0	0	0
Traction Control Warning Light	4	0	9	8	0
Oil Warning Light	0	0	0	0	0
ABS Warning Light	5	1	7	7	2
Incident	0	0	0	0	0
Harsh accel	4	2	20	25	6
Over rev	4	1	20	20	6
Active Stability Control Warning Light	0	0	3	3	0
Mileage	0	-10	-3	-6	-8
Blue Light Usage	4	3	10	15	6

Figure 17 – Vehicle maintenance profile

In a similar way to driver's reports, users of this report shall be able to drill down; ideally by clicking on the parameter to provide additional detail. E.g. current mileage or the event, time, date and location of where a warning light was activated and the subsequent vehicle usage or even which driver was using the vehicle at the time. This may also be produced on a map.

7.17.2 Technicians Report

This report is a summary of the vehicle report providing the technician an overview of how the vehicle has been used since the last service or inspection. This may assist a technician when inspecting the vehicle or for fault finding.



Figure 18 – Vehicle technician’s report

7.18 Searches

The DVDMS shall have a simple and easy system for authorised users to quickly and easily produce customised reports or searches for a range of commonly used search parameters. The reports that are produced should be customisable in a similar format to those above or as defined in the responses below. The search forms shall be easy to use, such as a series of drop down boxes or template that can be checked or completed rather than complex searches.

7.18.1 Vehicle Usage

The following reports details an example of how a vehicle usage report should be created, together with a number of examples of the outcomes of different searches. This report is expected to be frequently run by a range of users to understand how vehicles are used or by whom. This report will require a range of variations to suit the different users requirements, the parameters below should not be regarded as exhaustive.

Not Used Consecutive period		Search area		Vehicle Typ	
Not Used	Select	Force	Select	vehicle	Select
now		Division A		Marked car	
8 hours		Division B		Plain Car	
24 hours		Division C		HP Car Marked	
weekend		CID		HP Plain	
3 dyas		Ops		PSU	
7 dyas		RPD		Van	
28 days		Training		M/cycle	
Night 2200-0600		Other		Fierams	
				4x4	
				Dog Van	
				Specialist	
				Other	

Figure 19 – Vehicle usage search criteria

This report identifies vehicles that have not been used for at least 3 days. This may indicate under utilisation or a vehicle with a problem that has not been rectified.

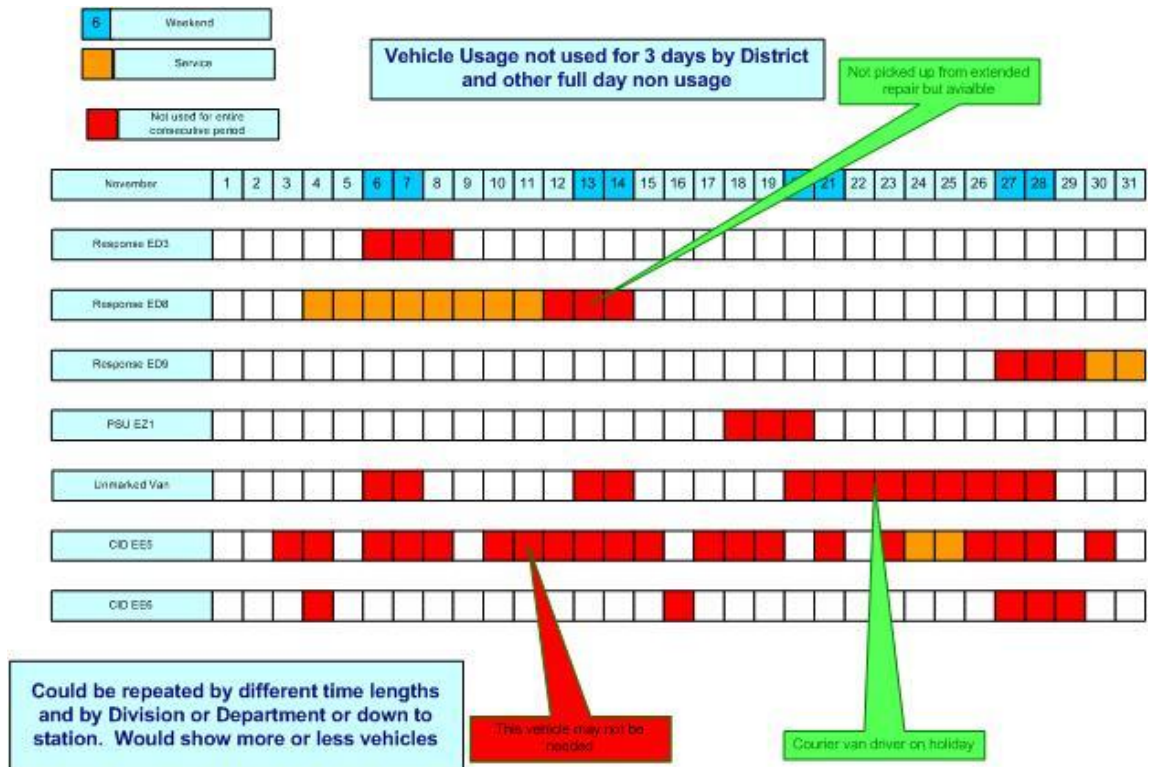


Figure 20 – Vehicle utilisation report by Division, Department or Station
 The second report details similar information but for a specific vehicle.

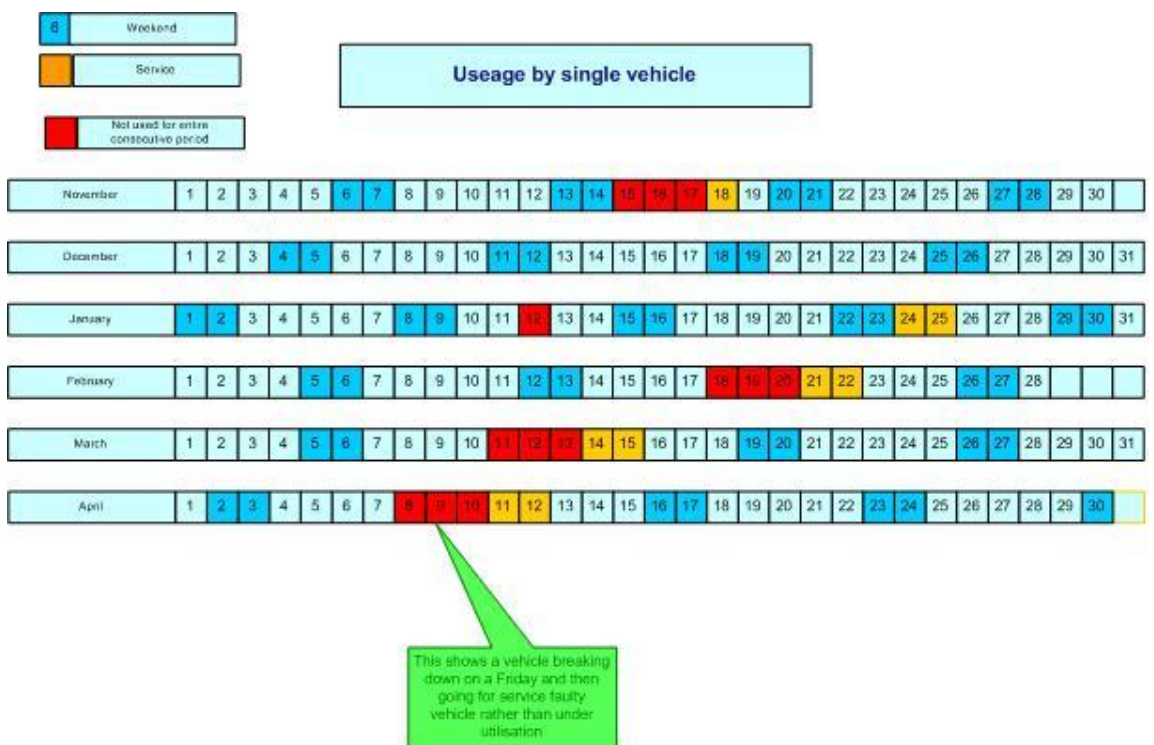


Figure 21 – Specific vehicle utilisation report

7.18.2 Vehicle Speed Search

The vehicle speed search is another commonly used search to identify where vehicles are used at excess speed and by whom. This search may be customised for emergency and non emergency driving.

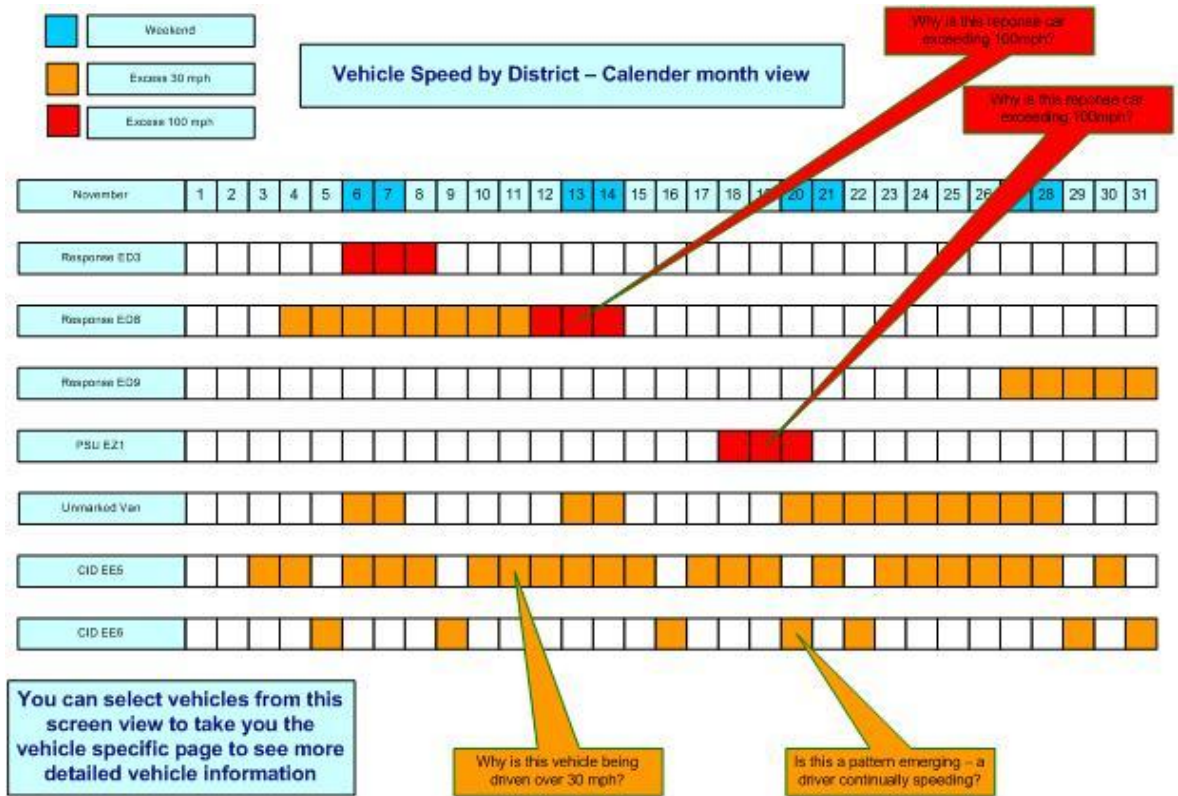


Figure 22 – Vehicle speed report by District

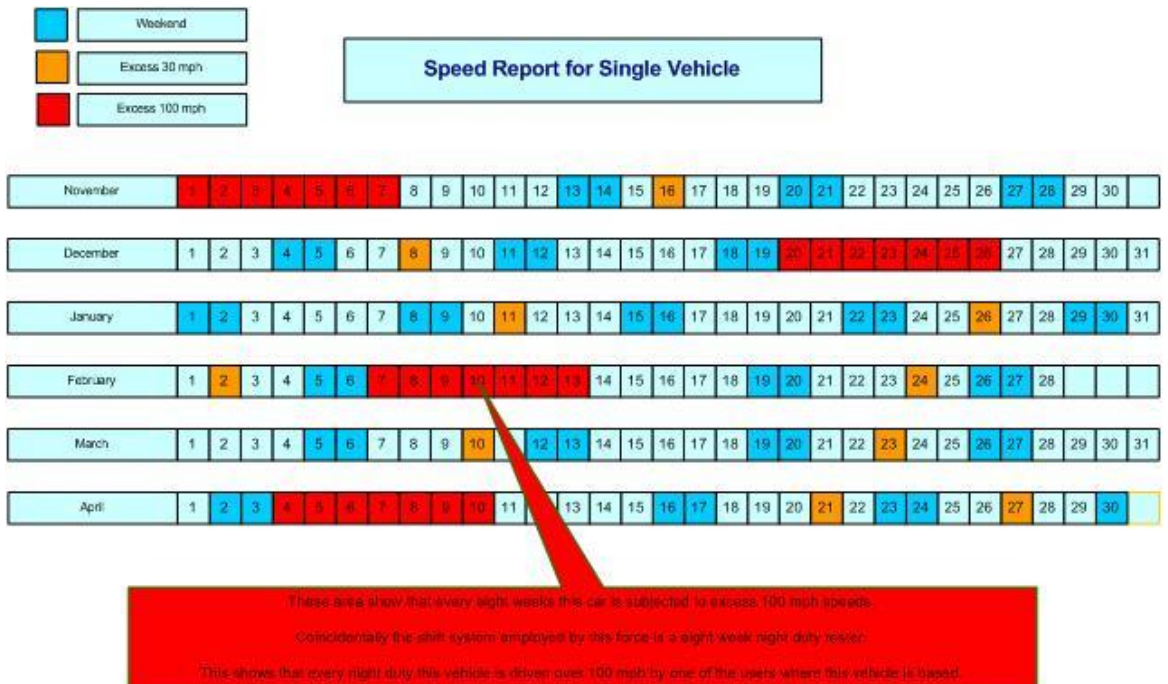


Figure 23 – Speed report for a single vehicle

Other searches will be defined in future versions of these criteria as more systems become operational. All such searches shall follow the principles outlined above.

8 DVDMS Compliance Procedure and Evaluation

8.1 Introduction

This chapter sets out the protocol for the Compliance Procedure to be applied to the accreditation of One Box Driver and Vehicle Data Management systems (DVDMS) and their interface with emergency service equipment through the esCAN. It should be read in conjunction with the other sections of these criteria, which defines the functionality, quality and performance specification of the DVDMS.

The DVDMS criteria are owned and maintained by the Home Office Centre for Applied Science and Technology (CAST). They will be managed operationally by CAST, who will oversee accreditation and testing of newly developed systems by accredited test houses against the DVDMS criteria.

The DVDMS criteria incorporate a programme for the evaluation of DVDMS against a defined set of requirements, for the purposes of generating a periodically updated Notification List of approved systems or components.

These criteria are intended to ensure that DVDMS equipment works as an integrated solution in emergency service vehicles.

The DVDMS criteria document is a published specification but, given the pace of change of technology and emergency service requirements, it will be kept under review and updated when necessary, to ensure that it remains current. A requirement for review at least every 12 months has been incorporated within the criteria, so that any omissions or proposed changes brought to the attention of the Home Office, Association of Chief Police Officers (ACPO) Intelligent Transport Systems (ITS) or an accredited test house can be subsequently considered and added in a timely manner throughout the life of the DVDMS criteria document.

If any DVDMS criteria user wishes to suggest amendments for the next review process, these should be notified for the attention of the criteria review board via email to ACPO ITS, CAST or an accredited test house for consideration at the next review. Specific email addresses are not included in this document. Users should contact one of the relevant bodies to ensure the correct current email address is used.

Systems submitted for testing are expected to achieve full compliance with all relevant aspects of the criteria contained within the document. However, it is recognised that it may take time for suppliers and users alike to move towards full system compliance.

To ensure that progress towards full compliance is recognised, accredited test houses will have the ability to report and certificate partial compliance with defined areas of the DVDMS criteria. For example, the DVDMS may meet the majority of requirements but may not be able to produce all of the reports or may not have all of the functionality. Where such derivations are relatively minor or temporary in nature, with a clear plan for resolving them, a part compliance certification may be considered where a system meets all elements of a particular section(s).

8.2 One Box Driver and Vehicle Data Management System

DVDMS are accredited primarily to demonstrate that they meet the functions, performance, quality and security requirements set out in this document and in doing so, evidence their safety and operational effectiveness and benefits as a telematics solution, recording a wide range of data from the vehicle and the emergency service equipment in operation.

Clearly, the DVDMS needs to be operated within the context of emergency service vehicles. The quality of integration of DVDMS and the connection to the emergency service equipment and original equipment manufacturer (OEM) vehicle systems, via the esCAN will be considered as part of the process of accreditation.

The Compliance Procedure is applicable to the systems fitted to the vehicle as part of its construction (OEM) or installed before or after the sale of the vehicle aftermarket. Therefore, an application for evaluation may be made by a vehicle manufacturer or importer or by an emergency service equipment manufacturer or importer or by a duly accredited representative thereof, to CAST.

The DVDMS will be designed and installed in cooperation with vehicle manufacturers and equipment providers, so that it does not conflict with vehicle manufacturers or emergency service systems, yet provides the functionality to support current and future in-vehicle emergency service systems.

The DVDMS criteria also recognise that there may need to be different installation requirements and Compliance Procedures between systems installed as part of vehicle manufacture (OEM) and that of post-build or aftermarket. These are to be identified within the criteria, where applicable.

8.3 DVDMS Accreditation

The DVDMS accreditation scheme is directed by CAST and supported by a public-private partnership the One Box Consortium, led by the ACPO ITS Working Group.

The accreditation of DVDMS will be led by CAST, which will appoint accredited test houses that will carry out end-to-end system compliance tests and technical component assessments, either on their own or in partnership with other facilities (for example, sub-contractors). The decision to accredit candidate DVDMS will be made solely by CAST who are the Test Authority. Systems can be determined as:

- Compliant;
- Non Compliant; or
- Partially Compliant.

8.3.1 Publication

CAST will publish the names of those systems accredited as meeting the requirements defined by the DVDMS criteria. These systems will be included in a Notification List of recognised, accredited systems, hereinafter referred to as 'the List'. A DVDMS shall be added to the List following the issuing of a Notification of Compliance statement by the accredited test house.

The List shall normally be updated four times a year or at more frequent intervals, if circumstances require. CAST shall solely determine the frequency

and means of publication. The List shall normally be made available to the emergency services, trade bodies, manufacturers and/or importers, installation companies and other relevant interested parties.

8.3.2 One Box DVDMS Criteria List

Any information contained within the List may be utilised as required by public authorities. It may also be relevant to systems installed as standard by vehicle manufacturers.

There are a number of sections incorporated within the List, principally to aid and benefit potential purchasers and manufacturers. The systems are divided into classifications depending on the type of system, together with any fitment policy. A brief explanation of any special features of a system that may be supplementary to the base requirements is included. Vehicle manufacturers' systems are cross-referenced against fitment policy on vehicle models and their variants.

Systems will be entered onto the List and they will be described as having full or partial compliance with the DVDMS criteria.

Systems that fail the accreditation process will not be entered onto the List.

8.4 Period of Application of the Compliance Procedure

The Compliance Procedure is only applicable to the evaluation of systems that fall under one of the classifications defined in this document.

CAST reserves the right to; periodically revise the DVDMS criteria, including the Compliance Procedure. The existing DVDMS Notification of Compliance statements issued in accordance with the Compliance Procedure shall remain valid for a minimum of one year after a major revision of the criteria. Major criteria revisions shall be identified by a change of version number.

During this period, repeat inspections shall be performed on the basis of the version of the criteria applicable at the time of accreditation. In order to maintain List quality, there shall be a maximum period notified to those affected suppliers, vehicle and system manufacturers governing the time permitted for old issue level systems to remain Listed. The accredited test house may stipulate a maximum Listing period in the Notification of Compliance statements issued for each system, after which the expired DVDMS may be removed from the List.

The Compliance Procedure and criteria may be subject to minor interim revisions by the publication of addenda to modify the current documentation. A transition period during which systems may be submitted for evaluation against the minor revision level shall normally be applied at the discretion of CAST.

8.5 Partial Compliance

In an effort to assist manufacturers to become fully DVDMS compliant, an accredited test house can offer partial compliance certifications to recognise manufacturers working towards a compliant system. The test process for partial compliance will be the same as for full testing. The only difference being the outcome. Where a particular DVDMS meets the majority of requirements but is not be able to produce, for example all of the reports or may not have all of the functionality and where such derivations are relatively minor or temporary in nature and there is a clear plan for resolving them, a part compliance

certification may be considered. These certifications will be provided according to the heading or sections of this criteria to which it is compliant, clearly identifying derivations.

The system would be Listed as part compliant.

The partial compliance certification is an interim measure and will be phased out over time and is likely to be withdrawn within 24 months from the launch of the first version of these criteria, as suppliers work towards full compliance. The ongoing provision of the partial compliance option will be considered every six months, when the document will be reviewed, utilising processes explained above. Therefore, the provision of partial compliance certifications should be regarded as a temporary measure to support, encourage and recognise the efforts of manufacturers as they work towards full compliance with the DVDMS criteria.

Partial compliance certifications will only be endorsed and appear on the List for 12 months. After that time the certification will expire and another full test must be applied for through a test house, so that the system presented can be entered onto the List for another 12 months if it remains partially compliant. If the system achieves full compliance, the system will revert to those processes for fully compliant systems explained within this document.

8.6 Compliance Procedures and Administrative Requirements

8.6.1 Conditions of Evaluation

To qualify for a Notification of Compliance of a DVDMS:

- The Applicant shall agree to the Terms and Conditions for assessment by submitting the Request for Evaluation form.
- The DVDMS shall be demonstrated to comply with these criteria and shall have passed the tests successfully.
- All evaluation fees shall be paid, prior to Listing.
- The Applicant shall agree to the Terms and Conditions of Listing.

8.6.2 One Box DVDMS Already Accredited to Relevant Standards

Where manufacturers or suppliers of equipment can evidence compliance with AES Specifications that are referenced within this document or other recognised test procedures and are relevant to the DVDMS Compliance Procedures, at the discretion of CAST and the accredited test house, they may be released from the requirement to undertake specific portions of the test regime.

This shall be dependent upon the exact accreditation that was obtained to the relevant standard or standards.

This shall take into consideration the date of the most recent test or audit in order to ensure that these processes are given full regard in accrediting or re-accrediting a system.

The decision of CAST in this matter shall be final and shall not be subject to an appeal process.

8.6.3 Application Procedure

The assessment shall be requested by submitting the Request for Evaluation form, completed and signed by the Applicant, to CAST. CAST will ensure that the application form is correctly completed and will issue a unique reference number for the application, which must be used in all future documentation and testing for this application. CAST will supply a list of Accredited Test Houses.

The Applicant will choose an Accredited Test House.

The Accredited Test House will supply to the Applicant all the required documentation for testing, together with a list of charges, Terms and Conditions and timescales for testing. The Accredited Test House will be responsible for the testing of submitted systems against the DVDMS criteria and ensuring that the ongoing compliance and quality checking is undertaken.

The application, with supporting technical and administrative documentation, shall be considered commercially sensitive. All communications shall only be with the designated Applicant or Applicants. The primary Applicant may nominate secondary representatives for correspondence. It is requested that for an evaluation against the DVDMS involving two or more interested parties, reporting access is permitted to all parties.

8.6.4 Evaluation

The evaluation is intended to demonstrate a minimum acceptable level of compliance by the system under test against the performance levels set out in the DVDMS, in the context of the real-world operation of emergency service vehicles, with respect to security, safety, reliability, interference, functionality, distraction and documentation. The level of validation is high and is broadly based upon the One Box Single Vehicle Architecture criteria and test regime.

The evaluation shall be performed, in accordance with the DVDMS criteria and the Compliance Procedure, on the sample systems/vehicles and documentation submitted to the accredited test house by the Applicant. The Applicant shall ensure that the test sample material is complete and identical to that in production.

For the evaluation, normally one complete test sample shall be submitted free of charge at specified times in the process. The exact number may vary depending upon the test programme.

The evaluation is progressed through three Phases of assessment, whereby validation is conducted progressively in order to avoid committing high testing costs and test capacity to systems, where they are unlikely to comply through all Phases. Part fees are payable in advance of each Phase for the commencement of work. Work shall not commence until such time that these fees are paid.

A system under test may progress to a subsequent Phase, only if the period between sign-off compliance of the current Phase and the commencement of the subsequent Phase is no longer than six months. If the period is longer than six months, the system shall then be defaulted to the start of Phase 1, as per a new application.

A system under test shall be required to complete each individual Phase of the evaluation within a period no greater than 12 months. Failure to complete each Phase within 12 months shall cause the system under test to be defaulted to the start of Phase 1, as per a new application.

No Applicant can claim compliance with the DVDMS criteria for emergency service vehicles, until such time that the testing process has been successfully completed and the Applicant has agreed to the Terms and Conditions of Listing and paid the required fees.

8.7 Phases of Evaluation

8.7.1 Phase 1: Questionnaire

The Request for Evaluation form shall be submitted together with a detailed Questionnaire and the supporting documentation requested in the Questionnaire. These shall be examined for compliance with the DVDMS criteria. A meeting with the Applicant, together with an initial examination of the system, shall normally be requested as part of this Phase. A close dialogue is encouraged between the Applicant and the accredited test house. The requirements for testing at Phase 2 and Phase 3 shall be discussed and agreed. It is acceptable at this stage to present a prototype sample of the system.

Defined Phase 2a Vehicle Test requirements may specify that several vehicle models or manufacturers are to be inspected and multiple reports are required depending on defined vehicle fitment policy. (The DVDMS under test may be vehicle manufacturer or model specific or a component within an identified system, and compliance will be determined within that agreed installation.) This may require a system versus vehicle model matrix, which shall be provided to the accredited test house in order to clearly define fitment policy of the system or system variant. In this case, the accreditation fee may be higher than the standard charge.³ Requirements for inspection of quality control procedures at installation locations will be defined. This phase will also test the communication and functions of the Back Office.

An analysis of the system under test for Phase 2b testing requirements may demonstrate that it has multiple derivatives, variants, optional components or will have to be tested in a modular way. The fee may be higher than the standard charge for a singular system.

Documentation and sample requirements for Phase 3 accreditation testing will be specified at this Phase and these items will be requested and checked.

8.7.2 For Vehicle Original Equipment Manufacturer Systems

Where a vehicle OEM develops, manufactures and installs a DVDMS, as part of the process of building the vehicle, or where a vehicle is or is planned to be fitted as a vehicle manufacturer approved part, fitted by a vehicle manufacturer approved dealer/installer option, be that pre-sale or aftermarket as part of a vehicle manufacturer warranted option, this may already have been checked and found compliant with the relevant legislation and standards. Where this is the case, the vehicle OEM will be required to submit a Parts Submission Warrant for all DVDMS criteria parts. These shall be supplied in electronic format. The accredited test house will check the information and retain electronic copies.

For the audit process, the accredited test house will require a new Parts Submission Warrant every two years after initial Listing, with a full reassessment after six years.

³ Accreditation fees are at the discretion of accredited test houses.

Documentation for Phase 2b compliance will be specified at this phase and these items will be requested and checked.

The accredited test house shall supply a master copy of the 'Certificate of Commissioning' to CAST.

8.7.3 Phase 2a: Vehicle Test Programme

At least two vehicles of different manufacturers or models shall be made available to the accredited test house and its accredited sub-contractors and/or agents with the system or systems under test pre-installed.

Specific installation instructions shall be provided at this Phase.

The system under test and installation shall be accurately representative of standard production specification with all components provided for inspection.

The quality of installation of all OEM and aftermarket DVDMS shall be inspected in accordance with the technical standards laid down in the DVDMS criteria and, where appropriate, the agreed AES/National Association of Police Fleet Managers (NAPFM) Guidance for fitment of equipment to emergency service vehicles.

A series of tests shall be conducted on the installed system under test.

The installed system shall be subject to end-to-end system test and monitoring, covering all areas and functionalities to include:

- Safety;
- Operation;
- Reliability;
- Effectiveness;
- Interference – with vehicle systems (as per AES Specifications 5, 6 and 13);
- Interference with emergency service equipment (as per AES Specifications 5, 6 and 13);
- Human-machine interface, in-vehicle and presentation of reports to users:
 - Ease of use;
- Data collection/management/storage/communication/security:
 - In-vehicle;
 - Connection to OB SVA esCAN vehicle and aftermarket equipment CiA 447;
 - Back Office;
- Crash protection of the in-vehicle DVDMS;
- Back Office operation/storage/analysis/integration with force systems;
and
- Reports.

If failures and non-compliances arise during a test, the Applicant shall be approached with details of the failures and provided with a summary describing the nature of the failure, the root cause and the corrective action to be taken to eliminate the failure.

The summary report shall be issued to the Applicant detailing any non-compliances and recommendations. A statement of compliance or non-compliance shall be issued to the Applicant at the conclusion of this Phase.

A minimum of two models of different manufacturers or models shall be assessed by a thorough vehicle inspection, and other vehicles shall be validated by the inspection of vehicle-specific installation instructions to establish conformity across the range.

This will include inspection and validation of the connection to and the operation of the Back Office, as part of a whole system test. The level of validation shall depend upon the particular circumstances and shall be determined by the accredited test house at Phase 1 after defining the fitment policy.

The fee at this Phase shall be dependent upon the level and complexity of the system under test and the validation required.

8.7.4 Phase 2b: Functional Test Programme for Aftermarket Systems

Normally, one complete sample of the system under test shall initially be provided free of charge by the Applicant directly to the accredited test house. This shall be checked against documentation and sample lists for completeness. Further samples shall be provided, free of charge to the accredited test house, if required, to a maximum number of three. Samples shall be supplied in various formats depending on the projected test programme. This may require that they are functionally connected and mounted on test boards; functionally connected only; or boxed/packaged as supplied to the installer. These samples shall be subjected to the component test regime defined by the Performance Test Specifications.

A reference sample of the system under test shall be required upon completion of testing and retained for future auditing checks. The samples provided shall be complete and accurately representative of the standard specification with all components provided.

For evaluations of some integrated vehicle-specific original equipment systems, one or more vehicles may require to be inspected or tested at this Phase. The Phase 2b testing body shall be approved by CAST, as part of the approval process for the test house.

Validation of software may involve detailed discussions with the Applicant in order to establish the integrity of the design.

Note: In order to ensure an audit trail, it is strongly recommended that any important correspondence with the accredited test house should be conducted by email and that notes of telephone conversations are kept in an organised fashion.

During Phase 2b testing, the accredited test house will, at its discretion, issue periodic reports to the Applicant indicating progress and failures. It should be noted that the accredited test house is not obliged to issue interim reports on request.

The test regime shall require to be completed satisfactorily and a test regime completion report issued in order to progress to Phase 3. A statement of compliance or non-compliance shall be issued to the Applicant at the conclusion of this Phase.

The fee at this Phase shall be dependent upon the level and complexity of the system under test and the validation required. The extent of testing shall take into account factors such as different systems under test variants, including build to specification and print types. It will also take into account minor system derivatives based on hardware or software and optionally specified components. It should be noted that multiple system derivatives or variants can lead to high test fees.

At the conclusion of the Phase 2b programme, the accredited test house shall return all test samples except one to the Applicant. The test house shall keep one test sample as a reference sample.

8.7.5 Original Equipment Manufacturer System Component Certification Programme

This phase shall be accomplished by the submission of the relevant certificates, for the compliance for the DVDMS criteria system parts, in line with the latest EC regulations.

8.7.6 Phase 3: Review and Notification

The results of the previous Phases shall be examined and, if considered satisfactory, a Phase 3 statement shall be issued to the Applicant by CAST indicating a Notification of Compliance. This shall request from the Applicant further information relating to the List and require the Applicant to sign and return a statement, which agrees to further Terms and Conditions for Listing the system.

The name of the system under test shall be confirmed and agreed at this time. The name selected shall be such that it is sufficiently dissimilar from recognised systems, or from earlier non-compliant versions of the Listed systems on the DVDMS. The Phase 3 Notification of Compliance statement represents an agreement between the accredited test house and the Applicant, and will lead to the issue of a Certificate of Compliance for the DVDMS.

The system under test shall be issued with a unique reference number issued through CAST. This number shall be stated on Certificates of Installation and quoted in any further correspondence with the Applicant or the accredited test house.

CAST shall normally include the system that has passed the compliance tests on the subsequent Notification List following the issuing of the Phase 3 Certificate of Compliance.

8.7.7 Compliance Procedure Summary

<p>Phase 1 – Questionnaire</p> <ul style="list-style-type: none"> • Complete and return Request for Evaluation form with fee • Complete and return Questionnaire • Parts Submission Warrant (OEM only) • Submit documentary evidence of compliance • Questionnaire reviewed and test programme established • Notification of Compliance/Non-Compliance statement
<p>Phase 2a – Bench / Vehicle Test Programme</p> <ul style="list-style-type: none"> • Requisition of a vehicle, vehicles or use of bench • Requisition of components – installed on vehicle • Check vehicle installation quality for compliance with criteria • Check Back Office operation • Notification of Compliance/Non-Compliance statement
<p>Phase 2b – Functional Test Programme</p> <ul style="list-style-type: none"> • Requisition of system for testing (OEM Component Certificates) • Carry out performance and environmental testing (aftermarket only) – to include communication to and from the Back Office • Functional test of Back Office to include information outputs, searches and reports • Verification of OEM system Certificates • Notification of Compliance/Non-Compliance
<p>Phase 3 – Review and Final Notification</p> <ul style="list-style-type: none"> • Final notification to the manufacturer and CAST of level of compliance with the DVDMS criteria
<pre> graph TD Phase[Phase] --> Comply{Comply?} Comply -- Yes --> NextPhase[Next Phase] Comply -- No --> End[End] subgraph Options ReApply[Re-apply with fee] Rectify[Rectify and comply] end ReApply --> Phase Rectify --> NextPhase </pre>

Note: At the discretion of the accredited test house, Phase 2b can be initiated prior to or during Phase 2a.

Table 3 – Summary of compliance procedure

8.8 Management of Failures

In the event of failure, the Applicant shall be notified of the areas of non-compliance by the accredited test house. The Applicant may then do one of the following:

- Withdraw from the Compliance Procedure indefinitely;
- Rectify the system under test with modifications to documentation, installation or system within one month incurring no penalty. Areas of non-compliance shall then be retested. The retesting fees shall be charged to the Applicant; or
- Restart the testing process, incurring the full or part test fee as required by the test house, within six months.

8.8.1 Minimisation of Failures

In order to achieve a steady progression of the submitted DVDMS for evaluation through the Compliance Procedure, the Applicant shall observe the following guidelines:

- Ensure the return of the Request for Evaluation form and fee;
- Complete the initial Questionnaire comprehensively;
- Read and understand the specifications thoroughly;
- Conduct extensive validation prior to submission of the system in order to establish high confidence that the system will comply. Failures shall delay the progression of the evaluation, and may lead to enforced delays of two months before work may continue;
- Ensure that samples are identical to those in production;
- Check samples functionally and visually before submission. Physically non-compliant samples shall be rejected at an early stage. Samples shall be properly marked;
- Ensure the Back Office is fully functioning;
- Ensure the candidate DVDMS can connect to the esCAN/OEM system;
- Ensure the Back Office can produce the information reports and outputs in the required form;
- Check that all documentation is complete and accurate – only correct drawings and instructions shall be accepted. Failure to provide adequate and complete documentation in the correct format shall delay testing and shall constitute non-compliance; and
- Ensure that manufacturing quality of samples is satisfactory. Poorly manufactured samples shall be rejected immediately.

If retesting is requested as a result of non-compliances, this can extend the duration of the evaluation significantly and the Applicant will incur associated retesting fees. These will be charged at normal accredited test house rates, supplemented by an administration charge.

8.8.2 Timings

Assuming no non-compliances at any Phase or Phases, the evaluation process timing shall normally be expected to be within four to six weeks. It shall be stressed that this is based upon good system performance combined with timely and accurate support from the Applicant.

8.9 Administrative and Technical Documentation to be Submitted at Each Test Phase

Correct and complete documentation is a prerequisite of testing at each of the Phases 1, 2 and 3. It may also be required on request in the event of a system or random audit following Listing.

All documentation submitted shall be in English.

All documentation shall be submitted to the accredited test house in either paper or electronic format.

The following documentation, normally one copy of each item unless otherwise indicated, shall be submitted to the accredited test house no later than the commencement of the appropriate Phase.

8.9.1 Phase 1

- Request for Evaluation form.
- Parts Submission Warrant (OEM only).
- Supporting documentation as specified in Questionnaire.
- System/vehicle fitment plan (matrix).
- Part test fee as specified.

8.9.2 Phase 2a

- User Instructions, as required in the appropriate section of the DVDMS criteria.
- Vehicle-specific Installation Instructions.
- Back Office access operation and instructions
- Part test fee as specified.
- Software versions
- Build standards

8.9.3 Phase 2b

- User Instructions (as requested in the appropriate section of the DVDMS criteria).
- Special Operating Instructions for the system under test samples. These shall include commissioning procedures, use of any vehicle emulation or diagnostics equipment, data transmission protocol, timing diagrams/flow charts, decoding of data/batch codes on labels, vehicle functions

(aftermarket only). This will also include those elements relevant to the Back Office.

- General Installation Instructions for the system under test. These may be in draft form, the definitive version being submitted subsequently. The Installation Instructions shall meet the requirements laid down in the appropriate section of the DVDMS criteria.
- Part test fee as specified.
- Certificate of Compliance for DVDMS criteria parts (OEM only).
- (Aftermarket only) An electronic copy of a Technical File of documentation on all system components under test (those parts as specified in section 8.7.4 of the criteria) comprising the following:
 - System parts list and descriptions;
 - Component parts list;
 - Mechanical drawings;
 - Moulding drawings of enclosures;
 - Assembly drawings;
 - Printed circuit board layouts;
 - Circuit diagrams;
 - Circuit descriptions;
 - Connector and crimp specifications;
 - Connector pin-out details;
 - Current ratings for I/O
 - CiA 447 compliance
 - Back Office:- reports security
 - Data storage – in-vehicle and Back Office
 - Data communication
 - Driver identification method;
 - A statement that all components submitted are representative of series production;
 - Details of existing test results including reports.
 - Software versions
 - Build standards

The system parts list shall include, for each system: description, manufacturer, part numbers, and issue level and software revision.

The electronic documentation shall be provided in indexed format. There shall be a register of the items included in the (aftermarket only) Technical File.

Electronic technical aftermarket documentation submitted shall be provided with the name of the manufacturer, component identification, drawing/document number and date. System issue levels shall be clearly specified.

Part numbers, descriptions, issue levels and dates shall be clearly marked on all drawings.

Part numbers shall permit complete traceability as to the build level and date of manufacture of the system under test.

All documents shall be complete, clear and legible.

All items of documentation shall be consistent with the system under test.

All drawings shall be originals or, where produced electronically, certified copies.

8.10 Aftermarket Systems to be Submitted

The evaluation shall be conducted in accordance with the Compliance Procedure and the DVDMS criteria on the aftermarket system submitted to accredited test house by the Applicant. The Applicant shall ensure that any samples of the aftermarket system under test that are submitted are representative of series production and shall confirm this to the accredited test house in writing.

Submitted samples of components to include access to the Back Office constituting the aftermarket system under accreditation testing shall include all the items listed in of these criteria and shall include any optional equipment.

For the purposes of the evaluation, one complete sample (fully functional) of the aftermarket system under test shall be submitted (the Back Office element may be achieved by providing access to the Back Office component). Additional components may be requested for the purposes of component substitution. All necessary simulation and diagnostics equipment shall be provided, if requested. Connected systems, shall be such that monitoring of all outputs is straightforward.

The aftermarket system under test shall be visibly marked with the following information:

- The system under test manufacturer's name or trade mark;
- The model number or name;
- Component part number;
- Linked components, for example, data bearers; and
- Serial number, batch number or date of manufacture of the system.

In addition, each component of the aftermarket system under test containing software shall be labelled with the software version, number or code. This may be implicitly identified within the main part number.

There shall be directions provided for decoding data/batch codes and software revision levels.

Replacement or additional components shall be readily made available on request during the evaluation.

An audit trail of component samples submitted as part of aftermarket system accreditation testing shall be supplied on request by the Applicant to the accredited test house for quality control system monitoring purposes, if required.

8.11 Name Changes or Additions

The following shortened procedure shall apply if the Applicant has requested the Listing of a DVDMS, the name of which has been changed or to which an additional name has been given with respect to a previously existing, accredited and Listed system.

The Applicant shall submit:

- A Request for Evaluation form;
- A completed Questionnaire;
- Supporting documentation as specified in Questionnaire;
- A signed statement that the submitted DVDMS is identical to the existing compliant system;
- User Instructions to include Back Office;
- Installation Instructions;
- The appropriate fee; and
- (If requested) one complete sample of the name change/addition system for inspection (aftermarket only).

A Phase 2a test programme shall be required if the system or vehicle application is considered dissimilar. This shall be at the discretion of the accredited test house, which shall conduct a comparison of the submitted name change sample against the original reference sample. Subject to a satisfactory evaluation by the test house, the system shall normally progress as per the normal Compliance Procedure.

If it is established that the system is not simply a name change or addition based upon an identical system, then the system shall be regarded as a new system and shall require to be progressed through the complete evaluation procedure.

The number of different name designations permitted for any specific DVDMS, shall not normally be limited.

8.12 Branding of Systems by Vehicle Manufacturers or Adding Additional Vehicle Models (Original Equipment Manufacturer Only)

The following shortened procedure shall apply if the Applicant has requested the Listing of a DVDMS, the name of which has been revised due to the system being offered for fitment to vehicles from a different vehicle manufacturer or to new vehicle models with respect to a previously existing Listed system.

The Applicant shall submit:

- All documentation and components as specified in the section on name changes/additions in the application form; and

- An explicit statement from a qualified representative of the vehicle manufacturer or importer requesting or giving permission to this name change/addition in the branding of the vehicle manufacturer.

Subject to a satisfactory evaluation by a test house, the system shall normally progress through to Phase 3 as per the normal Compliance Procedure.

In addition to the inclusion of the DVDMS or component name in the system list section of the Notification List, there shall also be a limited listing in the vehicle manufacturers' fitment policy section, specifying the fitment of the DVDMS or component on vehicle models, referenced against start and end dates and specifying whether the system is fitted on an optional or retro-fit basis.

If it is established that the system is not simply a name change or addition or that it is a new OEM vehicle model based upon an identical system, then the DVDMS shall be regarded as a new system and shall require to be progressed through the complete evaluation procedure.

8.13 System Derivatives

A system derivative is a system that has only minor changes with respect to a previously validated aftermarket system. Examples of acceptable derivatives may have depopulated circuit boards or other such minor variations. Also considered to be system derivatives are similar systems that are defined as 'build to specification' or 'build to print' from second source suppliers.

More complex systems, such as those with enclosure changes or significant component or circuit board modifications, are not normally considered to be acceptable system derivatives for these purposes and as such shall be treated as new systems.

The testing of an OEM or aftermarket system derivative may realise some economies in test timings and fees, although these are to be set by the test house and as such cannot be guaranteed. CAST reserves the right to oversee the level of validation that is deemed appropriate for any system derivative. This shall normally be considered and defined at Phase 1.

If the Applicant requests to have an aftermarket derivative of a DVDMS that has previously been issued with a Phase 3 Notification of Compliance included on a Notification List, then the following shortened procedure shall apply:

- The Applicant shall submit a short Technical File for all aftermarket DVDMS, describing any and all changes from the original DVDMS or systems submitted for testing. Any additional information supporting the application may be included in the Technical File;
- The Technical File shall be accompanied by one complete aftermarket DVDMS criteria sample with a statement relating this derivative system to an existing compliant system. For build to print variants, drawings shall be identical;
- At the discretion of the accredited test house, an agreed, shortened test may be acceptable. The test house may require further samples to be submitted on request, along with any outstanding items of documentation specified;

- If it is established that the aftermarket DVDMS is not simply a system derivative based upon a very similar system, then the DVDMS shall be regarded as a new DVDMS and shall require to be progressed through the complete evaluation procedure; and
- Appeals by the Applicant over system derivatives will be forwarded to CAST for a final decision, which shall be binding upon both the Applicant and the accredited test house.

8.14 Documentation Available to Applicants

Applicants may request the following documents from CAST:

- A Request for Evaluation form;
- The DVDMS criteria document; and
- List of accredited test houses.

8.15 Documentation Available from Test Houses

- A Questionnaire
- Schedule of fees from accredited test houses
- The Performance Test Specifications;
- Test documentation;
- The Terms and Conditions;
- A OEM Parts Submission Warrant (part of the OEM Questionnaire);
- The approval process.

8.16 Schedule of Evaluation Rates

The cost of the evaluation depends upon the classification of the submitted DVDMS.

Details of current fees are available directly on request from accredited test houses.

The quoted rates are based upon testing of a single system requiring one vehicle inspection and one set of system samples. Costs may be higher for more complex submissions based on multiple vehicle inspections and multiple system variants, combinations or optional components. These must be clearly defined before Phase 1 compliance is issued.

Accredited test houses may reserve the right to charge for additional meetings and consultation during the course of the evaluation that is considered to be above and beyond what is considered to be reasonable. This may possibly attract an administration charge.

The accredited test houses reserve the right to change rates charged for evaluation without prior notice, following notification to CAST. The exact rate or rates can be confirmed prior to application from specific accredited test houses at a specified Phase. All rates must be paid prior to the start of the

evaluation Phase. A submitted DVDMS shall not be Listed as DVDMS compliant until all outstanding rates are paid in full.

8.17 Reporting

8.17.1 Evaluation Progress Reports

The outcome of the evaluation shall be reported at the end of each of the three Phases, indicating either compliance (including partial) or non-compliance. During testing, the accredited test house, at its discretion, may issue periodic reports to the Applicant indicating progress and failures. It should be noted that accredited test houses are not obliged to issue interim reports on request. The final report at Phase 3 shall be submitted to CAST. On approval of the report, CAST shall instruct the accredited test house to issue a Certificate of Partial or Full Compliance. The accredited test house shall communicate the contents of the reports only to the registered Applicant or Applicants, meaning nominated secondary representatives.

The Phase 3 Certificate of Partial or Full Compliance report shall specify an alphanumeric code, known as the accredited test house Evaluation Number, which shall be specific to a Listed system. It shall take the format of:

- Code letter for test house;
- DVDMS – Generic type of system;
- i – major Issue level of specifications;
- n – internal Evaluation Number;
- mm – Month of first Listing; and
- yyyy – Year of first Listing, for example, 2012.

This code is unique to a specific Listed system and shall be quoted on Certificates of Installation and in any formal correspondence.

The accredited test house will also prepare a factual summary report of the key functionalities provided by each device in accordance with the DVDMS criteria to be included within the List to assist potential purchasers. The list of functionalities will be sufficiently generic to ensure that security benefits are retained.

8.17.2 Period for the Notification of Compliance

The evaluation shall normally be completed by issuing a Phase 3 Notification of Partial or Full Compliance statement within six months of the Application being submitted. The Notification of [Full or Partial] Compliance shall be issued by CAST, following notification by the accredited test house. If during the tests it is found that the requirements are not met so that at the end of the complete evaluation or individual phase, no Listing of the system under test can be granted, the Applicant shall be contacted as soon as possible. This may result in the extension of the complete evaluation period as estimated.

8.18 Use of the Names – Centre for Applied Science and Technology, Accredited Test Houses and Association of Chief Police Officers

The Applicant shall be permitted to use the name of the Home Office CAST or the accredited test house subject to the following provisions:

The Applicant may use only this statement or these statements, which may be reviewed at a later date in relation to the compliant DVDMS:

- ‘Complies with/meets the CAST DVDMS criteria for the management of driver and vehicle data for Emergency Services.

OR

- ‘As evaluated/assessed by the accredited test house for the testing of compliance with the management of driver and vehicle data for Emergency Services.’

In particular, the Applicant may not use, without the specific authority of the relevant organisation or organisations:

- The figurative mark or logo of the Home Office CAST or the accredited test house unless permitted to do so;
- The name or designation of ACPO or its related working groups or business areas;
- The figurative mark or logo of ACPO or its related working groups or business areas; OR
- ‘CAST, accredited test house [Name of test house], ACPO, approved’ or any similar form of words.

The Applicant shall be obliged to submit electronically to CAST for review purposes proofs of all publications, including advertisements, leaflets, packaging materials and labelling, which use the names of CAST and/or ACPO. If the publication is not in compliance with the required stipulated provisions, CAST or the accredited test house shall issue a written statement prohibiting its use and shall enforce its ruling, which if not resolved may ultimately result in the product and the company being removed from the List.

If the Applicant should become non-compliant or fail to comply with the DVDMS criteria and consequently the Notification of Compliance should be withdrawn, the Applicant shall no longer be permitted to use any form of the names of the Home Office CAST, the accredited test house, ACPO or any of the statements specified above.

8.19 Compliance Verification and Term of Validity

8.19.1 Quality Assurance

The Applicant shall:

- Demonstrate the existence of production procedures for effective quality control of the proposed DVDMS;

- Ensure that production test result data are recorded and results remain available for a minimum of seven years;
- Analyse the results of each test in order to verify and ensure the consistency of the DVDMS characteristics, making allowance for permissible variations in industrial production;
- Ensure that for each type of DVDMS, the tests prescribed are carried out on a statistically controlled and random basis, in accordance with the regular quality assurance procedures;
- Ensure that any set of samples or test pieces giving evidence of non-conformity in the type of test in question shall give rise to a further sampling and test; and
- Take all necessary steps to ensure DVDMS conformity of the corresponding production as rapidly as possible.

8.19.2 System Quality Audit

Throughout the ongoing Listing of a DVDMS on a Notification List, the accredited test house will periodically audit the total system, as Listed, by means of repeat inspections.

For the purposes of the repeat inspection, the Applicant for an aftermarket DVDMS shall be required to comply with the quality control audit trail procedure through the accredited test house upon request.

Alternatively, the accredited test house can select samples at random from production or from distribution locations.

During the repeat inspection, an investigation shall be conducted to determine whether DVDMS being manufactured still conform to the DVDMS as originally accredited in accordance with the Compliance Procedure, and whether these systems still comply with the DVDMS criteria.

A total system (as distinct from model) audit shall normally be conducted at two-yearly intervals to ensure that the quality and consistency of the system is maintained. The audit will be carried out every two years, from the date of first Listing irrespective of any additional vehicle models (OEM only) tested between times. The audit may also apply to the vehicle installations of Listed systems (aftermarket only). The audit will consist of full function test as defined in the criteria to include the Back Office functions, reports and other outputs. In addition, for OEM only, resubmission of the Parts Submission Warrant form will be required.

The process of auditing and associated costs shall be agreed between the accredited test house and CAST. These costs shall be met from charges levied by the accredited test house on the Applicant.

8.19.3 Audit Process

An external visual examination of components to compare the quality and construction against the reference sample held by the accredited test house shall be carried out. This shall include an examination of User Instructions and Installation Instructions.

A series of functional tests shall be performed, in accordance with the Performance Test Specifications to include in-vehicle and Back Office.

The manufacturer of the aftermarket DVDMS may be asked to demonstrate which version of software the randomly-chosen sample incorporates and to provide a complete listing, on request.

Provided that the construction, software and operation of the audit sample system is unchanged from the original test sample and the requirements of the appropriate functional tests have been met, a short report shall be filed indicating continued compliance.

If changes are found during the visual examination software audit or functional tests, the Applicant shall be informed. In order to demonstrate continued compliance, further testing may be conducted at the expense of the Applicant. Failure to agree with the testing will cause the Notification of Compliance to be withdrawn and the aftermarket DVDMS to be removed from the List with immediate effect.

It may be necessary to conduct any other tests that the accredited test house deems appropriate in order to assess specific changes to DVDMS.

If the sample examined does not correspond to the reference sample to include the Back Office and reports held by the accredited test house, is not compliant with the aftermarket DVDMS criteria or fails to meet the requirements of the tests performed, then the Test Authority shall have the right with immediate effect to forbid the Applicant from continuing to use the name of the accredited test house, the DVDMS name and other designated statements, as specified in the Compliance Procedure. If the non-compliances are of a serious nature, significantly compromising safety, security or reliability, or the system has been changed out of all recognition, then the non-compliant DVDMS shall be de-Listed immediately.

In this event the Applicant shall:

- Investigate immediately whether or not the method of production or the materials used show any irregularities. If this is the case, the Applicant shall correct these as quickly as is practicable;
- Send a written report to the accredited test house on the investigation conducted, the conclusions thereof and the corrective action taken; and
- Have the test that was performed with negative results, repeated at the Applicant's expense on additional – normally three – samples from the same production series.

If requested samples pass the repeat inspection successfully, the temporary denial of the use of the 'names', as specified in section 8.18, shall be cancelled. At this stage the accredited test house may request a name change for the system to differentiate it from potentially non-compliant previous samples. This may also apply to other forms of misrepresentation of the aftermarket non-compliant DVDMS name in the field.

If one or more of these requested samples fail to pass the tests successfully, then ACPO, CAST and the accredited test house shall continue to deny the further use of the name, as detailed in 8.18 and other designated statements. The Listing on the List shall then be withdrawn.

If the Applicant completely ceases to manufacture or market a type of system in accordance with these criteria, the Applicant shall inform CAST in writing immediately. As long as the DVDMS remains accredited, it may remain on the

List as detailed by section 8.3.2. Otherwise, the name of the system and associated details shall then be deleted from the Notification List.

8.19.4 Random Audit

In addition to the bi-annual system inspections, the accredited test house may, with the agreement of the Test Authority perform tests on Listed systems obtained independently from the field. The accredited test house shall inform the Applicant of any negative results of such random tests, and the procedure as defined in section 0 shall be initiated.

The process of random auditing and associated costs shall be agreed between the accredited test house and CAST.

8.20 System Changes

The Applicant shall have a nominated representative or officer responsible for documenting all changes made to the DVDMS in its lifetime. The representative shall consider the effect of each modification with respect to the ongoing compliance of the system. It should be stressed that if a modification gives rise to non-compliance or non-compliances at the system or random audit stage, the Applicant shall be liable to incur further test costs, possibly leading to the temporary or permanent deletion of the system name from the List.

The Applicant shall carefully monitor any modification to the system, installation or documentation for potential non-compliance with the DVDMS criteria. This shall include software changes. Each such proposed modification shall be reported in the following format to CAST on request. The modification shall be reported in advance of its implementation if likely to affect compliance. The following documentation shall be submitted to CAST:

- A Request for Evaluation form, specifying modified DVDMS;
- The appropriate evaluation fee;
- A brief description of the modification concerned and, at the request of the accredited test house, submission of the system, installation or documentation as modified;
- Drawings of the components or installation as modified; and
- The original drawings of the component or installation on which the modification concerned has been indicated, clearly showing all amendments, additions and deletions. All modifications shall be completely and accurately numbered and dated.

Upon evaluating the modification on the basis of the information supplied, CAST may refer the matter to the accredited test house for advice before informing the Applicant as to whether or not the modification concerned can be implemented in the production process by an administrative assessment without performing further testing, or whether a complete or partial revalidation shall be required, to be carried out at the expense of the Applicant, to demonstrate continued compliance. CAST will then update the List.

It is the responsibility of the Applicant to raise changes to the attention of CAST, if they may be judged to affect the compliance of the approved DVDMS with the DVDMS criteria. The Applicant shall also have the responsibility to, have in place procedures to control changes that may be made by installers in the field

when fitting or servicing the DVDMS. If it is found that this procedure is not effective and installers are changing the system in the field, leading to non-compliances, then the Listing of the DVDMS-compliant system shall be at risk. This control of changes will be subject to audit at random and via pre-planned inspections by the designated inspection authority, CAST or its accredited agents.

8.21 Warranty, Notification Incidents and Performance Information

Information on warranty incidents, to include, failures, accidents, interference, and de-Listing of companies, shall be supplied to CAST monthly, free of charge, from the accredited test house or its designated agent. These will be collated to monitor the take-up and use of the system. If the warranty or incident levels on a specific system or by a specific organisation are demonstrated to be high, then the Applicant shall be contacted to implement remedial action. After six months from this date, if no significant improvement has been observed, then CAST shall give consideration to withdrawing the Notification of Compliance and deleting the system from the List. This will be subject to a process of appeal.

8.21.1 Misrepresentation of Listed System Name

All Listed systems shall have easily identifiable and recognisable names. It shall not be possible for an organisation or user readily to confuse these names with similar names or non-compliant or unrecognised systems. If it is found that a Listed name is being misrepresented or may be readily confused with an unrecognised name, then consideration shall be given to withdrawing the Notification of Compliance and deleting the system from the List.

8.21.2 Discontinuation of Production

If the production or availability of the DVDMS is discontinued at any time, the Applicant shall be required to inform CAST and/or the relevant accredited test house as soon as possible. The List shall be amended to note the equipment being out of production but still accredited to the requirements of the DVDMS criteria for a period of no more than two years.

8.21.3 Withdrawal of the Notification of Compliance

If the Applicant fails to adhere to the Terms and Conditions of the Compliance Procedure, the Notification of Compliance shall be withdrawn with immediate effect. All systems falling under these circumstances shall be removed from the List managed by CAST, which shall under normal conditions give 28 days' notice of removal from the List. At the discretion of CAST, this period may be reduced. Under certain circumstances, CAST may decide to issue a suspension of recognition of a Listed DVDMS prior to investigations, which may result in removal from the List, or alternatively may lead to reinstatement of the full Listing. If the Applicant wishes to regain a Listing of the system in a compliant form, the Applicant may, at the discretion of CAST, be permitted to re-enter the Compliance Procedure at an appropriate point and at the Applicant's own expense.

If the Notification of Compliance is withdrawn from a previously compliant DVDMS in circumstances where there is considered to be a significant safety or security risk associated with the system, then CAST shall immediately issue a bulletin clearly drawing attention to the system deletion to all relevant parties.

8.21.4 Renewal of the Notification of Compliance

Subject to meeting the requirements of section 8.19 above, the DVDMS shall continue to be Listed. The Listing shall normally continue to be valid for a minimum of two years following the deletion of the criteria issue against which the DVDMS was originally tested. Specifically, a random audit may be conducted against any DVDMS (see section 8.19.4). Additionally, continued Listing shall be subject to an audit and annual Listing fee.

8.22 Audit and Annual Listing Fee

Each product system Listed will be subject to an audit and annual Listing fee, the rates of which shall be listed in the CAST schedule of charges. This fee will cover any ongoing audit of the systems, administration of information on usage, faults and random audit inspections.

The annual Listing fee is mandatory and is required to ensure ongoing quality control and standards are maintained following initial testing. This is essential to maintain confidence in the system.

Failure to pay the fee will result in removal from the List and may require retest or administration fees to be paid prior to reinstatement onto the List.

Partial compliant systems will be required to be fully retested every year and therefore will not be part of the audit and re-Listing process. This both recognises those manufacturers that have achieved full compliance but also provides a time-limited option for those manufacturers wishing to work towards that aim.

8.23 System Specification and Classification

The DVDMS specification and classifications are specified in chapters 2 - 7 of this document.

8.24 Liability

CAST, ACPO and accredited test houses and their associates accept no liability, howsoever arising, for any personal injury, loss, or damage caused by any of the systems or services that may, from time to time, be supplied having been Listed as compliant with the DVDMS criteria.

8.25 Performance and Environmental Test Regime

The components of the DVDMS in-vehicle device shall be tested in accordance with the test methods and parameters laid down in the Performance Test Specifications (section 8.25.1), which support these criteria. Test houses shall draft Performance Test Specifications in support of this standard, which shall be agreed with the Authority (CAST), in advance of their adoption. These practically validate the system and components for security, safety, reliability, functionality and documentation as laid down in these criteria.

It is the strong preference of the Test Authority that, where appropriate, test houses are accredited to ISO 17025, which is the standard used by test and calibration laboratories. This standard is applicable to test houses carrying out environmental testing

For OEM systems, the performance criteria for success shall be the same as applied for other OEM systems, or parts fitted to that vehicle.

8.25.1 In-Vehicle Testing

Components to be tested include:

- Fixings;
- Brackets;
- Protective shields;
- Audible or visible indicators or displays;
- Wiring;
- Connectors;
- Fuses;
- DVDMS control equipment;
- Electrical power source backup systems;
- Antennae;
- Coded keys;
- Coded key receptacles, locks or receivers;
- Audible or visible indicators for change of status;
- Connection to esCAN;
- Data storage and protection;
- In conjunction with the Back Office:
 - Reports;
 - Data communication;
 - Search capability;
 - Security;
 - Audit;
 - Access control;
 - Geofence;
 - Alerts;
 - Movement detectors to include g-force;
 - Visible warning device;
 - Audible warning device; and
 - Location technology.

8.25.2 Additional/optional Equipment to be Tested

Cameras- where linked to DVDMS

8.25.3 Changes of State and Failure Modes

The components of the DVDMS shall demonstrate environmental compatibility with regard to the following conditioning and shall operate without failure under it.

A failure shall be considered to be an inadvertent change of state, or non-functioning status following the test, depending on the test. A failure shall also be considered to be mechanical or electrical damage which may lead to subsequent failure at a later time.

For the avoidance of doubt, changes of state of the DVDMS shall be considered to be:

- Driver identity: set to unset;
- Driver identity: unset to set;
- False alert signal;
- Operation or non-operation of other output signal such as radio transmission, audible or visible indications;
- Corruption or loss of data; and
- Failure to communicate to the Back Office.

8.25.4 Performance and Environmental Testing Failure

Suppliers will be expected to submit systems for evaluation that have already been tested by a recognised test house or in house processes to meet the performance tests set out below. Evidence of such testing will be provided to the Accredited Test House for assessment and validation. Repeat testing is not normally required unless issues are raised with regard to the test procedures or results. Where this occurs additional testing or validation may be required, which will only be undertaken with the agreement of all parties to include CAST. Where such tests have not been performed prior to submission, they will be required to be carried out by the accredited test house.

A failure is considered to be an inadvertent change of state, non-functioning status, corruption or loss of data, following the test, depending on the test. A failure is also considered to be mechanical or electrical damage, which may lead to subsequent failure at a later time.

Failure in accreditation, audit or dip testing shall result in a report to CAST, which shall consider remedial action, issuing a warning or de-Listing the relevant system.

The Test House shall make reference to its performance test specifications for complete parameters and test procedures. Test parameters shall be at such a level as to validate the DVDMS for a universal fit automotive environment. Test applications shall be determined as a function of installed component locations.

Environmental tests:

- Dry heat BS EN 60068-2-2:1993, Test B, Dry heat, maximum temperature of 85C for 72 hours;
- Cold BS EN60068-2-1:1993, Test A, Cold, -20C for 72 hours;
- Cyclic temperature and humidity BS EN60068 –78: steady damp test 30C 93% humidity 12 hours;
- Salt mist corrosion;
- Fire Resistance;
- Vibration, operational and endurance BS EN60068 or Vehicle Security Directive 95/56EC;
- Impact test - Resistance to crush or damage by striking 80g for 0.1mS;
- Impact Resistance of data connections to impact Resilience of data connections MIL – D – 38999;
- Impact Resistance of data storage- to sudden deceleration - Resistance for data so storage and processing in device on sudden acceleration Impact Resistance 80g for 0.1mS;
- Free fall (Driver Identity Device – DID) 1 metre drop test;
- Temperature shock (DID);
- Electromagnetic compatibility testing EMC –The DVDMS must meet 104/2004/EC; SAE J 113 part 25 and EN61000-4-20 provide additional test methods Transients as ISO 7637 in 104/2004/EC and BS EN61000-4-2 for ESD. In addition DVDMS must not interfere with mobile radio AES Specification 5 (1) Automotive Conformance Specification 5 (issue 10) Revised December 2007Automotive EMC Directive for method but 75 V/m immunity level;
- AES Specification 5 is a specification relating to the EMC performance of a vehicle mounted, electrically powered equipment, designed for use by the Police & Fire Services of England and Wales;
- Vibration – the DVDM device must meet 95/56/EC, 5 Hz to 500 Hz max amplitude 5mm peak to peak up to 3g. Frequency variation of 1 octave per minute using 10 cycles in each of 3 axes and a Shock test such as BS EN 60068-2-31 using 1 metre drop test 3D; and
- Water and dust resistance – the DVDM device shall have as a minimum, IP54.

8.25.5 Tracking/Field Trials

A test vehicle shall be tracked over a specified predetermined route representative of the operational environments relevant to emergency service vehicles operating in the UK, of not less than 10 km selected by the accredited test house to assess DVDMS functionality, tracking and location performance and to include the use of multiple close parallel routes, which will additionally require the Back Office to determine exactly which route is being used by the test vehicle. This shall include areas of low or no coverage of location or communication, in order to fully test effective re-connection and re-send of information capability.

The route and number of repetitions is to be determined by the test house. The route is expected to provide the full range of conditions, driving events and driver behaviour that will fully test the functionality of the end to end system and to ensure that it is repeatable.

NB: Given the requirement for activation of emergency service warning equipment, harsh braking and exceeding speed thresholds, this type of testing is expected to take place in off road but realistic conditions.

This trial may also be conducted using a simulator (such as at the INNOVITS test facility at MIRA) where this can be shown to robustly test and evaluate the performance of the DVDMS in a more effective or cost effective way.

The field trials will cover all aspects of the functionality to include alert generation for:

- Geofences – entering and leaving
- Speed thresholds
- Braking thresholds
- Cornering thresholds
- Idle times
- Driver identity accuracy
- Impact sensors
- Data accuracy
- Data Retention
- Activation of Emergency service equipment
- Connection to esCAN
- Communication, receipt of processing vehicle CAN data as listed in the OBSVA
- Priorities for data
- Driving environments

The test plans for DVDMS will be produced BY CAST in conjunction with the Accredited Test House. These will include testing developed as part of the DVDMS field trials. These provide guidance on the type and extent of testing that has to be conducted. It is possible, with the permission of CAST, for companies with live systems in operation with the emergency services to provide test data in the format of the test plans, to provide the corroboration of the tests. This may/would reduce the requirement for repeat testing by the test house. This is solely at the discretion of CAST.

8.26 Acknowledgements

The Home Office, AES and ACPO ITS Working Group wish to acknowledge the valuable assistance received from the National Association of Police Fleet Managers (NAPFM), ACPO, police forces, motor vehicle manufacturers and

importers, emergency service equipment manufacturers and importers, the Motor Insurance Repair Research Centre (Thatcham) and the UK and international technical bodies, institutions and associations that participated in this project.

Appendix A – Data Dictionary and Coding for Emergency Service CAN (esCAN)

The ACPO ITS Working Group, in discussion with the One Box Consortium membership, has had to find a suitable code set for the esCAN system to operate to. This code needed to be open and freely available to all Consortium members to ensure fairness and an equal commercial base to work from. ACPO ITS and Consortium members identified CAN in Automation (CiA) because they had begun work on a CAN standard for special vehicles, including police.

About CAN in Automation (CiA)

In 1992, several companies founded the CiA non-profit organization in order to provide technical, product and marketing information. The aim was to promote the image of CAN and to provide a path for future developments of the CAN protocol.

Approximately 560 companies are currently members of this international CAN user and system manufacturer group. The CiA group is registered in Nuremberg, Germany as non-profit organisation.

Representatives of the CiA actively support the international standardisation of CAN protocols and CiA members develop specifications to be published as CiA specifications. CiA specifications cover physical layer definitions as well as application layer and device profile descriptions.

Companies are encouraged to become members of the CiA should they wish to secure access to the draft standard prior to it being made available publicly.

Access to the CiA can be found by following the link below:


<http://www.can-cia.org/>

CiA 447 Standard

The CiA 447 standard and how it covers the requirements of esCAN is set out in the table that follows.

The additional requirements that have been marked “TBD” (to be defined) will be developed between ACPO ITS Working Group and CiA, which should deliver the full standard within the next 24 months.

The table will give those organisations striving towards One Box Single Vehicle Architecture-compliant systems a basis to work from. These organisations are encouraged to enter into a dialogue with the ACPO ITS working group to ensure their needs are met as the standard evolves.



Home Office Centre for Applied Science and Technology
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051
Fax: +44 (0)1727 816233
Email: CAST@homeoffice.gsi.gov.uk
Website: <http://www.homeoffice.gov.uk/science-research/>
ISBN: 978-1-78246-002-2