Civil Traffic Enforcement

Certification of Approved Devices

The UK will fulfil its obligation under Article 12 of Directive 98/34/EC when this guidance is officially published.

Civil Traffic Enforcement

Certification of Approved Devices

Table of Contents

Table of Figures

Civil Traffic Enforcement

Certification of Approved Devices

Chapter 1 General Introduction

1.1 Introduction

Parking restrictions, bus lane use and certain other moving traffic contraventions are increasingly being enforced by local traffic authorities who have sought and been granted civil enforcement powers.

Changes to legislation are harmonising the civil traffic enforcement procedures throughout England and include provisions for the production of evidence from Closed Circuit TV cameras and associated recording equipment. Such devices not covered by an existing recognised approval must be certified as "approved devices" by the Secretary of State for Transport. The Vehicle Certification Agency has been appointed to do this on his behalf.

This document describes the certification procedures and requirements. It underpins, and must be read in conjunction with, applicable legislation concerning "approved devices" made under the Transport Act 2000 or the Traffic Management Act 2004 as appropriate, which prescribe the fundamental requirements that must be met. This document details the considerations which, when applied collectively, will demonstrate whether equipment is fit for purpose and meets the statutory requirements. (The Department for Transport and local traffic authorities will produce guidance on other operational aspects of civil enforcement).

A device may be designed and produced by one manufacturer or may be a system specified by a system designer incorporating sub-systems and/or equipment produced by one or more manufacturer.

Civil enforcement reduces the burden of proof for contraventions from 'beyond reasonable doubt' to 'the balance of probability'. Detection can be via equipment that is manually controlled, or that is triggered automatically. Increasingly it uses digital technology. This document is concerned with ensuring that the certification of such devices or systems meets the 'balance of probability' criterion, although, some of the requirements may go beyond this and meet the 'beyond reasonable doubt' principle. The overall objective is to ensure that evidence produced by devices certified in accordance with the procedure described shall be defensible when taken to adjudication.

Consideration is also given to the need for all those involved to be able to demonstrate that the operation of the certification process is transparent, fair and ultimately defensible in law, and that the individual applications also satisfy those criteria.

Following this introduction there are four chapters that describe the certification procedure:

Chapter 2 explains how applications for certification should be made and defines how subsequent changes to the system should be dealt-with.

Chapter 3 covers the particular considerations that apply to attended systems - i.e. those that record evidence as seen by an operator at the time a potential contravention is observed.

Chapter 4 covers the considerations that apply to unattended systems - those that record potential contraventions automatically for subsequent review.

Chapter 5 contains annexes of abbreviations and terminology and as otherwise described in the body of the document.

In order to allow for the expected range of technologies that are likely to be used and to allow for future-proofing, some of the certification criteria are presented as guidance. Any relaxation from the criteria specified herein will require a full justification during certification. Of necessity, all sections of this document are not specific about the technology to be used for contravention recording, target imaging and evidence recording. As a result, manufacturers, test houses and purchasers shall agree how the tests in this document shall be applied to the specific technology used in individual products.

This document is the result of consideration by a number of authorities, manufacturers, and organisations involved with the technology or in enforcement activities generally as listed in Annex 2.

1.2 The Policy Context

The overall policy on civil traffic enforcement is derived principally from:

- The 1998 White Paper *"A New Deal For Transport",* which set out the key themes for an integrated transport policy.
- The Transport Act 2000, which provided powers to prescribe civil enforcement arrangements for bus lanes.
- The 2004 White Paper "*The Future Of Transport*", which developed the 1998 strategy.
- The Traffic Management Act 2004, Part 6 of which provides for a single framework in England for the civil enforcement of parking, bus lanes, some moving traffic contraventions and the London Lorry Ban. (Note: this will replace local legislation in London, under which civil enforcement has previously operated; and legislation on civil bus lane enforcement under the Transport Act 2000).

1.3 Scope

This document applies to the certification of devices used for civil traffic enforcement under the following primary legislation:

Section 144 of the Transport Act 2000 - Civil penalties for bus lane contraventions.

The Bus Lane Contraventions (Penalty Charges, Adjudication and Enforcement) (England) regulations 2005 and The Bus Lanes (Approved Devices) (England) Order 2005 SI No: 2005/2756 apply until such time as they are replaced by legislation under the Traffic Management Act 2004 - see below.

Sections 72 and 73 and Schedule 7 of the Traffic Management Act 2004 - Civil penalties for road traffic contraventions.

Legislation to implement these provisions is being prepared. It will cover the following:

- parking contraventions
- bus lane contraventions
- London lorry ban contraventions
- moving traffic contraventions - as listed in Annex 3

Chapter 2 General Requirements for Certification of Systems

2.1 Certification Process

2.1.1 Technical Construction File

Applicants should document their systems in a Technical Construction File, which is submitted to the Secretary of State to gain certification. The suggested contents for the file are listed in section 5.5. There is nothing to stop the file containing more information than is listed.

The file should be sufficiently detailed so that important aspects of the system outlined in this document are clear and may be assessed. Essentially the file should provide at least the necessary evidence that the design is in accordance with relevant requirements.

It is intended that the file should be maintained along with any future changes to the system as is outlined in section 2.2 below.

2.1.2 Test House Tests

Where a test house is employed to test a new system, they shall record in the technical construction file compiled by the applicant details of the tests carried out. This file shall then be augmented with the site specific testing records made as a result of on-site commissioning of the system. These site specific records shall be signed off by a competent person that may be either a representative of a test house appropriately qualified to certify site based testing or a experienced and competent member of staff from the enforcing authority or maintenance organisation.

2.1.3 Legacy Systems

Where a legacy system is to be certified, the technical construction file shall include documents containing the details described in paragraph 2.1.1 above. Evidence of previous certification or approval (where available) should be included. Upon first certification, the system shall be tested and certified and the test records included in the technical construction file.

2.1.4 Applications to the Secretary of State

The Secretary of State will decide whether to issue an approval to the applicant on the basis of the Technical Construction File and any other exchanges that take place subsequently.

2.2 Modifications to Certified Equipment

This section describes the requirements for the management of changes and modifications to certified traffic enforcement systems. All modifications (regardless of category assessed) to certified systems should be maintained in the System Technical Construction File.

The applicant shall maintain records of the serial numbers or dates of delivery of equipment that is manufactured to a revised Technical Construction File.

2.2.1 Requirements

It is a requirement that all modifications that are made to certified system are notified to the Secretary of State for Transport. This should be by ensuring that the Technical Construction File is kept up to date. The method of notification is subject to agreement by the Secretary of State.

Applicants are required to assess whether the change is a Significant Change, a Minor Change or a 'Supplier Equivalent' change. The three categories are defined below.

The Secretary of State for Transport will take into account the assessment of the applicant's, but reserves the right to reclassify any modification at his sole discretion. Further evidence may be requested to justify any classification.

2.2.2 Significant Change

A significant change is any modification made to an enforcement system that increases or changes its **functionality**. The replacement of subsystems or components that change the way the system performs its task are considered significant changes. In general, these will require fairly major changes to the system explanations and specifications in the Technical Construction File. Where such change occurs, a full recertification is likely.

Changes of software version or variant are considered significant changes.

2.2.3 Minor Change

Changes which may improve the **performance** of subsystems or components, but where the function carried out within the overall system by them has not changed are considered minor changes. This is unless an increase in overall system capacity is achieved.

Software maintenance or upgrades where the functions carried out by the software have not changed (or been added to) are considered minor changes. These include low-level driver updates and bug fixes except those responsible for any of the following areas: Cryptography, Evidence authentication, Enforcement Schedules and Secure interfaces.

In general, where a minor change is made, limited or no recertification testing will be required. The extent of this recertification will be subject to agreement between the body seeking equipment recertification and the Secretary of State for Transport.

2.2.4 Supplier Equivalent

A supplier equivalent change is one where a generic component of the enforcement equipment is replaced with a functionally equivalent item from the same or another supplier. In order to be considered functionally equivalent, the component shall have sufficiently similar performance in terms of value and tolerance. A supplier equivalent change shall not usually be subject to recertification. However, the Technical Construction File shall be maintained accordingly.

No software modifications are permitted in the supplier equivalent modification category.

2.2.5 Variation

These provisions are intended to provide a rigorous control over the configuration management of certified enforcement equipment in order to maintain confidence of all

stakeholders. It is not the intention of these requirements to restrict the Secretary of State unduly and it remains within the discretion of the Secretary of State to nominate a reduced level of testing wherever that is deemed appropriate. Some examples of where this discretion could be used include (but not limited to):

- Where elements of the design being submitted have already been part of a certified system and are used unchanged
- Where elements of the design are outside the scope of a significant change and are demonstrably unaffected by that change
- Where compliance with certain requirements is intrinsic to components within the enforcement system being certified.

In these cases, it may be acceptable for the Secretary of State for Transport to accept a reduced level of recertification. Applications for this test scope reduction should be agreed on a case-by-case basis before the start of certification.

2.3 Certification Procedures

Manufacturers or designers seeking civil certification by the Secretary of State for Transport should in the first instance contact:

The Vehicle Certification Agency.

1 The Eastgate Office Centre,

Eastgate Road,

Bristol. BS5 6XX

Telephone: 0117 951 5151

e-mail: civil-enforcement@vca.gov.uk

Web: http://www.vca.gov.uk/

Chapter 3 Requirements for Attended Systems

3.1 Imaging Devices / Cameras

3.1.1 Image requirements

3.1.1.1 Context View (CV)

The context image shall provide a clear, sharp and free of motion blur image of the vehicle in its context within the road environment. The context image shall have the same resolution as the CCTV camera as defined in 3.1.2.1 below

3.1.1.2 Close-up View (CUV)

The close up image shall provide a clear, sharp and free of motion blur image of the VRM in its context within the vehicle committing the contravention. The close up image shall have a resolution that allows the VRM to be read unambiguously.

3.1.1.3 Frame rate

The system shall record close-up and context views. The frame rate of the evidence pack image sequence shall be a minimum of 5 frames per second or equivalent with no two images being more than 200ms apart.

3.1.2 Minimum Technical requirements for CCTV Cameras

3.1.2.1 Resolution of the CCTV Camera

The camera shall be capable of recording video at the standard PAL video resolution of 720 x 576 pixels. However cameras recording PAL standard format video in the UK are normally defined as having a resolution of 752 (H) x 582 (V). Cameras may also use a higher resolution.

3.1.2.2 Zoom Capability of the CCTV Camera

Most CCTV cameras will use an optical zoom lens to zoom in and out – at the full standard resolution for that camera. Where a digital zoom facility is used, the full video frame obtained shall not be less than the equivalent of 20% of the resolution of the standard PAL resolution (i.e. 144 x 115 pixels) at the point of video capture on the camera. This is the equivalent of a 5x digital zoom on a PAL resolution camera – but may be the equivalent of a larger digital zoom on a higher definition camera.

3.1.2.3 Low Light Performance

The CCTV camera shall be capable of producing usable video at 2.0 lux. This should allow enforcement to be carried out even with average quality street lighting.

3.1.2.4 Environmental Operating Conditions

Attention should be given to the environmental operating range of the camera equipment (e.g. temperature, humidity, etc.) indicated by the manufacturer prior to it being procured or used for traffic enforcement purposes. Cameras shall not be used for enforcement outside the manufacturer's indicated acceptable operating conditions.

3.1.2.5 Electromagnetic Compatibility

The CCTV camera shall comply with the current European legislation that applies to all apparatus liable to cause electromagnetic disturbance, or the performance of which is liable to be affected by such disturbance. (That legislation prescribes the relevant protection requirements, compliance procedures, and the technical documents and/or marking that must be associated with the equipment).

3.1.3 Factors for consideration in relation to the procurement, siting and operation of CCTV cameras and associated systems

The following information has been produced to assist the providers of Traffic Enforcement systems. This is based on current best practice and user experience, but is ***not*** a requirement for the certification of systems.

3.1.3.1 Imaging Device, CCTV Camera

Most current CCTV cameras are likely to employ a CCD or CMOS device to obtain the image. Previously only 1/2inch CCDs were capable of recording adequate quality and resolution images. However, with emerging technologies and miniaturisation, smaller imaging devices (e.g. ¼ inch CCDs) are likely to be capable of providing high quality images at an appropriate resolution that would meet the requirements for enforcement.

3.1.3.2 Camera / lens arrangements

Traditionally professional quality CCTV cameras have come as two part combinations – with a camera body (including a defined lens mount – such as a 'C' or 'CS' mount) – and a separate lens (for which many options would be available). This arrangement allows for a wide range of camera combinations and facilities that would be suitable for enforcement. However there are now also various miniaturised integrated camera/lens units that can provide high specification imaging facilities and that may meet the requirements for enforcement in a smaller sized unit that is more consistent with the environmental aspirations of many Local Authorities. Either camera arrangement is acceptable in principle, subject to meeting the other requirements for providing high quality images for use in enforcement.

3.1.3.3 Zoom Speed

The time required for a camera to zoom between the CUV and the CV should be sufficiently low to allow satisfactory operation across the required range of the enforcement zone. Particularly at sites where there are a large number of contraventions, or where long enforcement zones are being monitored, fast zoom lenses can ease the camera operator's enforcement duties and may be particularly effective in operation.

3.1.3.4 Shutter Speed

The camera may need to be capable of working at fast shutter speeds, to reduce blurring of the video images of vehicles passing the camera. Depending on site specific conditions, a shutter speed of between 1/250 and 1/1000 second may be necessary to obtain clear images of VRMs - to prevent images becoming blurred through movement of the vehicle during the exposure (of each video frame). However this may cause problems in low lighting conditions. Therefore, for maximum flexibility of operation, the CCTV camera should be capable of being (remotely) switched between different shutter speed settings. Typically this may be done using software and/or hardware activated by an operator / observer at the CCTV control room. Large horizontal or vertical angles of view (from oblique and/or high locations) may require video to be recorded using the faster shutter speeds indicated. (Note – whilst all cameras have a shutter speed, this generally relates to an electronic 'virtual' shutter – not a physical camera shutter).

3.1.3.5 Stability of the CCTV camera during PTZ operations

On some cameras the quality of the video recorded whilst panning, tilting or zooming may be reduced or become blurred. This may depend on the camera/lens combination, the motor equipment performing PTZ operations, the stability of the column that the camera is mounted on – and other factors (such as the height of the camera – and current weather conditions). This may restrict useful images being recorded for enforcement purposes except when the camera is virtually stationary in the CUV and CV views. However, faster shutter speeds may resolve this problem.

3.1.3.6 Quality of the camera and lens (or the camera/lens combined unit)

Very high quality camera/lens combinations may make it possible to clearly identify a VRM with a less zoomed-in view. Conversely, (relatively) lower quality equipment may require longer (and possibly faster) zoom lenses to show the VRM as a higher percentage of the frame width in order to compensate for the reduction in quality.

3.1.3.7 Quality of other system components

In specifying a camera enforcement system, consideration needs to be given to all the components of the system, as these could have an effect on the required specification for CCTV cameras. Overall, the quality of the recorded video (and any extracted still images from the video stream) – may depend on the quality of the camera/lens combinations; the communication systems and cabling between systems; the recording equipment; and the facilities for grabbing still images from the video stream. If there is any noticeable degradation of the video recordings when re-played, (by comparison with the video stream as observed by an operator) or the images grabbed, the quality of some components of the full system may need to be re-assessed.

3.1.3.8 Electronic Enhancement of Video and Still Images

Most cameras will provide some automatic and manually operated facilities to improve the quality of the image being viewed (and recorded) – such as auto-iris (brightness), white balance, contrast and saturation levels. Some cameras may provide other more advanced facilities (e.g. to reduce headlight glare). Whilst video recordings should ***not*** be adjusted or enhanced after they have been recorded, it is normally necessary to use some additional processing (e.g. using image filtering technology) to produce acceptable still photo images from the video stream. This is particularly necessary for recordings from analogue video

streams where some form of de-interlacing is necessary to produce acceptable still images of moving vehicles.

3.1.3.9 Environmental Conditions

CCTV cameras may be required to operate in a wide range of operating conditions. However temperature, humidity and other factors can affect camera operation and the clarity and accuracy of the images produced. When procuring (or using existing) cameras, consideration should therefore be given to the environment in which the camera will need to work, so that it is not necessary to operate the device outside the manufacturer's indicated operating conditions for enforcement purposes.

3.1.3.10 Maintainability

It is essential that CCTV cameras on-street are inspected and cleaned regularly, and maintained as necessary, to ensure that clear video recordings are obtained. It might therefore be desirable for the same or similar cameras to be used at more than one site – to increase the ease and consistency for operation and maintenance.

3.1.3.11 Other Site Related issues:

3.1.3.11.1 Height of the camera

This affects the vertical angle of view of the VRM, and it's readability by an observer.

3.1.3.11.2 Horizontal angle of view (in relation to the direction of traffic)

This affects the horizontal angle of view of the VRM, and it's readability by an observer. However it also increases the potential for the speed of a vehicle to cause blurring of the images recorded on video. More oblique angles of view are therefore more likely to require faster shutter speeds to obtain clear video images.

3.1.3.11.3 Proximity of the Enforcement Zone

If the enforcement zone is very close (just underneath the camera) – or too far away, there may be problems obtaining satisfactory video images. A video zone very close to the camera may require fast combined PTZ operations – particularly if the enforced area is not directly in line with the camera - and this may be difficult for operators to carry out. Distant observations may occasionally suffer from mist/fog/haze reductions in visibility that could make VRMs more difficult to read.

3.1.3.11.4 Street Lighting

Where street lighting is poor, it may be more difficult to read a VRM and also to identify a vehicle type (make and model) in hours of darkness or poor light – which is necessary for enforcement purposes. Improvements to street lighting – and cameras with better low light sensitivity - could overcome these problems.

3.2 Time and date

The enforcement equipment shall maintain a system clock that is regularly synchronised to a nationally recognised standard clock. The system clock shall, at all times, be within 10 seconds of coordinated universal time (UTC) as disseminated in the United Kingdom by the

National Physical Laboratory using the MSF clock. The system clock shall be synchronised with a suitable standard clock a minimum of once in any 14-day period

3.3 Transmission systems

Transmission systems should be demonstrably transparent to video and telemetry signals and should be immune to third party interference.

3.4 Recording Systems

3.4.1 Digital Recording with no data redundancy or recovery facilities

Where recording takes place on a system with no real time data recovery or data redundancy facilities, two simultaneous recordings onto separate media shall be made at the time of capture. It is preferred, but is not a requirement, that the two copies be made after conversion to the digital domain. In this scenario, it would be acceptable for the second recording to be made at lower resolution and frame rate or at higher compression settings than the first. In the case that the second recording is made at lower resolution, frame-rate or at higher compression, then once a decision to proceed with issuing a PCN is made, (after Review of the contravention), a master copy of the evidence shall be made on a second media.

3.4.2 Digital Recording with Data redundancy & recovery facilities

Where an enforcement system provides digital facilities for recording video data such that the system provides Security, Integrity and Reliability, (see definitions below). The system may be considered to comply in full with the requirement for dual simultaneous recording - as the recorded data is securely stored on a minimum of two independent storage devices, and recovery of data should be possible even if one or more storage devices fail.

3.4.2.1 Method for Single Recording systems

3.4.2.1.1 Initial Process

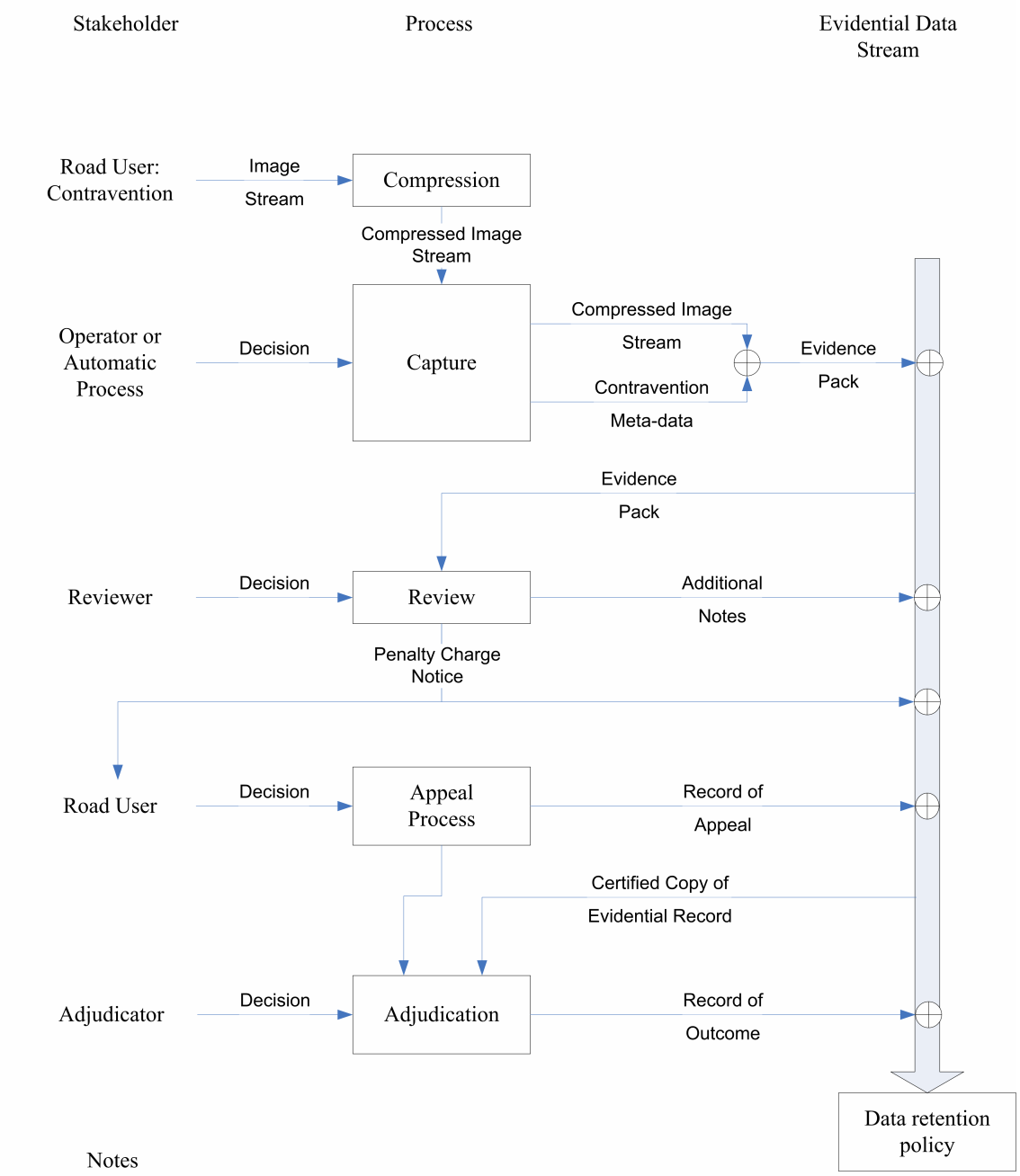
a) Record video from CCTV Matrix – of a whole Enforcement session - onto a secure server (or other high volume digital storage device) – at the time of observation.

b) Identify start and end of Contraventions during enforcement session – using start/end controls - that are tagged (or otherwise identified) on the recording.

c) Clips of the Contraventions (from the start to the end point of each contravention – possibly including an additional period of video before and after each clip) are copied to a Traffic Enforcement Video Store – TEVS - (possibly with related text contravention data) – on a secure server (or other secure high volume digital storage device). The copying process for producing these video clips should ***not*** compress or otherwise modify the format or quality of the original video recordings. See figure 1.

Figure 1 Traffic Enforcement Data Flow

This data flow diagram illustrates the typical process for a PCN taken to appeal. As such, a number of the processes may be repeated a number of times (e.g. the review process) or may be omitted completely (e.g. the appeal and adjudication processes if the PCN is not appealed).



Notes

1 ⊕ Incoming information streams added to give output stream

2 ⊕ Incoming information streams added to evidential stream

3 Information that is added to the evidential stream shall not be changed or deleted until data retention policies dictate that deletion / destruction is permitted. Normally this is a defined period after the PCN is resolved (either paid or withdrawn).

4 Compression of the images used for evidential purposes should ensure that close-up and context views remain fit for purpose. It is recommended that temporal compression techniques are not used for evidential data. Lossy compression techniques may be acceptable provided that the fitness for purpose requirements are met.

5 The decision to capture a contravention may be made by either an operator or, in the case of an unattended system, an automatic detection process. For details the requirements of the automatic contravention detection processes in unattended systems, see the relevant part of Chapter 4

d) Each clip is reviewed to assess if the contravention is an actual violation of the TROs at the site. If necessary, earlier or later video (not contained in the clips) might be available for viewing at this time to clarify whether the Contravention is an actual violation.

e) Still images of each ***confirmed*** Contravention are selected, extracted (grabbed) and stored with (or linked to) the Contravention data records (that are likely to be in text format) during the Contravention Review process.

f) Contravention data (including still images from the video) is sent for processing – so that a PCN can be issued to the owner / driver of the vehicle (note – the PCN issuing process is ***not*** described further here as it is outside the scope of this certification process).

g) Video recordings of the full enforcement sessions may be deleted or overwritten after the Contravention Review process is complete – as the Contravention video evidence is now securely stored in the TEVS.

h) **If there is an appeal against the PCN**, a further video copying and transfer process is required. This is described in Section 3.2.3.1.2 below.

i) If there is no appeal, and the PCN is cleared or paid, all video, video clips, and contravention data should be deleted after the PCN is cleared or paid (although this should be after an appropriate archive period).

3.4.2.1.2 Where Working copies are required

The following process for creating and storing further copies of Contraventions (on removable media – or in an electronic format that may be encrypted and sent by e-mail or by some other form of electronic transfer) is only likely to arise if there is a request to view the video of the Contravention, or if the PCN is referred for adjudication: -

a) The Master copy is effectively considered to be the video clip which is stored on the TEVS. A separate Master or Working copy of the contravention would ***not*** normally be produced on removable media.

b) Working copies of a Contravention are produced directly from the Master copy which is held on the TEVS – **if and when these are required** for viewing; for sending to the adjudicator, the appellant (and/or their representatives); for use in the adjudication hearing; or for supplying to other approved parties as determined in local procedures – and the relevant Code of Practice. Unless specifically required (for example - for display only to authorised viewers on a web site), the copying process for producing these working copies should ***not*** compress or otherwise modify the format or quality of the original video recordings. The copies may be on a removable WORM medium (CD-R, DVD-R, or similar) – or a computer file, for example – for sending by e-mail (which may be encrypted) or for use to display on a web site (to authorised persons).

c) Once the PCN has been settled at adjudication, all video recordings, video clips, WORM media and contravention data should be deleted or destroyed (although this should be after an appropriate archive period in accordance with data protection legislation).

3.4.2.1.3 Data Safeguards

As all the contravention data in this process may be held within a single digital recording system, additional safeguards are required to protect the evidential quality of the data. These safeguards should be the digital equivalent of the physical safeguards used to protect contravention data on Analogue systems using removable media. The following provisions are general requirements. Other requirements may be determined by an adjudication service, in local system procedures or in a relating Code of Practice.

3.4.2.1.4 Integrity

The system must provide facilities to ensure that if (image) data is amended or altered in any way, the changes are detectable. Typical examples might include hash functions or watermarking of the data. Where a hash function is used, a change to the data would show up as an error, whereas with a watermark – the watermark would normally become visible in some way if the data is altered. Other methods may also be viable.

3.4.2.1.5 Security

The system must provide a means to protect the data and system information so that only people who are authorised to access, use, edit, copy or delete the data have access to it for these purposes. Typically, this may involve a hierarchy of password protection so that individuals are only able to carry out the activities for which they are authorised. Physically, this might also require the systems to be located in secure areas so that only authorised operational and maintenance personnel can get access to these computer systems.

If the recording system is connected to a PCN processing (or other) system via a network or the Internet, the contravention and video data must be secured so that it is inaccessible via this connection except to authorised users and systems. This may require the use of firewalls, data encryption and/or other measures to prevent unauthorised access to the contravention evidence.

Where data is released from a secure environment, (e.g. to send the data to an adjudicator), this is likely to require other forms of protection. Where data is sent electronically (e.g. by e-mail or using FTP transfer), data encryption is likely to be required – to ensure that unauthorised persons cannot see or amend the data. Data released on removable media should be secured in a WORM format (i.e. the DVD, CD, etc. should be 'closed' – so that it is not possible to amend the data on the media).

3.4.2.1.6 Reliability

It is important that should an equipment failure occur on the computer system - or on one or more of the storage devices, the computer systems should (so far as is possible) continue to operate, and that enforcement data is retained – or is available on the system in some other way such that it is recoverable. Typically this may be achieved through the use of RAID server technology. However regular data backup facilities may be an alternative or complementary means of achieving this objective.

It should be noted that where suitable digital storage arrangements are made, using RAID servers or an equivalent technology, and there is a sufficient degree of data redundancy such that data is preserved even if one or more storage devices fail, this form of storage may be considered to provide the digital equivalent of a dual recording capability. This is because the data is clearly stored more than once in the system such that data recovery is still possible even if some data is lost as a result of an equipment failure.

Power protection may also be required (e.g. Uninterruptible Power Supplies for the system) to ensure that the computer system does not corrupt data in the event of a sudden power failure.

3.4.3 Recordings to Removable media (e.g. video tapes and DVDs)

Where the recording system employs removable media, two recordings of the image stream must be made on separate media (e.g. tape or DVD disk) at the same time. One of the resulting media will be preserved as the Master and stored securely until no longer needed, whilst the other will be deemed to be the Working copy and used to process the contravention and for later processes. The recordings may be analogue or digital

3.4.4 Electromagnetic Compatibility

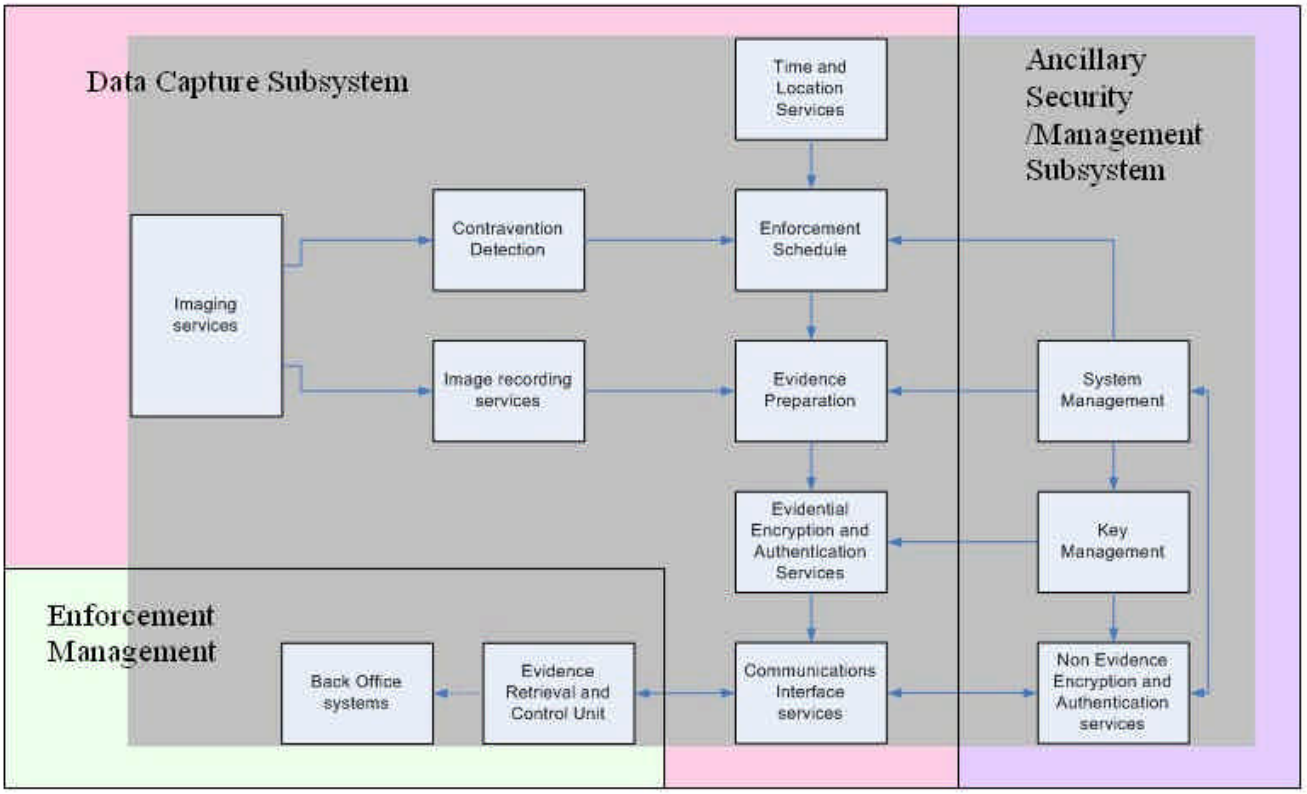
The provisions of paragraph 3.1.2.5 shall apply to recording systems also.

Chapter 4 Requirements for Unattended Systems

4.1 Introduction

It is a guiding principle of unattended systems that they only record suspected contraventions when there are good grounds to believe that a contravention is taking place. In meeting this principle, systems will be required to include positive mechanisms to prevent recording at times outside enforceable hours. In the case of mobile systems, they should include a mechanism to allow the location of the enforcement camera to be determined with sufficient accuracy to restrict enforcement to locations at which a contravention may be committed.

Figure 2. Illustrative Enforcement System Functional Block Diagram



4.2 Functional Requirements

These requirements are presented as a series of statements of fitness for purpose. In a number of cases, it has been necessary to define the requirements using definitive limits. It should be noted that where definitive limits are given, then these are the minimum acceptable criteria.

These requirements are presented based upon the illustrative design shown in Figure 2. Each of the main sections of this part reflect the top level functional groupings shown with the

shaded areas of the diagram. Within each major section, the functional elements that make up functional grouping will be described in detail

4.2.1 Data Capture

This section covers requirements for the components of an unattended enforcement system that are to do with the acquisition of evidence of a contravention and the functions necessary to compile the evidence into coherent evidence packages (hereinafter called Evidence Packs).

4.2.1.1 Imaging Services

Fundamental to the verification of the detection of a contravention is a persuasive sequence of images. This section discusses the requirements for the images that need to be captured in order to achieve this objective. This section describes the fundamental requirements for the image quality, the refresh rate and the camera operational performance

4.2.1.2 Image requirements

Imaging services shall generate images that allow an enforcement operator to simultaneously determine the target vehicle registration mark (VRM) and to examine the context under which the contravention took place. In this context, the term simultaneously shall be taken as meaning that the context and close-up images have demonstrably been taken at a point that is demonstrably between the start and end points of the context recording. All images shall, as a minimum, be marked with location, time, date and a unique frame identifier and shall be fit for purpose.

4.2.1.2.1 Context View

The provisions for attended systems in paragraph 3.1.1.1 apply to unattended systems also.

4.2.1.2.2 Close-up View

The provisions for attended systems in paragraph 3.1.1.2 apply to unattended systems also except that the close-up view is permitted to be monochrome and may, if required, be taken with an infra red (IR) sensitive camera and illuminated with an IR source.

4.2.1.2.3 Frame rate

The context image shall be refreshed a minimum of five frames per second. It is permissible for a single close-up view to be captured provided that this image is demonstrably contemporaneous with the context image sequence.

4.2.1.2.4 Low Light Performance

The provisions for attended systems in paragraph 3.1.2.3 shall apply to unattended systems also.

4.2.2 Time and Location Services

Time and Location services provide the enforcement system with the time, date and, where appropriate, location information that is used both to determine (when used in conjunction the enforcement schedule) whether a contravention has taken place and to record the same

information for evidential purposes. For both these reasons, it is imperative that both time and location information are accurate. Clock synchronisation events shall be recorded in the system operation logs and if unsuccessful for more than the required synchronisation period, enforcement shall be suspended and an appropriate system log entry made.

4.2.2.1 Time and date

The unattended enforcement system shall maintain a reference clock as described in paragraph 3.2.

4.2.2.2 Location

For mobile systems, the enforcement equipment shall be capable of determining the location and direction of travel of the camera with sufficient precision that an enforcement officer viewing the resulting evidence can unambiguously identify the place that the contravention took place. This requirement shall be met for all conditions of the built environment (including, but not limited to, urban canyons, bridges and tunnels). The location system shall update sufficiently regularly that this requirement is met for all permitted enforcement vehicle speeds. Failure of the location system to generate an appropriate location reference shall cause enforcement to be suspended and shall be recorded in the system log.

For static and portable systems, the site commissioning procedure shall be used to enter the known location of the enforcement equipment

4.2.3 Contravention Capture

Contravention Capture provides the mechanisms for detecting that a contravention is possibly taking place, for determining that the detected potential contravention is taking place at an enforceable time (and in the case of mobile systems at an enforceable location) and recording the evidential information necessary to allow appropriate enforcement actions to be taken.

4.2.3.1 Contravention detection

Unattended enforcement systems shall have an automatic method for detecting possible contraventions in progress. This mechanism shall not require any form of operator intervention when in use. In operation, the contravention detection system should seek to minimise the number of false positive contravention detections .

4.2.3.2 Enforcement Schedule

Unattended enforcement systems shall incorporate a mechanism that prevents enforcement evidence from being gathered at times that there is no valid enforceable regulation. In the case of mobile systems, the enforcement schedule functionality has to ensure that both the location and the time are enforceable before permitting the gathering of evidential data. It shall be noted that it is permitted for mobile systems to allow a positive guard-band around an enforcement zone to allow for possible navigation system or camera orientation errors.

4.2.3.3 Evidence Recording

This component is responsible for ensuring that when a contravention is detected, an appropriate amount of pre-trigger and post trigger image sequence is recorded to allow an enforcement operator to determine whether a contravention took place and that no mitigating

circumstances were present. This image sequence shall be recorded with sufficient image refresh rate that it is clear that a specific action took place.

This component of the enforcement system is permitted to compress image sequences using both spatial and temporal compression techniques. Where lossy compression techniques are used, the compression settings shall be such that when viewed by an enforcement operator the resulting images are suitable for enforcement.

These principles are illustrated in Figure 1.

4.2.4 Evidence Packaging and Transmission

In order to be useful an unattended enforcement system has to be able to get the captured evidence back to a back office facility where the evidence is viewed and an enforcement officer makes a decision about whether a penalty charge notice is justified. To do this, the evidence has to be packaged and transmitted securely to the back office.

Transmission may take place over a secure private network in which case encryption is not required and the data merely needs protecting by means of appropriate evidence package authentication. Where data is to be transmitted over a network that is accessible to any third party, then both encryption and evidence package authentication shall be used. In addition, where a third party accessible network is used, a secure interface shall be used at both ends of the link. The secure interface shall reject any communications coming from any source other than an Evidence Retrieval and Control Unit (ERCU) using a predefined schedule or protocol.

4.2.4.1 Evidence packaging

Prior to transmission, the collected evidence for each contravention shall be packaged into a single coherent whole that can be verified as a complete package. This evidence pack shall contain, as a minimum, an image sequence showing the context of the contravention taking place, a close up view (where appropriate, this may be a pointer to a segment of one of the context images) and metadata relating to the circumstances of the contravention.

4.2.4.1.1 Authentication

Once complete, the evidence pack shall be authenticated using a suitable authentication algorithm. Annex 6 provides further details of suitable authentication techniques.

4.2.4.1.2 Cryptographic services

Cryptographic services (Encryption and decryption) are required where any part of the data channel between the unattended outstation and the back office is carried over a publicly accessible network (including any form of wireless communication). Data shall be encrypted using a suitable data encryption technique. Annex 6 provides further details of suitable encryption techniques.

Where data encryption is required, all data exchanged between the back office and the unattended outstation shall be appropriately encrypted. Data relating directly to the evidence collected (evidential data) and all other (non-evidential) data shall be encrypted with different keys

4.2.4.2 Management Functions

It shall not be possible to take any kind of control over the unattended outstation other than by the delivery of a correctly authenticated system control packets (including but not limited to: enforcement schedules, status polls and key management).

Whenever an enforcement outstation is installed on a network that is accessible to a third party, the unattended outstation shall provide a secure interface through which only authorised traffic may pass. This interface shall be demonstrably resistant to a real time attack.

4.2.5 System Management

The unattended outstation shall provide a number of management functions. These shall be responsible for the recovery and implementation (at the appropriate time) of the enforcement schedule, the recovery and implementation of the initial keys (or key encryption keys) and the management of system operation, including the secure shutdown of the system in the event of any unauthorised access.

The system management functions shall also monitor the operation of the system and suspend enforcement should any of the following conditions apply. In the event that enforcement is suspended, the system shall transmit a clear-text alarm message indicating that it has suspended enforcement. In addition, a cipher-text (encrypted) detailed status message describing the fault detected shall be transmitted to the back-office.

- Local environmental parameters exceed certified limits
- Clock sync fail
- Location missing / error >30m
- Encryption keys out of date
- Enforcement Schedule out of date.

4.2.5.1 System management and Audit trail

System management functions are also responsible for the preparation of a range of evidential support information such as audit trail information and such other data, such as the system log, that may be useful to the enforcement operator in judging whether an enforceable contravention has taken place. Any such management data shall be packaged as defined by the manufacturer and regularly transmitted to the back office as an integrity protected and authenticated package. System management information shall be protected with a second set of encryption / authentication keys. These 'non-evidence' keys shall be of similar security level to those used to protect evidential data.

With the exception of urgent system alarms, which may be in clear-text (unencrypted), all system management information shall be protected as described above.

4.2.5.2 User Access

System management functions are responsible for the management of user access to the unattended enforcement system. Any attempt to access the unattended enforcement system shall be logged in the system audit trail and access to the system shall only be permitted where the user validates their access using a Password, Personal Identification Number or a service token. Where an unauthorised attempt to access the unattended enforcement

system is detected, the system shall inhibit any enforcement recording that may be in progress and securely delete all encryption keys or unsecured evidence packs

4.2.6 Enforcement management

The enforcement management component of the unattended enforcement system, also known as the back office is that part of the system housed in a secure environment (a trusted environment). The back office is made up of a number of interlocking functions. These are: the secure interface, the evidence retrieval and control unit, the internal secure interface and enforcement management system.

4.2.6.1 Secure interface

Where the external interface to the back office shall provide a secure interface that mirrors the functionality of the secure interface housed in the outstation. This secure interface shall only permit the receipt of correctly authenticated data packets (including but not limited to evidence packs, evidential support packages, outstation status messages and outstation alarms).

4.2.6.2 Evidence retrieval and control unit

The Evidence Retrieval and Control Unit (ERCU) manages all communications with the unattended enforcement systems. It is responsible to acting as a gateway for Evidential and non evidential information being received from the unattended enforcement systems and for enforcement control information being sent from the back office to the outstations.

Where the ERCU is receiving evidential data from unattended enforcement systems, the ERCU shall ensure that the data received is within 24 hours of the possible contravention taking place before writing the evidence pack to the internal secure interface. Where the internal secure interface is an air gap, the ERCU shall write the evidence pack to Write Once Read Many (WORM) media within 24 hours of the possible contravention being detected.

4.2.6.3 Internal secure interface

The internal secure interface (represented by a dashed line on Figure 1) isolates the publicly accessible or external components from the secure environment that manages the enforcement operation. Where an applicant wishes to retain compatibility with the criminal process as documented by the HOSDB, this shall be an air-gapped interface with no direct data connection. In this case data shall be written to WORM media within 24 hours of capture to ensure that the evidence cannot be compromised.

Where compatibility with the criminal process is not required, an appropriate arrangement of firewalls and transfer servers may be used.

Where the enforcement management system does not provide secure and reliable storage for evidence data, then the internal secure interface shall generate WORM media as described above.

4.2.6.4 Enforcement management system

The operation of the enforcement management system (EMS) is not part of the certification requirements for the system and this description is only given here to aid reader understanding. The enforcement management system provides the system operators the

facilities to view retrieved evidence packs, to issue penalty charge notices if appropriate, to prepare enforcement schedules and to monitor the health of any outstations connected to it. It is an assumed requirement on the EMS that it provides reliable and secure storage for evidence data. If this is not the case, the internal secure interface shall generate all evidence on WORM media.

4.2.7 Non Functional

This section is concerned with those environmental factors that could cause the evidence generated by an enforcement system to be tainted by some question of incorrect operation. It is not intended that this section in any way replaces the normal environmental requirements that would be included as part of the procurement statement of requirements. Indeed, these requirements will normally be insufficient for procurement purposes

4.2.7.1 Thermal

Unattended enforcement systems shall be capable of being stored, unpowered, for long periods under adverse conditions.

In operation, the unattended enforcement system shall function correctly in all respects from -10°C to +40°C. At all temperatures above 20°C, the unattended enforcement system shall operate correctly in the presence of 80% relative humidity. It should be noted that these are the minimum requirements and manufacturers are free to seek certification of unattended enforcement equipment to wider temperature ranges if required.

Unattended enforcement equipment shall be fitted with a sensor to prevent the equipment operating outside the temperature range certified.

4.2.7.2 Electromagnetic Compatibility

Unattended enforcement systems are required to be immune to interference from a wide variety of electromagnetic threats. Therefore in addition to testing to ensure that systems meet the requirements of European Directives 2004/104/EC (electromagnetic immunity for automotive applications) or 2004/108/EC (Generic immunity), unattended enforcement systems shall be tested for immunity to enhanced levels of interference. Electromagnetic immunity shall be in accordance with section 7.4 and 7.5 of HOSDB publication 41/06.

4.3 Recommended Design Limits and Tests

This section will describe the design limits that are necessary to meet the fitness for purpose requirements in section 4.2 above. It also describes recommended tests that should be carried out on any system submitted for certification. It is made up of a number of parts. In each part, suggested test methods are provided together with illustrative test limits. It is the responsibility of the designer seeking certification to provide a fully worked up test procedure for the approval of the Secretary of State for Transport. It should be noted that whilst this section is guidance; any deviations from the limits given in this section will require a full and detailed justification before certification will be granted.

4.3.1 Data Capture

This section covers testing of those functions that are to do with the capture of a potential contravention and preparation of the evidence pack.

4.3.2 Context sequence capture

4.3.2.1 Image quality

The context sequence as whole, and individual images on a sample basis should be checked and confirmed to be of adequate resolution, focus, clarity and substantially free from compression artefacts. The minimum resolution for the context images should be 720 Pixels wide by 276 Pixels high.

4.3.2.2 Frame rate

The context image stream should comprise a minimum of 5 frames per second and no two images should be more than 200ms apart. This should be confirmed by counting the number of frames in each second of the context image sequence.

4.3.2.3 Embedded data

In addition to the image of the context of the potential contravention, each image within the context sequence should contain embedded data consisting of the enforcement location, the equipment identifier and a unique frame code. It should be noted that if compliance with the HOSDB requirements is sought, this information should be (in the order given): the date in days, month, and year, the time in hours, minutes, and seconds, the day of the week, location and frame count from the beginning of the recording.

4.3.2.4 Close-up view capture

The unattended enforcement outstation should generate an image that it is possible to unambiguously read the contravening vehicle's VRM. The close up view should have the following minimum characteristics:

- The image presented as the close-up view should have a minimum resolution of 720 Pixels wide by 276 pixels high. (Note: this reduced image height applies for a de-interlaced PAL video signal).
- The vehicle registration mark should be represented by an area that can wholly enclose a parallelogram 140 pixels wide by 30 Pixels high for a vehicle displaying a 'one line' style plate in accordance with The Road Vehicles (Display of Registration Marks) Regulations 2001

4.3.3 Time and Location

4.3.3.1 Time

System time accuracy should be tested by recording a number of simulated traffic contraventions with a clock accurately synchronised to a reference time source present in the field of view of the context camera. A number of simulated contravention captures should be carried out. For all tests, the time recorded on the evidence pack should be within 10 seconds of the time displayed on the reference clock. The test should be repeated 14 days later and again the time difference should be less than 10 seconds.

It should be noted that there are a number of possible sources for reference time and that they may differ in the absolute time recorded by an offset that is from time-to-time altered. The principal reference source that should be used for traffic enforcement is the time broadcast by the National Physical Laboratory via the MSF transmitter

4.3.3.2 Location

For mobile systems, the system should be driven around a fixed complex route over a number of accurately surveyed datum points. The route should include a variety of built-up environments. Simulated contraventions should be recorded at each of the datum points and the location recorded by the enforcement system under test should be compared with the known values for the datum point. The total error (made up from the vector sum of the error due to movement since the last navigation fix and the intrinsic inaccuracy of the navigation system) should be less than 30m

4.3.4 Metadata

The data supplied as part of the evidence pack should be checked and should contain, as a minimum, the following items:

- Time and Date that the suspected contravention was detected
- The evidence pack unique identifier
- The unique identifier for the equipment that captured the suspected contravention
- The location at which the contravention was detected (for mobile unattended enforcement systems only)

It is recommended that the data contained within the evidence pack be kept to the minimum. Where additional information is proposed by the system manufacturer, a description of that information should be provided to the Secretary of State for Transport with suitable performance limits and a justification for their inclusion.

In addition, it should be noted that the encryption and authentication information appended to the evidence pack prior to transmission is not treated as meta-data.

4.3.5 System Management

4.3.5.1 Key Management

The operation of the key management suite should be demonstrated for all anticipated key operations. This includes, but is not limited to, the following items:

- Receive, validate and implement new keys for both evidential and non-evidential data
- Manage key validity periods and inhibit the generation of evidence if any keys have expired
- Secure deletion of key data in the event of any unauthorised access to the system

Any operation that modifies, or has the potential to modify, a key should be logged in the system audit log and this should be confirmed.

4.3.5.2 Environmental Monitoring

Unattended enforcement systems performance in the event of environmental conditions exceeding the certified range should be demonstrated. In the minimum case this should be the prevention of enforcement in the event that the system temperature exceeds the certified range. This should be demonstrated for both extremes of temperature. Where the system inhibits enforcement, this should be logged in the system audit log.

4.3.5.3 System Audit Logging

The system audit log should be transmitted back to the back office regularly and should contain a record of any significant event at the outstation. Testing should confirm that all events identified in this document and any additional elements as identified by the system designer are in fact recorded in the system audit log file. Testing should also confirm that system audit logs are integrity protected and authenticated

4.4 Non Functional Requirements

4.4.1 Thermal

4.4.1.1 Storage

The unattended outstation should be held, without power, for at least three hours at -25°C and then +70°C, with low humidity. The units should then be allowed to return to room temperature and tested to ensure correct operation.

4.4.1.2 Operational

The equipment should function within specification over a temperature range of at least -10°C to + 50°C, with 80% humidity above 20°C. The temperature should be varied in 5°C steps, and the equipment left for 30 minutes or longer to obtain thermal equilibrium; the equipment should function correctly at each temperature step.

4.4.2 Electro-magnetic Interference

4.4.2.1 General

The test arrangements are applicable to both radiated and conducted tests. The object of the test is to confirm that the traffic enforcement camera is capable of operating in the presence of electromagnetic fields without recording any erroneous or inaccurate information.

The layout of the traffic enforcement camera should be representative of the normal operating conditions, in so far as this will permit a repeatable measurement. The measurement should be carried out in screened test facilities described in EN 61000-4-3 with the equipment set up as intended for use. The field uniformity criteria of EN 61000-4-3 apply for the radiated immunity tests.

If an extension cable for remote operation is supplied with the equipment it should be connected and positioned within the test field.

4.4.2.2 Modulation

All test signals should be 90% amplitude modulated with an appropriate signal depending on the device. During these tests offences should be simulated by simulating all inputs necessary to trigger the device and monitor the correct operation of the equipment under test by examining the information on the recordings made.

4.4.2.3 Vehicle-mounted mobile traffic enforcement equipment

Vehicle mounted cameras should be wired as intended in a test harness appropriate to the type of vehicle the equipment is likely to be used in. One of two standard test harnesses should be used. One test harness representing the mounting of the device in a bus type vehicle (i.e. with long wiring looms) and the other representing the mounting of the device in a car type vehicle. The radiating antenna should be positioned in turn, in front of, and to the off side of the test harness; both planes of polarisation should be measured.

4.4.2.4 Conducted immunity test

The test is conducted in basic accordance with EN61000-4-6 with the following test method deviations:

- The clamp injection procedure is to be used with the signal being applied to the total cable bundle i.e. common mode injection. The signal is injected at each electronic unit of the device under test, connector by connector. The current probe monitoring the injected current is placed 0.05m from the devices connector on the bundle under test. The injection clamp is placed 0.05m from this.
- The modulation and limits are as defined below.

4.4.2.5 Test limits and frequencies

The test limits for all electro magnetic susceptibility tests should be:

- Field Strength 10V/m from 80 MHz to 2000 MHz and
- In the presence of common mode currents from 27 MHz to 100 MHz to level 2 of EN61000-4-6 and

The test limits defined above are in terms of the cw value of the signal; the modulation being applied on top giving peak readings 90% higher than the cw limit. The RF signal should be applied at each test frequency at the test limit for a time long enough to fully operate the device under test. The frequencies should be stepped incrementally across the test range with a step size not exceeding 1% of the previous frequency. If any effect is observed, the applied signal should be reduced by 12dB and increased in steps of 3dB until the required test level is reached. The level at which the threshold of any effect should be observed, logged and recorded in the test report.

4.4.2.6 Electrostatic discharge

The traffic enforcement camera should be tested in accordance with EN 61000-4-2:1995. At least ten single discharges should be applied to the exposed surface of each separate part of the equipment.

For permanent installations, tests may be performed in the final installed position. A maximum test voltage of 4 kV should be employed i.e. at level 2.

Chapter 5 Annexes

5.1 Annex 1. Abbreviations and Terminology

5.1.1 ABBREVIATIONS

BLE – Bus Lane Enforcement

CCD - Charge-Coupled Device (see definition below)

CCTV – Closed Circuit Television - is the use of video cameras to transmit video images to a specific, limited set of monitors.

CLEF - Commercial Evaluation Facility [see definition below]

CMOS - Complimentary Metal Oxide Semiconductor [see definition below]

CUV – Close-up View (see definition below)

CV – Context View (see definition below)

DVD - Digital Video Disk (various formats are available)

DVR – Digital Video Recorder (generally uses hard disk or DVD)

EAL - Evaluation Assurance Level [see definition below]

EBU - European Broadcasting Union – sets standards for video and broadcasting

EMC - Electromagnetic Compatibility

EMS - Enforcement Management System

ERCU - Evidence Retrieval & Control Unit

FTP - File Transfer Protocol (a protocol that allows users to copy files between their local system and any system that can be reached on the network)

HOSDB - Home Office Scientific Development Branch

IACS - International Association of Classification Societies

ISO - International Organisation for Standardisation

MSF - The radio signal which broadcasts the national time standard for the UK. (The letters do not stand for anything. MSF is simply a call sign which uniquely identifies the broadcast).

PAL - Phase Alternating Line - an analogue colour video encoding system used in broadcast television systems in large parts of the world, including UK and Europe

PCN – Penalty Charge Notice (issued for Traffic contraventions under a Civil Enforcement regime)

PTZ – Pan, Tilt and Zoom – standard camera controls for CCTV mechanically operated cameras

RAID - Redundant Array of Independent Disks. A method of storing data more reliably on (computer) file servers (see definition below)

TCF - Technical Construction File (see definition below)

TEVS – Traffic Enforcement Video Store – area of file storage (typically on a computer file server) where video of contraventions is securely stored.

TRO – Traffic Regulation Order (in London, this is referred to as a Traffic Management Order – or **TMO**)

VCR – Video Cassette Recorder (generally uses VHS tapes)

VRM – Vehicle Registration Mark – as displayed on the front and rear 'number plates' of most road vehicles (but only on the rear of motorcycles) in accordance with applicable legislation.

WORM – (Write Once, Ready Many) - A recording medium that once written to, cannot be amended - e.g. a (non-rewritable) CD or DVD

5.1.2 TERMINOLOGY

Note – some of these terms may have a more generic meaning – but are explained here in relation to Video, Camera and Recording Systems for civil traffic enforcement.

Approved Device - The combination of camera(s) and recording system which meets the specified requirements for civil traffic enforcement in applicable legislation and guidance. This will normally be demonstrated by certification by the Secretary of State.

Attended CCTV system - A system that relies on an operator to observe and log potential contraventions as they happen.

Authentication (of a video signal or file) - Authentication establishes the authenticity or credibility of a video signal or file. Typically this may be through use of Hash functions or (digital) Watermarks.

CCTV (Video) Matrix - The core of most traditional *analogue* CCTV systems is the video (hardware) matrix. This is typically an electronics rack that is situated close to the control room. The matrix is a switch that routes video inputs from cameras to video outputs that are fed to monitors and DVRs / VCRs or other equipment for recording as required, normally using desk-mounted keyboard controls.

A ***virtual matrix*** runs on a data network that carries information encoded as TCP/IP (Transfer Control Protocol / Internet Protocol). Whereas an analogue hardware matrix switches video and PTZ (pan/tilt/zoom) controls, a virtual matrix can also handle the

processing of alarm and access control data. It can also accommodate the communications required for VOIP (Voice over IP) and bi-directional, full-duplex audio.

Charge-Coupled Device (CCD) - This is an image sensor technology, consisting of an integrated circuit containing an array of linked, or coupled, light-sensitive capacitors. CCDs are used to obtain images in most CCTV cameras.

Close-Up View (CUV) - The camera should be capable of zooming in to obtain a clear close-up view (CUV) of the VRM. In general the close-up view should be able to show a (horizontal style) Vehicle Registration Mark (VRM) as between around 15% to 30% of the video frame width to enable the VRM to be clearly recognised. However, depending on other factors (see section 8 below) this range may be extended to between around 10% and 35% of the frame width.

Context View (CV) - The camera should be capable of zooming out to show a clear context view (CV) of the vehicle within the enforcement zone. Typically, a (horizontal style) VRM should be displayed as between around 3% and 10% of the video frame width – although it is not necessary for the VRM to be clearly readable in this view. This view should allow an observer to clearly identify that the vehicle is the same as that shown in the CUV image.

Commercial Evaluation Facility (CLEF) - A CLEF is an commercial evaluation facility that is certified under the ITSEC scheme to undertake testing of system security

Complementary Metal Oxide Semiconductor - This is an image sensor technology, consisting of an array of CMOS transistors. Recent developments in CMOS technology have produced image sensors that rival the quality of the more mature CCD technology.

Encryption Key - An encryption key is a data string that is used by an encryption process to convert the clear-text data into the cipher-text string for transmission. Dependent upon the encryption method chosen, these keys may be single shared values or a matched pair of public / private keys. In all cases, the private key or the shared key must be kept secret.

Enforcement Schedule - The enforcement schedule contains data that is used, normally by an unattended enforcement system, to determine whether enforcement action is justified at a particular location at a given time and if action is justified, then what types of contravention are permitted at that time / location

Enforcement Zone the Enforcement zone is a component of an enforcement schedule. It relates to a particular geographical area and dictates what contraventions can be enforced and during what hours.

Evidence Pack - An evidence pack is a package of evidential data that is used to 'prove' a contravention has taken place. It will normally contain a close-up view a context image sequence and a small amount of meta-data (such as time, date, location, contravention number, and unit number). It will often be encrypted and authenticated. It is advisable that the evidence pack contains the *minimum* information necessary to demonstrate a contravention has taken place.

Evidence Retrieval and Control Unit - This device acts as a secure extension to the remote contravention detection equipment. It allows the collection of contravention information at a convenient 'office' location. One of its main functions is to preserve the evidential integrity of

the contravention records by processing encrypted data through a pair of secure interfaces to a public communications network. The ERCU operates on the benefit of doubt principle.

In systems that are being designed to be compatible with the criminal process or are to be type Approved by the Home Office, the ERCU writes data to a WORM media within 24 hours to protect data from tampering.

Evidential Data - Evidential data is only that data that is required to demonstrate to an enforcement officer or an adjudicator that a contravention has taken place. It is considered good practice for the evidential data to contain the minimum necessary information

Frame rate - The frame rate of an evidence package is the number of complete images rendered by the enforcement system in any second. It should be noted that some image encoding algorithms do not encode complete frames. For these encoders, the frame rate requirements will be met if the encoded video provides a clear impression of scene movement.

Hash function - An algorithm that calculates a value from the contents of a data file which can then be used to detect alterations to the file. Similar to a checksum but with greater security, hash functions play an important role in secure cryptographic systems, where authentication is as important as hiding the data from third parties.

Integrity the provision of facilities (on computer storage systems) to ensure that if data is amended, the changes are detectable. Typical examples include hash functions and watermarking of the data – so that if the data is amended, the hash function shows an error – or the watermark becomes visible.

Legacy System - A system that employs pre-existing equipment (either wholly or in part) and certification is required (either wholly or in part) in order to comply with applicable legislation.

Master Copy - The original video clip of the contravention, which is held securely (usually in the Traffic Enforcement Video Store) pending determination of any PCN procedure.

Matrix - see CCTV Matrix

Negative Guard Band - A negative guard band is one where although the reported position of the enforcement device is within the defined enforcement zone, enforcement does not take place because it is within the allowed error margin.

Non Evidential Data: Non Evidential Data is all data other than evidential collected or generated by an enforcement system component. In practice this may include information that demonstrates that the system is operating normally, logged data relating to the normal operation of the system (such as the generation, transmission of data packets, the updating of keys etc) and information that may assist an enforcement operator in processing a contravention record (for example the suspect vehicle's VRM could be returned as non evidential data)

Positive Guard Band - A positive guard-band is one where although the reported position is outside the enforceable area, it is within the allowed error margin so enforcement is permitted.

RAID Server – a file server using RAID technology. The acronym RAID (redundant array of independent disks) refers to a data storage scheme using multiple hard drives to share or

replicate data among the drives. Depending on the configuration of the RAID (typically referred to as the RAID level), the benefit of RAID is to increase data integrity, fault-tolerance, throughput or capacity, compared with single drives. Note: RAID 0 does not provide any form of data redundancy and should not be used in enforcement applications

Reliability – the ability of (computer & similar) systems to continue to operate and retain valuable data even if some parts of the system fail. RAID servers are a good example of this in practice.

Security - the protection of data and system information (on computer storage systems) so that only people who are authorised to access, use, copy or delete the data have access to it for these purposes. Typically, this may involve a hierarchy of password protection so that individuals are only able to carry out the activities that they are authorised to do. Where data is released from a secure environment, this is likely to require other forms of protection – such as data encryption – to ensure that unauthorised persons cannot see or amend the data.

Server (File server) - A form of disk storage that hosts files within a network.

Technical Construction File - The information that describes in full the enforcement system's design and operation. The file forms the basis of applications for certification of an "approved device" to the Secretary of State and records changes made to the equipment during its life.

Unattended CCTV system - A system that records potential contraventions automatically for subsequent review.

Version - Software unique identifying number. An instance or a configuration of a piece of software. Once a version is completed, it cannot be changed without creating a new version. Once the development team considers a software version as being sufficiently mature, the software version can be turned into a software *release.*

Variant - A software version that is an *alternative* to another version. A variant or variation is the same version of a piece of software that meets a conflicting requirement. For instance, the same version of software doing the same job in the same way but designed to control different hardware.

Watermark (digital) A Watermark is a (generally invisible) identification and authentication mark that is embedded into a (video) signal or file that can be detected if required. It can be used to confirm the integrity and/or source (or authorship) of the video file.

Working Copy - a video clip of a contravention either produced directly from the Master Copy or made contemporaneously with it for the purpose of evidence review and related procedures.

5.2 Annex 2. Organisations contributing to the production of this document.

British Security Industry Association

Department for Transport

EMC Test Labs Association

Institution of Engineering and Technology

ITS-UK

Manchester City Council

Newham Borough Council

Nottingham City Council

Pips technology

Qinetiq

Redflex Traffic Systems Pty Ltd

Sheffield City Council

Siemens Traffic Controls

Transport for London and technical advisers Atkins

Transport Research Laboratory

TUV Product Service Ltd

Vehicle Certification Agency

Westminster City Council

5.3 Annex 3. Moving traffic contraventions within the scope of this document

Those indicated by the following traffic signs and their permitted variants. (The number in brackets is the sign drawing that corresponds with the description in the Traffic Signs Regulations and General Directions 2002).

Vehicular traffic must proceed in the direction indicated by the arrow (606)

Vehicular traffic must turn ahead in the direction indicated by the arrow (609)

Vehicular traffic must comply with the requirements in regulation 15 [of Traffic Signs Regulations and General Directions - keep to the left or right of the sign] (610)

No right turn for vehicular traffic (612)

No left turn for vehicular traffic (613)

No U-turns for vehicular traffic (614)

Priority must be given to vehicles from the opposite direction (615, 615.1)

No entry for vehicular traffic (when the restriction or prohibition is one that may be indicated by another traffic sign subject to civil enforcement) (616)

All vehicles prohibited except non-mechanically propelled vehicles being pushed by pedestrians (617)

Entry to pedestrian zone restricted (618.2)

Entry to and waiting in pedestrian zone restricted (618.3)

Entry to and waiting in pedestrian zone restricted (variable message sign) (618.3A)

Motor vehicles prohibited (619)

Motor vehicles except solo motor cycles prohibited (619.1)

Solo motor cycles prohibited (619.2)

Goods vehicles exceeding the maximum gross weight indicated on the goods vehicle symbol prohibited (622.1A)

One way traffic (652)

Buses prohibited (952)

Route for use by buses and pedal cycles only (953)

Route for use by tramcars only (953.1)

Route for use by pedal cycles only (955)

Route for use by pedal cycles and pedestrians only (956)

Route comprising two ways, for use by pedal cycles only and by pedestrians only (957)

With-flow cycle lane (959.1)

Contra-flow cycle lane (960.1)

Box junction markings (1043, 1044)

5.4 Annex 4. Attended Systems Check List

Sample Test Procedures

No	Action	Comments
A	**Observational Tests of CCTV Cameras**	
1	Start video recording of 'test' (or ensure that recording is running)	On some (mainly server based digital) systems, recording may be continuous
2	Pan & Tilt camera to align with 1st approach	
3	Zoom camera out to Context View (CV) of approach - at the ***minimum*** viable range	
4	Measure time to 'zoom in' from the CV to a Close-Up View (CUV) of a VRM on this approach - at the ***maximum*** viable range	Zoom times may be measured to the nearest second - using a manual or electronic stopwatch facility
5	Ensure that the VRM is clearly readable on screen	
6	If appropriate - recording of this test may be stopped	
7	Repeat tests (1-6) for other enforced approaches visible from this camera	
8	Repeat tests (1-7) for all enforcement cameras, for all enforced approaches visible from each camera	
B	**Playback & Review tests (for recording and image grab facilities)**	
1	Playback the video recordings taken during tests (section A) on the Review facility	Recording may be on tape, disk (typically CD or DVD), server or other digital recording equipment
2	Grab images of CV and CUV on each enforceable approach on each camera	
3	Ensure that CV and CUV images are relatively sharp and clear, and that the VRM of a vehicle is clearly readable in the CUV	

4 Repeat 2 & 3 for all enforceable cameras and approaches

NOTES

1 *Video recordings and grabbed images for all enforceable cameras and approaches should be retained (on disk) for the Technical Construction File for the system - for approval purposes.*

2 *The above procedures may be more appropriate for vehicles observed from the rear, moving away from the camera. For forward facing cameras, where vehicles approach the camera, the CUV may need to be observed at the maximum viable range, and the CV at the minimum viable range. In these circumstances, which will be site specific - a lower zoom range may be required.*

3 *Whilst it is **not** a requirement to repeat the above procedures in varying light and weather conditions, the documentation for these tests should indicate the lighting and weather conditions under which the tests were conducted.*

4 *Where a number of very similar or identical specification New or Legacy CCTV cameras require approval as a part of a System Certification, by agreement with the Secretary of State, tests from a sample of these cameras is likely to be acceptable.*

5.5 Annex 5. Suggested Technical File Contents

These are the suggested contents of the Technical Construction File required for civil traffic enforcement applications.

1. Name and address of applicant organisation, name of principal contact, (plus email & phone number).

2. Name, title and qualifications and/or experience of the competent person who commissions the system and signs test declarations. (Also name and address of any external test house and engineer if necessary).

3. A list of all the documents enclosed in the technical file.

4. A list of all the equipment with serial numbers and software that comprise the system.

5. A description of the system architecture in full, as well as details of any significant design elements. This should be with reference to issues discussed in the guidance. We suggest it should include:

    - Software versions (and issue dates).
    - The number of workstations.
    - Camera handling capacity and planned number of cameras deployed.
    - Specifications for the system and ancillary equipment to demonstrate compliance with any performance minima specified in the guidance.

6. Test reports and declarations demonstrating the required performance as applicable. Which tests were performed and why the tests were selected or omitted.

7. Where the application relates to bus lane enforcement under the Transport Act 2000, documentary evidence of prior home office approval or evidence of use for civil bus lane enforcement in London prior to November 2005 as applicable.

8. A maintenance plan.

5.6 Annex 6: Data Security

5.6.1 INTRODUCTION

5.6.1.1 This annex describes the requirements for data security for a civil certified enforcement system. This first generation data security annex is based upon the requirements published by the Home Office for equipment intended to be Type Approved under the criminal process.

5.6.1.2 Subject to the generation of an appropriate Protection Profile, it is intended that the requirements for data security will move to implement the common Criteria at Evaluation Assessment Level 4 in accordance with ISO / IEC 14508. At that time, this annex will be withdrawn and replaced with the required protection profile.

5.6.1.3 The integrity and full acceptance of the evidence by the public and the adjudication service is of paramount importance. It is therefore essential this continues to be ensured by the use of data protection methods that will themselves be recognised as adequate by the stakeholders. The following data protection is required for devices used for automatic unattended operation.

5.6.2 GENERAL REQUIREMENTS

5.6.2.1 The purpose of the data protection is to ensure that a defence based on an allegation that the data could be tampered with by anyone accessing the network will be implausible and have no credibility at adjudication. The standard data security measures used by major financial institutions for the protection of financial data meet that requirement and are specified in published international standards. It is a requirement that data protection as used in the financial sector is applied to the evidence data produced by all devices approved for automatic unattended use.

5.6.2.2 If the following data protection measures are adhered to, then any public or private data network, including digital radio networks, may be used.

5.6.2.3 A financial sector data protection system provides three levels of protection:

i. Authentication
ii. Encryption
iii. Error protection.

5.6.2.4 Authentication is the principal element in establishing the integrity of the evidence. A Message Authentication Code (MACs) comprising 4, 8, 10, 12 or 16 8-bit bytes of data is computed and appended to the image and associated evidence data (evidence package). The MAC is a complex function of a 112 bit, a 128 bit or a 168 bit authentication key. The integrity of a received evidence package is verified when re-computing its MAC using the same key produces the same answer.

5.6.2.5 Encryption transforms the evidence package into unrecognisable random data. For the encryption, another 112 bit, l28bit or 168 bit encryption key, chosen to be different from the authentication key, shall be used.

5.6.2.6 For any data net work, standard error correction methods such as a 32bit Cyclic Redundancy Check (CRC) shall be used to ensure no accidental errors can be introduced during the transmission process.

5.6.2.7 The data protection process implemented in the device at the roadside site, which must be undertaken in the following order, shall be to***:***

i. Calculate the MAC of the whole evidence package
ii. Encrypt the evidence package
iii. Append the MAC to the encrypted evidence package
iv. Compute the CRC for each transmission segment
v. Transmit each segment

5.6.2.8 At the receiving end, the process which must be undertaken in the following order, shall be to:

i. Check each CRC and request re-transmission when necessary
ii. Decrypt the evidence package
iii. Recalculate the MAC from the decrypted evidence package
iv. Compare this MAC with the transmitted MAC
v. Accept as valid data only if they are the same.

5.6.3 DATA PROTECTION STANDARDS

5.6.3.1 The data protection shall be based on the following published standards.

5.6.3.2 Both the authentication and encryption process are based around any sub-process known as a block cipher. For the traffic enforcement system the same block cipher shall be used. Systems being submitted for certification shall use either AES 128 or use the Triple Data Encryption Algorithm specified in NIST Special Publication SP800-67 using either option 2 or option 3 (known as 2TDEA and 3TDEA respectively). Option two requires two different 56bit keys while 3TDEA requires three different 56bit keys. After the 1 January 2010, systems using 2TDEA shall move to AES 128 or 3TDEA. Beyond 1 January 2030, all systems shall use AES 128. However, other block ciphers recommended by NIST as providing comparable security strengths may be used with the agreement of Secretary of State for Transport.

5.6.3.3 The authentication process shall follow that described in the draft recommendation given in NIST Special Publication 800-38B for the RMAC Authentication Mode.

Systems shall use RMAC with AES 128 and a MAC length of 64 bits. The length of the MAC generated will be 64bits long. In the case of the 2TDEA or the 3TDEA a salt 64 bits long will be used. On 1 January 2010 systems using 2TDEA shall move to using AES 128 or 3TDEA and generate a 64 bit MAC, the 3TDEA systems using a 64bit salt. Beyond 1 January 2030 all systems will use RMAC with an AES 128 block cipher and generate an 80 bit MAC with a l6bit salt.

5.6.3.4 The encryption process for systems to be certified by the Secretary of State for Transport shall use AES 128 in Cipher Block Chaining (CBC) mode as described in NIST Special Publication SP 800-38A. On 1 January 2010, systems using 2TDEA shall move to using AES 128 or 3TDEA in CBC mode. Beyond 1 January 2030 all systems shall use AES 128 in CBC mode.

5.6.3.5 The above data protection system requires the encryption and authentication keys to be known at both ends of the communication link. The security depends on these remaining unknown by any third party. Good security requires frequent changes of the keys and different keys used at each site. All systems shall generate new encryption and authentication keys for each evidence pack generated in the road-side equipment. A key management system shall be provided as part of the back office. It shall automatically generate, store, distribute over the data network, synchronise and destroy keys securely. It shall be as transparent to users as far as possible.

5.6.3.6 The keys generated and used in the roadside sites for data encryption and authentication shall be sent over the network encrypted using KEKs (Key Encryption Keys). The KEKs shall be manually loaded and changed no less frequently than annually. Systems shall use AES with a 192 bit or longer KEK. Systems migrating using 2TDEA or 3TDEA shall use 3TDEA and so use 3 KEKs. These higher level Key Encrypting Keys (KEKs) do not need frequent changing and shall be securely distributed manually to each site. This distribution is part of the evidential chain. Other methods of key encryption recommended by NIST maybe acceptable if agreed with Secretary of State for Transport.

5.6.3.7 Physical security shall be provided at each site. Any unauthorised access shall be detected and shall cause all security keys to be securely deleted.

5.6.3.8 Each site must have a battery back up so that, on detection of a failure of the mains supply, it can close down operations in a controlled manner maintaining the integrity and security of the stored data and enable operations to be automatically resumed when power is returned.