Enforcement Operations Agreement

Schedule 2

Appendix 31
Handling Evidence

(also General Statement of Requirements)

tfl_scp_000555

Service Operations Directorate
Transport for London
4th Floor, Palestra
197 Blackfriars Road
Southwark London SE1 8NJ

Table of Contents

The London Congestion Charging Enforcement Handbook

Name of Author Edition/Version Number Date

Management Summary

- The Authority supports the view that active enforcement of traffic management orders, regulations or signs, can be crucial to their effectiveness in meeting the objectives of the Mayor's transport strategy.

- Whilst recognising that the principle requirement of any civil enforcement system must be to secure the integrity of the evidence, the Authority wishes to increase competition in the market, in the interests of best value for public money and take advantage of advances in the various technologies, available for the enforcement of Road User Charging, (known as Congestion Charging within the Greater London area) and wishes to encourage the further development of existing and alternative Congestion Charging enforcement systems and their component parts.

- The key to the use of cameras for the detection of any traffic offence is the generation of a record which proves that potentially, a contravention has taken place. It is assumed that any camera based enforcement system involves first capturing this record and then interpreting it. For example, a set of images of a vehicle is captured, and then the VRM is interpreted from these images immediately or post capture either manually or using an ANPR system. A judgement is then made as to whether a charge event has taken place.

- This document contains a description of, or reference to, the technical requirements for the maintenance of the evidential integrity of the record. It does not cover the processes by which the interpretation of the record is managed.

- This Handbook is intended to provide information and guidance to industry on the minimum standards acceptable to the Authority for the creation and security of the Evidential Record by automatic, supervised and attended civil Congestion Charging enforcement systems. It does not cover the processing of a charge, payment mechanisms, exempt vehicle lists, or other 'back-office' systems.

- These requirements may be updated, where appropriate, and further editions of this handbook may be issued, in the future. Operational imperatives may also lead to additional or more stringent requirements.

Contents Page

1 INTRODUCTION

1.1 Historically, Traffic Regulations were enforced manually by the police under the Criminal Justice System, using the powers and procedures of the Road Traffic Offenders Act 1988 (RTOA 1988) and offences had to be proved “beyond reasonable doubt”: The use of camera technology was permitted by the Road Traffic Act 1991 (RTA 1991) which also introduced the requirement for all enforcement equipment and systems to be approved by the Secretary of State for the Home Office. Such approval was only recommended by the Home Office Operational Police Policy Unit (OPPU) if the equipment/system was tested and fully complied with the requirements of the Centre for Applied Science and Technology (CAST), formally known as the Home Office Scientific Development Branch (HOSDB)..

1.2 Schedule 23 of the Greater London Authority Act 1999 (GLA Act 1999) provides that the Authority (and with the authorisation of the Authority and in pursuance of the Mayor’s transport strategy, the London Boroughs) may make a Road User Charging Scheme. With the exception of Paragraph 25, of the Act, which deals with obscuration or distortion of VRMs, damage to enforcement equipment and use of false documents with the intent to avoid payment, contravention of this scheme is a civil offence and therefore is not enforced by the police,. Alternative methods of enforcement based upon the principles and standards used in Criminal enforcement, but following the requirements of civil law, have been developed by TfL.

1.3 As a Civil rather than a Criminal offence, the burden of proof required to demonstrate that a contravention of a Congestion Charge Order has occurred, is “on the balance of probability”. Liability to pay the relevant fees is incurred if it can be shown that a vehicle, which has not been exempted from a charge by Regulation (Paragraph 11 GLA Act), was wholly within the charging zone, at a time which was within the charging period. Should proof be required it must be usable within the appeal process administered by the Parking and Traffic Appeals Service (PATAS).

1.4 In order to monitor and record contraventions of a Road User Charging Scheme, the GLA Act allows the installation of enforcement equipment on roads (Paragraph 14) and grants the Authority the ability to “type approve” the equipment (Paragraph 29).

1.5 The GLA Act (Paragraph 4) also requires that an Order be made to introduce a charging scheme and (Paragraph 8) designate the area to which it applies. Paragraph 12 permits the Authority to issue and enforce penalty charges for non compliance to the Regulations.

1.6 The Authority may issue a penalty charge notice against any vehicle which enters the designated zone, within charging hours, without paying the prescribed fee within the allotted time period. Such a notice can be issued on the basis of an Evidential Record which is created and handled by the Detection and Enforcement Infrastructure. The Evidential Record uncontrovertibly establishes that a vehicle was in a known location at a known time.

1.7 The enactment of the Mayor's transport strategy required the implementation of a Congestion Charging Scheme (CCS) in a defined area of Central London, known as the Central London Zone or CLZ. This was introduced on the 17th February 2003. The strategy also permits the introduction of additional schemes within Greater London.

1.8 The acquisition and specification of the existing and proposed Civil Traffic Enforcement Infrastructure has been based on the standards and principles of the only national standard currently available, for enforcement equipment, the requirements of which are documented in various CAST (formerly HOSDB publications.

1.9 CAST publications also require the transmission of evidential data over a public network to be protected by data security measures of a comparable standard to those used by major financial institutions for the protection of financial data. The Authority continues to concur with this requirement, in order to maintain the integrity, weight and acceptance of the evidential record.

1.10 The development of alternative or additional methods for the Civil enforcement of Traffic Regulations and Signs, based on the principles and standards applicable to Criminal enforcement, but following the requirements of Civil law has been, and will continue to be, supported by TfL.

2 TERMINOLOGY

2.1 The Authority

The Greater London Authority (GLA) or the Mayor, acting on behalf of the GLA

2.2 TfL

Transport for London, its Agents or Representatives;

2.3 Evidential Record

A record containing one or more identifying images, which include a VRM which is clearly visible to the human eye, on a target vehicle, at an identifiable known location and time. The text data includes as a minimum the time/date/location or camera ID and a unique identification number. As a reference point for the processing of a Penalty Charge, the record may also contain other information which, in itself, has no evidential value such as an image or data generated by an ANPR system.

2.4 Detection and Enforcement Infrastructure

An enforcement camera which records target vehicles within its field of view, without continuing human intervention, together with the time/date/location/camera ID and unique identification number of the record and facilitates the secure transmission or transfer of the record to an in-station for processing.

2.5 Camera

A Digital or CCTV camera is an electronic device able to capture a single, or series of, images with the ability to produce an analogue or digital output. A camera may also be a component part of, and located in the same housing as, an ANPR processor.

2.6 ANPR

An Automatic Number Plate Recognition processor.

2.7 Session

A session is a period of time during which the Detection and Enforcement Infrastructure can be shown to be in an effective operational condition, both at the beginning and end of the period, generates Evidential Records, and logs any evidentially significant events.

2.8 WORM

Write Once Read Many data storage device

2.9 VRM

Vehicle Registration Mark, Number or Number-plate which, for the purpose of the Evidential Record, must be readable by the human eye, on the identifiable vehicle to which it is attached, in at least one of the images in the Evidential Record

2.10 PATAS

The Parking and Traffic Appeals Service which administers the processing of appeals regarding traffic and parking offences, including Congestion Charging in London, and provides the adjudicators who assess appeals submissions.

2.11 CAST

The Centre for Applied Science and Technology (CAST) was formerly known as the Home Office Scientific Development Branch (HOSDB). The relevant documents, detailing the minimum standards of enforcement equipment, required to maintain the evidential integrity, are referred to as the CAST documentation.

3 REFERENCE MODEL

3.1 A reference model has been adopted to demonstrate how evidential requirements are applied. The model contains the following elements:

- Outstation – the equipment at the roadside including cameras which is used to capture images
- In-station, if present, – equipment which may be centrally located and used to collect the images and related data from the out-station
- ANPR system – used to interpret VRM and image data and may be located at an Out-station or In-station
- Communications link or transport device, if present – the means by which images and related data are transmitted from the Out-station to the In-station
- Permanent Evidence Store – the database or medium on which evidence is secured for long term use, typically located at an in-station or integrated within an outstation if no in-station is used.
- Public network – where a communications link makes use of a public communications network which may be provided by a telecommunications service provider

3.2 The requirements set out in this handbook can be identified as applying to each or all of Out-station, In-station and Communications Link or transport device. Where a requirement applies to all items, it is termed applicable to the System.

4 GUIDING PRINCIPLES

4.1 Any Civil traffic enforcement system, supervised, automatic or attended, is required to prove that “on the balance of probability” the registered keeper of a vehicle is in contravention of a Scheme Order, relevant Regulation, Sign and/or Traffic Management Order.

4.2 Whilst recognising that non compliance to a Charging Scheme Order is not a criminal offence, the Authority has instructed TfL that it will only consider for approval enforcement systems and equipment that are based on particular guiding principles, set out in CAST documentation, for the maintenance of the evidential integrity. This applies, in particular, to the capture, security, transmission, storage and retrieval of evidential images and data.

4.3 It is expected that any system will employ various techniques to ensure that the interpretation of the evidential record is accurate and the record is a true representation of the captured event. These may include but not be limited to the automatic filtering of records to remove duplications, those likely to be incorrectly interpreted and the manual filtering and checking of records prior to processing. These processes are not addressed in this handbook, as they have no direct evidential value.

5 EVIDENCE

5.1 This section describes the components of an Evidential Record of a captured event, and then how the integrity of each of these components is to be ensured whether the capture is performed at the Out-station or In-station.

5.2 Evidential Record

5.2.1 An Evidential Record must, utilising photographic images and verifiable data blocks or strings, identify the vehicle, the location and the time of the captured event. Information which has no direct evidential value but may assist with the processing of a Penalty Charge, such as an image generated by an ANPR system, may also be included.

5.2.2 The Evidential Images must be of such resolution that, the Vehicle Registration Mark of the target vehicle may be read by the human eye whilst identifying the vehicle to which it is attached (Monochrome or Colour) and the vehicle must be identifiable in the context of its surroundings (Colour), to visually demonstrate both the vehicle identity and its location.

5.2.3 The Evidential Data Block must, as a minimum, contain the following, to confirm the veracity and uniqueness of the Evidential Record:

i. location (plain English or verifiable location code);
ii. time and date of capture of images;
iii. unique record identification;

5.3 Evidential Integrity of Record

5.3.1 The first requirement of Evidential Integrity is to be able to demonstrate that, once generated, Data is securely encrypted and can be authenticated at all times. This assures the integrity of the record as a whole. Compliance is therefore required with the CAST minimum standard, as discussed in Appendix A, though as techniques in the industry develop, superior technologies or algorithms may be considered for use.

5.3.2 In addition, the following aspects of system performance are required;

- Audit trails – to be able to track any user, System process or Data amendments attached to the Evidential Record;

- Systems Management – to demonstrate that the Detection and Enforcement Infrastructure was working correctly at the time of contravention;

- Operator maintenance and operations logs – to support the Systems management records;

- Systems Documentation to support the workings of the Detection and Enforcement Infrastructure.

5.3.3 Once created, the relationship between the individual components of the Evidential Record must be maintained at all times so that they cannot be disassociated. The relationship between the contextual images of the Capture Event, the close-up image, the unique identifiers and the Evidential Record Data block or string, and any additional non evidential processing information (e.g. the VRM plate patch image), must be locked to meet evidential requirements

5.3.4 All Evidential Records must be retained for a period of at least two days, to allow for quality checking and an Audit Trail created for all actions taken against an Evidential Record, including creation, access, transfer and deletion.

5.4 Evidential Integrity of Identification of Time.

5.4.1 Time synchronisation, linked to a remote reference time such as the MSF time signal or GPS, must be maintained. This is required to create an accurate and acceptable “Time Stamp” link between the images and Data, making up an Evidential Record.

5.5 Evidential Integrity of Identification of Location

5.5.1 The images shall show the location of the vehicle in the context of its surroundings and in relation to the scheme boundary and local landmarks through which the location may be recognised. This requirement could be met, for example, by the use of a ‘site pack’ which consists of a camera site plan and photographs of the site showing its location in relation to both the scheme boundary and local landmarks (railings, litter bins, lampposts etc), within the field of view of the Detection and Enforcement Infrastructure cameras.

5.5.2 The images showing the vehicles in the context of its surroundings shall include, at least some of the landmarks within the field of view of the camera.

5.6 Evidential Integrity of Identification of Vehicle

5.6.1 The image quality shall be such that it shall be possible to manually identify the make, model, colour and VRM of the vehicle, including any attempts to dissemble, distort or mask the VRM, or other elements in order to confuse automatic recognition systems. It is accepted that in the hours of darkness and in extreme weather conditions, it may not be possible to

confirm all aspects, in addition to the VRM, the image of which, must be visible under all conditions.

6 TESTING AND PROVING

6.1 Reliability and correct operation of the Detection and Enforcement Infrastructure is required by the Authority to ensure that enforcement and business operations can be carried out effectively and without the risk of loss of reputation or public confidence, in the integrity of the Evidential Record.

6.2 The Authority therefore requires of TfL that all testing and proving of the Detection and Enforcement Infrastructure including Outstation and In-station elements, is carried out to documented and agreed procedures covering Test Strategy, Test Plans, Test Specifications and Test Reports. This documentation shall be agreed and certified by TfL.

6.3 Test Specifications, as they relate to the integrity of the Evidential Record, must document the conditions to be tested (Test Criteria), with a reference for each condition back to the functional requirements and specifications.

6.4 Test Specifications must provide a mechanism to ensure trace-ability between specific Tests and the Test Criteria to which they relate, and to demonstrate coverage by the Tests of all the Test Criteria.

6.5 The Test Strategy must take account of the risks to the evidential integrity associated with poor performance and with Defects remaining in the various components and functions, and provide an approach commensurate with those risks.

6.6 Testing and proving are required at a number of levels and stages of an Implementation Phase:

- Design or ‘type performance tests’ of specially manufactured or configured equipment;
- Factory Acceptance Tests of any specially manufactured or configured equipment;
- Site Acceptance Testing of each Outstation and its component parts and alarms;
- Unit, System and Technical Integration Testing;
- Systems Integration Testing;
- Load and Stress Testing;
- Proving of the Detection and Enforcement Infrastructure;
- Ready for Service Testing;
- Regression Testing;
- Image Quality Testing and
- Routine Operational Testing following Maintenance.
- An annual test of any components which may have degraded with time or use (for instance, door switches).

6.7 Design or 'type performance tests' must be carried out at trial roadside sites and, where necessary, in a laboratory type environment operated by a testing house. At least one of the Evidential Integrity test environments must be representative of the operational environment such that realistic tests of performance and functionality can be performed during an Implementation Phase and the Operational Phase. If there are significant amendments, these tests will require re-execution following production of any initial production units. These tests must be completed before full scale manufacturing of any bespoke components, which will include but not be limited to: cameras, their housings and platforms; roadside cabinets or housings; and any other specialist components. These tests must be certified by TfL, who retain the option of witnessing or inspecting an agreed set of test reports and must cover as a minimum:

- Electromagnetic emissions and susceptibility;
- Inspection of the physical security of the equipment (keys, locks cables etc);
- Tests of actions on an unauthorised access to the equipment;
- Tests of Time Synchronisation and internal clock accuracy and operation of related alarms;
- Proving the Authentication and Encryption by making an "unauthorised" interception or modification to an Evidential Record.

6.8 Factory Acceptance Tests must be carried out by the manufacturer for each item of any specially manufactured or configured equipment to be supplied. TfL may optionally witness and approve the initial Tests and inspect the Test results and Test Reports. Following the initial Tests, the same Tests, or an agreed sub-set, must be run for every item before delivery from the factory and a certificate of testing provided with the delivered item.

6.9 Site Acceptance Testing which TfL may optionally witness or accept an agreed test report, will ensure that all elements of the Outstations are fully operational up to the point of connection to the communication links with the Instation and will include the capture of an image of optimum quality, of all "on site" cameras, as a bench mark for future comparison. Acceptance and certification by TfL will be on a site by site basis. Site Acceptance Testing will also be required during the Operational Phase, on an annual basis and following major maintenance or component replacement, such as significant changes to the camera, or to their configuration or set-up. These tests will include alarms for unauthorised access to the equipment.

6.10 Unit, System and Technical Integration Testing must be carried out for any programmable components of the Detection and Enforcement Infrastructure, carrying or interfacing with the

Evidential Record, and repeated annually. TfL will require evidence that this has been adequately undertaken.

6.11 Systems Integration Testing must be performed against Test Specifications agreed with TfL and will be witnessed by TfL. It may encompass the entire Detection and Enforcement Infrastructure together with the interfaces to other Service Providers.

6.12 Load and Stress Testing of all elements of the Detection and Enforcement Infrastructure is required to ensure that the security and integrity of the Evidential Record will be maintained under normal and extreme load conditions, and that the Systems remain reliable under extended and continuous use or any other stress conditions identified. TfL to agree to any load simulation tools used to carry out this testing.

6.13 Testing of the physical operational infrastructure to be used to deliver the Operational Services is required, in-so-far as it may impact on the evidential integrity. This will demonstrate that all Hardware, networks and any other equipment have been correctly installed, connected and configured, and that features such as component failure, backup and recovery, load balancing and Security mechanisms operate correctly.

6.14 Proving of the Detection and Enforcement Infrastructure must be carried out for an extended period during which each of the Outstations will be connected to the production Instation as they are commissioned and achieve Site Acceptance and will be operated continuously to provide assurance on image quality, reliability and performance. Any existing or additional Core Service Provider must participate in this stage of testing in order to ensure the suitability of their processes for use on Evidential Records generated from the Detection and Enforcement Infrastructure.

6.15 Ready for Service Testing must prove not just the technical aspects of the Detection and Enforcement Infrastructure but must examine the operational processes, procedures, and organisation across both a Service Provider, and if present a Core Service Provider, from the generation of Evidential Records from both existing and new zones through to generation of Penalty Charges, using the live operational Systems, where the risks to the live enforcement activity permit it, for at least some period of time.

6.16 Regression Testing, appropriate to the potential of the modification to affect the Evidential Record, is required for each Software release, change of hardware build standard or firmware, where existing functionality has been amended, or new functionality has been added to existing functionality. This is to ensure that the changes do not affect areas of the Systems not directly subject to the agreed modifications.

6.17 During the Operational Phase, Acceptance Testing will be undertaken, in addition to prior Testing undertaken by a Service Provider, where new releases include Changes. This will constitute the mechanism for acceptance of Changes to the Systems. TfL reserve the right to witness such testing for all Changes, and will agree and witness the Tests where a Change has been raised by TfL.

6.18 Test Issues and Defect Management

6.18.1 A Service Provider must provide and operate an Issue Management Log in which all Issues arising during Testing must be recorded.

6.18.2 A Service Provider must provide TfL on request with full extracts from the Issue Management Log for specific Issues in either electronic or paper format. TfL must be provided with direct read-only access to the electronic Issue Management Log on request, and shall be provided with full details of specific Issues in either electronic or paper format.

APPENDIX A

A STANDARDS

A1 The standards given in Table 1 are listed for reference and are indicative of the standards required by TfL for the preservation of the evidential integrity. At the time of introduction or replacement, all elements of the Detection and Enforcement Infrastructure should comply with the appropriate standard working practice and philosophy as defined by the relevant organisations. Where a UK standard is specified, equivalent standards from other EU countries may be acceptable by agreement with TfL.

A2 Where the relevant standards have been amended or superseded, the latest revisions or the superseding standards will apply, to any new or replacement elements of the Detection and Enforcement Infrastructure.

A3 Equipment must be constructed such that any parts likely to be exposed to the weather, shall comply with IP55 (BS EN 60529) against water and dust ingress.

Table 1: Standards

ISO/IEC 27002	Code of Practice for Information Security Management.
ISO/IEC 26514	Systems and software engineering -- Requirements for designers and developers of user documentation
BS EN ISO 90003	Guidelines for the application of ISO 9001:2000 to computer software
BS EN 60950	Specification for safety of information technology equipment, including electrical business equipment
BS EN 60529	Specification for degrees of protection provided by enclosures (IP codes)
EN 55022	Electro Magnetic Compatibility
BS EN 60073	Basic and safety principles for man-machine interface, marking and identification. Coding principles for indication devices and actuators
BS EN 60950	Specification for safety of information technology equipment, including electrical business equipment
HOSDB Digital Imaging Procedure v2.1 November 2007 Publication 58/07	Guide to the use and controls of digital images for enforcement use.

A4 The Detection and Enforcement Infrastructure must follow the guiding principles of the document used by the Criminal Justice System to determine whether digitally captured images are admissible as evidence. It is the (CAST formally, HOSDB) publication 3/96 entitled ‘Home Office and

ACPO Traffic, outline requirements and specifications for automatic enforcement Systems', including the clarification and update note 'Requirements for the Remote Recording from and Control of Unattended Home Office Type Approved Traffic enforcement Devices' Dr S R Lewis (July 2002), and the updated document (CAST, formally HOSDB) publication v2.1 November 2007, entitled 'Digital Imaging Procedure v2.1'..

A5 There are some instances where the above publications do not apply, because they are either superseded or specific to Police requirements, as follows:

- It is accepted that the requirement in the CAST, (July 2002) document to write to a WORM drive at the Outstation does not apply in the context of an analogue signal, which is transmitted to an in-station, via a dedicated fibre optic network. But, Section 4 of that document is relevant to a camera with a digital output and discusses how data may be transmitted over a public data network, utilising TCP/IP communications.

- The standard of Authentication and Encryption, must be as robust and secure as those in the above publication, which requires a standard comparable to those used by major financial institutions for the protection of financial data. If an unauthorised attempt is made to edit or change the record or images, the record and images shall be marked as such or defaced. In such a case, it shall be clear that the Evidential Record has been tampered with.

- The requirements specific to the Police National Computer and Offence Viewing and Decision System do not apply.

- There is no requirement for an air-gap between the network and in-station as there is no concept here of the PNC and PNN.

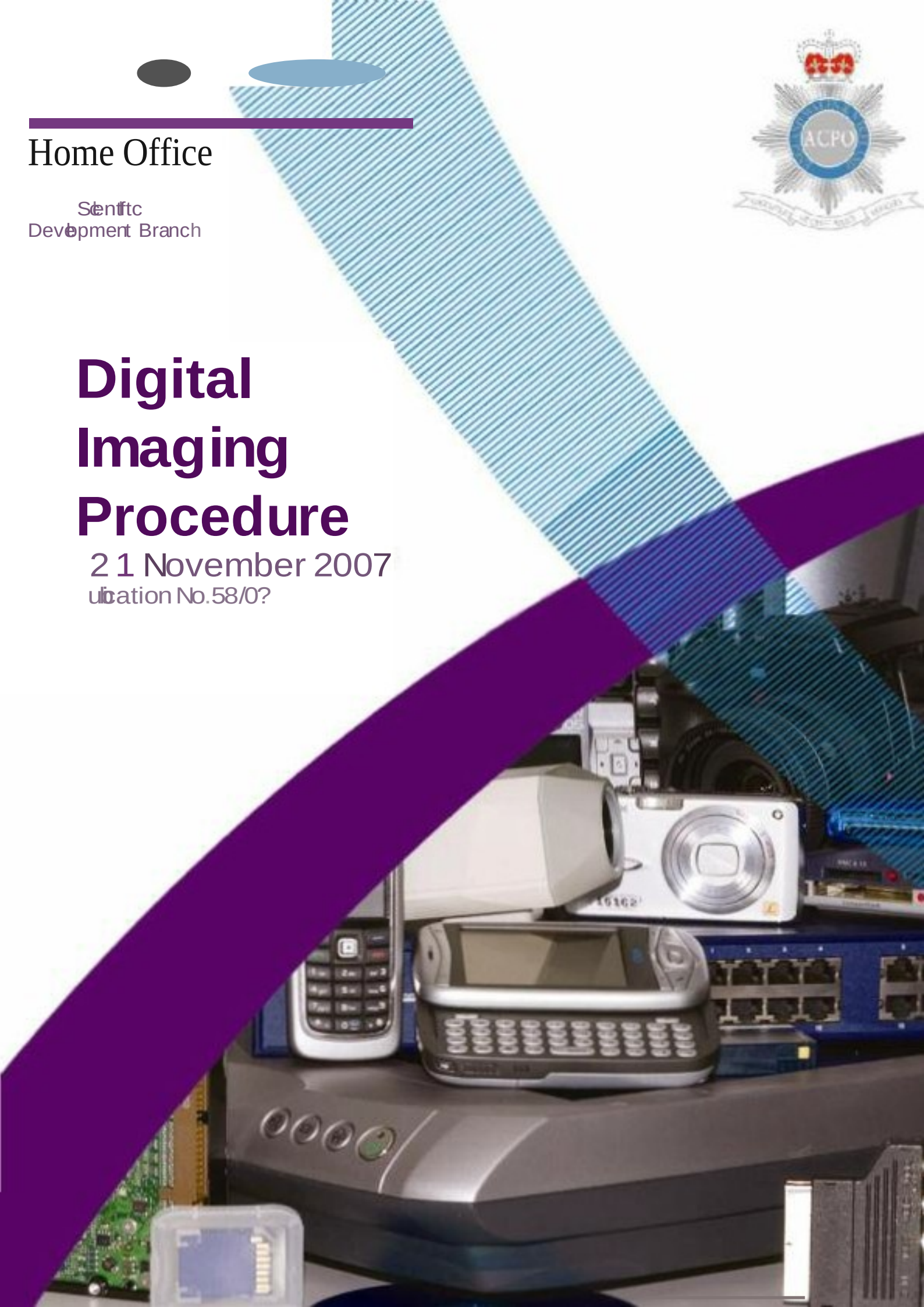
Home Office

Scientific Development Branch

Digital Imaging Procedure

2 1 November 2007

ublication No.58/0?



Digital Imaging Procedure

Version 2.1 November 2007

Neil Cohen
Ken MacLennan-Brown

Publication No. 58/07

2.1

With acknowledgement to Jim Aldridge and the project team who developed the original Digital Imaging Procedure on which this publication is based.

Digital Imaging Procedure

Version 2.1 November 2007

Neil Cohen
Ken MacLennan-Brown

Publication No. 58/07

2.1

ISBN: 978-1-84726-559-3

FIRST PUBLISHED NOVEMBER 2007

Home Office Scientific Development Branch
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051
Fax: +44 (0)1727 816233
E-mail: hosdb@homeoffice.gsi.gov.uk
Website: http://science.homeoffice.gov.uk/hosdb/

Foreword

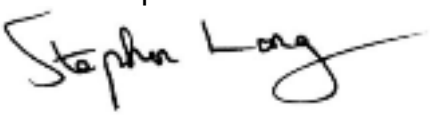
Digital imaging has become firmly established in the mainstream of public life and as a key enabling technology for the Police Service. With this in mind it was time to revise the *Digital Imaging Procedure*, first published in 2002. The aim of this new version is to build on the success of the original document and not only reflect current advances in technology, but also look to the future. The principal purpose of the procedure remains the same, i.e. to detail the processes involved in the proper capture and handling of digital images for police applications and to define best working practice. The target audience also remains broad, encompassing operational, administrative and judicial staff involved throughout all stages of the Criminal Justice System (CJS).

The key to the process is the creation of an identifiable and isolated Master reference copy at the earliest opportunity, whether on WORM media or within a secure network environment. This procedure enhances the integrity of proper evidential gathering processes whilst reducing the risk of malicious manipulation. Every effort has been made to keep the document as generic and technology-neutral as possible, however specific technologies and processes are addressed as necessary and references given for sources of more in-depth advice.

Digital imaging has enormous benefit for the swift and accurate outcome of investigations, particularly given the fuller use of network technologies. Whilst such technology has a price tag in terms of infrastructure and skilled technical support this is an enabling document that allows for the adoption of suitable technologies as the opportunities present themselves.

This document is not intended as a final or definitive report, as digital imaging and associated computer technology is a rapidly developing environment. We expect that operational implementation and court proceedings will refine some of the procedures set out in this document, although the framework itself is considered robust and defensible, and has been widely adopted since its original publication in 2002.

The information contained in this procedure has been derived, developed and reviewed through wide-ranging consultation with practitioners from the Police Service and related CJS organisations. This document also supports the *ACPO (2007) Practice Advice on Police Use of Digital Images v1.0*. I commend it to forces and other organisations for adoption as current ‘best practice’.



Stephen Long
DCC Wiltshire Constabulary
Chair ACPO Science and Technology Working Group

Contents

Introduction

The Digital Imaging Procedure is a guide for those practitioners within the Police and CJS who are involved with the capture, retrieval, storage or use of evidential digital images. It is focused around a flowchart that guides the reader through the process from the initial preparation and capture of images, through the transfer and designation of Master and Working Copies, to the presentation in court and finally the retention and disposal of exhibits. Supporting notes are provided for each step in the flowchart.

This version (v2.0) of the Procedure maintains the overall structure of the original document (v1.0), first published in 2002, but has been updated in two key respects. Firstly, it is recognised that there is now a broader range of technologies available for the capture and storage of digital imagery. Secondly, an allowance has been made for the possibility that the Police may wish to store Master and Working Copy data on a secure server instead of physical WORM (write once, read many times) media such as CDs and DVDs.

The bulk of this document comprises notes that should be read in conjunction with the flowchart. However, there are several issues that are not covered within the Procedure itself. These are introduced and discussed briefly in this section to answer some frequently asked questions about digital imaging.

What is the evidence?

Evidence, in terms of a still image or video footage, is the presentation of visual facts about the crime or an individual that the prosecution presents to the court in support of their case. The image will be presented either as hard copy or on a screen. This document is only concerned with the handling of evidential images, not those deemed to be 'Intelligence'.

With conventional photography, the negatives are often referred to as the 'primary' or 'original' images and the prints are all made from them. Similarly, with video and analogue recording the first tape is sealed as a Master once the first copy has been made from it. A copy of an analogue tape is always a degraded version because noise is added at each copying. This is compounded by the physical wear and tear of the tape.

However, it is possible to make a bit-for-bit identical copy of a digital image file. In evidential terms there is no distinction between the copy and the primary or original file because the files are the same and have the same evidential weight. It is not important whether the file is on a stand-alone or networked computer, a server, or on any type of storage medium. This assumes the operation of adequate security against unauthorised and unrecorded access.

If no discipline is applied there can be any number of identical files. For evidential purposes it is essential to be able to demonstrate that the images are authentic and have originated from the files captured in the camera and recorded to the first medium.

Digital image files can be used in exactly the same way as conventional photography and video with written audit trails. Electronic audit trails, if available, can augment or replace the written audit trails.

Digital images should not be thought of as replacements for conventional photographs and videos but as alternative technologies. It has to be recognised that digital images are not necessarily better than conventional ones. Some lower resolution digital images displayed on a computer screen or as hard copy might not appear very lifelike – but then neither do many simulations. The important and overriding factor is that the content of the image should be fit for purpose and that the quality is adequate. To this end the use of desktop printers for hard copies of stills and low resolution video footage must not be ruled out. It is not always necessary or feasible to produce the highest quality images to demonstrate the facts required for evidence.

Digital cameras use a multitude of complex image processing techniques to combine the signals from the charge coupled device's (CCD's) pixels into an image of the subject. However, the image is a representation of the subject in the same way as conventional photographs are. No one questions the chemistry involved in the development of the tiny grains in an emulsion and how the resolution and colour are chemically produced. In video, the images are

accepted as being fully electronically processed. Video recordings are admissible as evidence and the digital storage of the images does not alter that.

Compression

There are various compression algorithms used to reduce the amount of data in an image file to reduce both storage capacity and transmission bandwidth requirements. All compression algorithms remove data from the file and some are more effective than others at reconstruction of the data for replay. Generally, the greater the compression ratio, the more seriously affected is the replay.

If an image or video sequence is being presented as evidence and illustrates the facts of the offence then it is evidentially irrelevant whether the data has been compressed or not. What is important is the compression algorithm and ratio selected for particular applications.

Some compression algorithms are more suitable for fast movement, some for ‘talking heads’ scenarios. The compression can produce some artefacts which may mask the information or contaminate it with movement, patterns, outlining, etc. The algorithm must be tested on typical scenes. The image quality must be agreed and performance tests carried out to ensure suitability. Image processing cannot make up for inadequate data. Images should not be excluded because they are compressed and whilst there may be reasons to prefer some algorithms for reasons of quality, there is no reason to exclude any from evidential material.

File format

Digital data files can have a variety of formats.

The still camera industry is mostly using widely supported (or open) formats (TIFF, JPEG) although their highest resolution images are sometimes in their own proprietary format. This means these latter images have to be downloaded in a proprietary software package. An open format allows for ease of incorporating images into publications, printing and transmitting to others.

The manufacturers of closed circuit television (CCTV) video recorders are using a multitude of open, proprietary and mixed compression formats to meet the needs of massive amounts of information versus the cost of storage. Again, the format is not relevant to the admission of the evidence, only that the quality is fit for purpose.

Currently digital handheld video cameras mainly record to Hard Disk Drive (HDD) Mini-DV or flash memory (CompactFlash, SecureDigital, etc). As the market grows it is likely that more recording media will be introduced.

Secure server

Server storage has many advantages, particularly with regard to long term storage. The data can be migrated automatically and with no loss within a RAID array, ensuring that the data is accessible, as compared with a CD or DVD where once it has been noticed that the media has failed it is often too late. However, careful thought should be given to the administration and maintenance issues surrounding the server-based storage of images. If it is decided that server-based storage is the desired method then the following definition of a 'secure server' should be applicable to the installation.

The term 'secure server' should be taken to mean an environment, including a security management system, which is accredited to a level of at least 'RESTRICTED' under the Government Protective Marking Scheme (GPMS), in accordance with the ACPO Community Security Policy (CSP), as documented in an associated Accreditation Documentation Set (ADS) and as approved by either the local Force Information Security Officer and/or the National Accreditor for Police Information Systems.

Integrity Verification vs. Authentication

These two terms are frequently confused and often misused[*].

- **Integrity verification** is the process of confirming that the data (image, CCTV clip, etc) presented is complete and unaltered since time of acquisition. Relevant questions concerning integrity might include: "Has data been added to, or removed from the file?"; "Has the data within the file been changed?"

- **Authentication** however, is the process of substantiating that the data is an accurate representation of what it purports to be. Relevant questions concerning authentication would deal with issues such as: "Was the image taken at the time stated?"; "Was the image taken at the place stated?"

It should be noted that standard image processing techniques such as lightness or contrast changes would affect the image integrity but not the image authenticity; however, a change to the clock on a CCTV system could affect the image authenticity but not affect the image integrity. Robust audit trails are required in order to maintain image authenticity.

[*] Definitions taken from SWGDE / SWGIT Digital and Multimedia Evidence Glossary Version 2.2 November 2007 http://www.theiai.org/guidelines/swgit/swgde/glossary_v2-2.pdf

Preparation

These elements of the procedure include the preparatory steps before images are captured. This may be directly before the images are taken, or at an earlier stage or date where work can be anticipated. The steps identify the importance of:

- obtaining relevant authorisations;
- starting an audit trail at the earliest opportunity when it is known that the images are to be captured;
- checking equipment, either routinely or at the start of the image capture activity.

Such checks will avoid the embarrassment of failure and/or challenges about conformance with an accepted procedure. Digital image capture systems may increasingly be used by non-specialists in operational situations and locations so adherence to an established procedure will assist in safeguarding those captured images.

Obtain authority [1]

This instruction applies to all image capturers by virtue of their role or position within the Police Service. They are empowered to capture images for the purposes of their particular work. Specific roles and responsibilities, for example for a Scenes of Crime Officer or a Collision Investigator, will be written into their job descriptions, training and instructions, together with any verbal instructions. Obtaining authority is not necessarily required for each separate operational task.

However, police forces need to be aware that authorisations do need to be obtained before some images are taken, for example authorisation to permit images to be taken where ‘Directed Surveillance’ is requested under the Regulation of Investigatory Powers Act 2000. That authority must be obtained and recorded within the audit trail of the operation.

Start audit trail [2]

One of the fundamental requirements of digital imaging is the need to safeguard the integrity of images; part of this process involves an audit trail being started at the earliest stage. This may be a written audit trail, and/or incorporate an auto-generated electronic audit trail mapping the movement and changes of files on computers.

This Procedure relies on the written audit of activities. Where good practice is in place for the collection of evidence, including video and still images, there will be no change in principle. In practice, there probably will be little change in existing procedures with conventional photography except that the operator may receive reusable media to reformat and use; a process familiar to video operators.

The audit trail should include the following information (with date and time of action) when available and if appropriate:

- Details of the case.
- GPMS classification of the image (and any special handling instructions, if relevant) and the name of the person who classified the image.
- If the image is third-party generated, information about point of transfer including whether the image is the Master copy, a Working Copy or an exhibit derived from a Working Copy.
- Information about capture equipment and/or hardware and software used, including details of the maintenance log relating to capture equipment and calibration of hardware and software.
- Identity of the capture operative including third parties and image retrieval officers, where applicable.
- Details of exhibits and disclosure officer(s).
- Description of the images captured, including sequencing.
- Details of retrieval or seizure process and point of transfer, if applicable.
- Creation and definition of the Master copy and associated metadata.
- Storage of the Master copy.
- Any access to the Master copy.
- Viewing of the Master and Working Copies, including a record of any associated viewing logs.
- Details and reasons for any selective capture.
- Any editing applications which may alter the image.
- Any details of processing applications allowing replication by a comparatively trained individual.
- Electronic history log of processing applications.
- Any copying required to ensure longevity of the data.
- Revelation to the CPS of the Master and Working Copies;
- Any copying carried out as part of a migration strategy to ensure the replay longevity of the image;
- Disposal details and retention time periods.

The practices may not be familiar where imaging is a new feature of the work and it may be worthwhile to consult the Scientific Support Managers or equivalent adviser.

Where detailed information is required reference should be made to *ACPO (2007) Practice Advice on Police Use of Digital Images*, Section 2.5 Starting an Audit Trail and Section 4.1.1 Completing the Audit Trail and/or individual Force procedures.

Check operation of equipment [3]

The correct operation of any equipment is essential to gathering evidence.

In particular it is suggested that checks are made to ensure that:

- operator adjustable settings are made appropriately;
- the time and date settings are correct;
- there are adequate supplies of recording media, including spares in case of media failure;
- the media should either be new, reformatted or erased in an approved manner;
- any media protection settings will not prevent recordings being made;
- if the equipment is battery operated, there are sufficient fully charged batteries available;
- a scheme of checks is carried out before deployment particularly for equipment that is used less frequently.

It is essential that time and date settings are correct, any inconsistencies should be documented and the equipment monitored to ensure that further drift of these settings does not occur.

This list is not definitive and detailed information should be obtained from the equipment manuals.

Where detailed information is required reference should be made to *ACPO (2007) Practice Advice on Police Use of Digital Images*, Section 2.1 Considerations at Capture Stage, and/or individual Force procedures.

Capture, Protection and Storage

Police-originated images

These steps cover the capture of still or video images onto the chosen medium with due regard for the image quality and integrity of the images.

Third party origination

The Procedure diagram should be used to establish the 'point of transfer' at which the responsibility for the handling of third party images transfers to the police. That 'point of transfer' will depend on the nature of images being transferred, the recording format and equipment used by the third party. At whatever stage this 'point of transfer' occurs the police audit trail must start from that point. Continuity of image handling should be demonstrated throughout by ensuring that the police audit trail links directly to any audit trail that is available from the third party.

Third party image systems

Town centre CCTV cameras, for example, should follow established and standardised procedures. These systems should allow the police to;

- take evidential recordings away in order to safeguard them;
- replay the recordings in order to view, copy and process them;
- make authentic (not materially different) copies in formats suitable for use by investigators, Crown Prosecution Service (CPS) and the courts;
- access viewing facilities if the original format recording has to be viewed.

Whichever still or video camera or format of medium is chosen for the capture and initial storage of images, effective means must be available for transferring the images to the computer system where they are to be used and possibly archived.

Take images. Do NOT delete images [4]

Generally digital still or video equipment is used in the same way as analogue cameras. Two main differences:

- a choice of recorded image quality;
- the option to delete recorded images.

Capture

The image quality setting should be selected appropriate to the operational requirements rather than to minimise the storage capacity. Operators should anticipate their requirements and have sufficient empty storage medium available.

Selective capture involves the switching on and off of recording devices and should not be confused with other editing processes. For further information on selective capture see *ACPO (2007) Practice Advice on Police Use of Digital Images*, Section 3.1.1.

Still images can be captured on many different types of camera using a multitude of memory storage devices/memory cards. The manufacturer's manual should be referred to for instructions on correct use of this equipment.

There are several technologies for capturing video images digitally. Each is illustrated in the Procedure:

- magnetic tape – includes digital recording to conventional video tape, special digital video tape and data tape;
- WORM (write once, read many times) media, for example CD-R and DVD±R;
- reusable, removable, non-tape media, for example memory cards;
- computer hard disk drive (HDD).

Because of the high data rates associated with digital video, the image data is usually compressed in order to:

- reduce the stored data volume;
- reduce the time taken to transmit and/or the transmission channel bandwidth;
- lower the cost of storage media, for example by using low read and write speeds.

Where image sequence(s) have come from a non-removable medium the Working Copy or copies could be made:

- at the same time as making the Master;
- from the non-removable media after the Master has been made;
- subsequently from copying the Master.

Deletion of images

One crucial aspect of the Procedure is that none of the images taken should be deleted without authority. Any deletion of images, intentionally or accidentally, may be the subject of a 'challenge' or legal debate during any prosecution. Where such authority is given, deletions must be recorded in the audit trail and be subject to the requirements of the *Criminal Procedure & Investigations Act 1996 and Attorney General Guidelines on Disclosure of Evidence.*

Much equipment, however, does have the facility to delete recordings. On most digital still cameras there is an option to delete image files that have already been saved to the storage medium. Video recorders are designed to allow deletion by over-recording. Images should not be deleted from the recording which will usually become the Master.

In CCTV systems, video is recorded directly to an HDD, which is often designed to over-record automatically after a set period. Before this happens some or all of the images may be protected on the HDD preventing them from being overwritten.

Transmission

Usually images will be transferred directly from one medium to another (e.g. from HDD to WORM). However, in some cases the images will be transmitted across a network. This may occur either at the point of capture (e.g. IP CCTV cameras) or during transfer from the initial storage medium to the Master.

The security characteristics of different transmission methods should be considered and where necessary documented in the audit trail. This particularly applies to wireless transmission methods that may be susceptible to interception or unauthorised access. This should also be considered when using wired network transmission, particularly if the internet forms any part of the network transmission.

Protection and Storage [5]

Images on reusable media should be copied from the original storage medium in the original file format onto a secure media. This secure media could be WORM or secure network storage. The term 'secure server' should be taken to mean an environment, including a security management system, which is accredited to a level of at least 'RESTRICTED' under the Government Protective Marking Scheme (GPMS), in accordance with the ACPO Community Security Policy (CSP), as documented in an associated Accreditation Documentation Set (ADS) and as approved by either the local Force Information Security Officer and/or the National Accreditor for Police Information Systems. Once the images and associated data have been copied onto the secure media, they cannot be overwritten or altered.

The generation of the secure copy should be carried out as soon as possible after the capture to reduce the time and opportunity for the accidental or malicious alteration to images.

All imagery Master or Working Copies should be appropriately identified in order to facilitate the storage, retrieval and eventual disposal of case material.

In terms of evidential value there is no difference between bit-for-bit copies of the data on the Master, Working Copies and the images on the storage medium. This does not remove the necessity to protect the Master as an exhibit in case of challenges to evidence handling procedures or image manipulation.

The software required for viewing proprietary formats must be available otherwise the images will be inaccessible. It is advisable to store any replay software with each recording to assist with the correct viewing of the files.

The choice of using network storage or WORM media is a matter for force policy and should be guided by factors such as volume of data, predicted storage time and longevity of WORM media. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper-proof usage logs.

Non-reusable removable medium (WORM) [5a]

Non-reusable removable medium technology includes CDs, DVDs and specially designed WORM devices. They represent the ideal in that once closed the recording on the disk cannot be altered. Other WORM media types may become available.

The WORM medium must be closed to prevent any of the image data files being subsequently changed and further data written to the disk.

Optical disks (CD-R, DVD±R) must be ‘finalised’ or ‘closed’ in the camera or CD-writer before the disk is removed otherwise the images may not be viewable on a computer.

Video images

To allow ease of current and future use of the recordings for investigations and appeals, etc, the CD/DVD should include:

- the image sequence or sequences clearly identified;
- an easily-read text file stating any requirements for special hardware or software for replay;
- all associated metadata (time and date should be bound to the relevant images);
- licence-free software enabling the sequences to be viewed correctly;

Other items that could be included:

- text data about the originating camera or system;
- audit trails;
- authentication or verification software;
- short test sequence to confirm that the recorded image sequences are being replayed correctly.

Still images

In general, still images are stored in widely supported formats and there is no need for viewing software to be stored with the images, but where proprietary formats are used then the viewing software should be included on the media in line with the information given above for sequences.

Storage

The WORM media will usually be stored as the Master. However, the creation of a network server based Master could be considered for reasons of storage efficiency or data longevity. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper-proof usage logs.

Reusable memory [5b]

These include solid state memory devices such as CompactFlash, Memory Stick or any other reusable media such as CD-RWs and DVD±RWs.

Once the image files are saved to the removable medium they may be locked via the menu functions on the camera so that accidental deletion is prevented. SmartMedia cards can also have a physical protective seal to prevent all the images being deleted accidentally but this does not prevent the card being reformatted if the seal is then removed.

Media cards may have to be formatted in the particular camera prior to use otherwise they may not accept the images to be stored. A card cannot always be formatted in one type of camera, placed in another make and be expected to work.

Reusable media are now a cheap and common form of storage used across the range of imaging devices. These media are however, only designed for short term storage and any data stored on them is vulnerable to corruption or accidental deletion and therefore should be transferred as soon as possible to secure storage.

Once images are transferred to the Master, the reusable medium must be reformatted to remove all of the previous image files in preparation for reuse. This reformatting should be carried out in preparation for the work ahead and the officer should have sufficient empty media for such purposes. Reusable media cards should be erased in accordance with force policy as soon as all data has been transferred.

Storage

Reusable memory should be treated as a transport medium and as such the imagery needs to be copied onto secure storage as soon as possible. Individual Force procedure will determine whether WORM or secure server is the most appropriate route. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Non-removable medium [5c]

These are usually in the form of HDDs and mainly used for direct storage of video, but sometimes are also used for large file-size still images, for example fingerprints.

Because of the high cost and finite capacity of HDDs, images stored on them will usually be overwritten after a preset time or after the images have been transferred (backed-up) to some other medium for transport or archive. The back-up might be selective, by automatic or manual selection. It may be necessary to bring in specialists to ensure that the data is safeguarded.

Any difficulties with obtaining evidential material should be referred to the force TSU or video units. Reference should be made to the *ACPO Good Practice Guide for Computer Based Evidence V0.3* and *Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems*.

The normal mechanism for erasing data recorded on hard disks is to delete the directory entry only. The computer controlling the HDD then reallocates the space ready for a fresh recording. The new recording will then erase the previous recording by writing over the top of it and a new directory entry will be made. This means the data still exists and is recoverable until it has been overwritten.

When an incident or offence has occurred and there is a requirement to take information from the HDD as evidence:

- check whether the required data has already been copied to a back-up medium;
- check that what is needed is not being over-recorded while arrangements to save the data are being made;
- stop the recording process if necessary to preserve the data – this may put the system out of action until the data transfer can be completed;
- be prepared to seize the hard disk if necessary;
- transfer the data in a file format with software for accurate replay that can be used by the police, retaining original file format if possible;
- transfer to a recording medium suitable for play by the police.

Storage

Data held on an HDD could be written to WORM, copied to a secure network, or the original HDD could be retained as the Master, though retention of the HDD is strongly discouraged due to the uncertainty of its lifespan. However, if it is necessary to seize a large amount of data from an HDD then it may be impractical to transfer it to WORM, as it may take a considerable time to copy and require many disks. It should be noted that if the HDD is retained then write-blocking measures will need to be implemented before the HDD is accessed. Furthermore, checks should be made to ensure that the data on the

HDD is in a replayable form, as an HDD from a CCTV system, for example, may not be readable on a standard computer.

It may not always be possible to make the Master directly from the HDD (e.g. a CCTV system with a network port but no CD writer). The data would first be copied to a transfer medium such as a laptop, from which the Master could then be created. Once the Master has been produced, the data would be deleted from the transfer medium. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Removable tape medium [5d]

There are several types of tape onto which digital video can be recorded. In the case of a handheld digital camcorder the most common type at present is MiniDV.

Other formats of digital video tape recording include professional formats such as:

- DVCAM and DVCPRO;
- Digital Betacam.

Where the video footage has been recorded onto a digital tape in a handheld camcorder then this video tape will usually become the Master.

In the case of CCTV, the images may be recorded onto a data tape format. Digital Audio Tape (DAT) is one example. Whilst these tapes are removable it may not be feasible for the police to view the evidence without first transferring the data to another more convenient removable medium.

Where hard disk recording systems use tapes for back-up, the recording format may be non-standard to accommodate time lapse and multiplex recordings. These recordings will require special playback and copying facilities.

Analogue VHS copy recordings can usually be made from digital recordings though this usually entails a marked drop in quality and often causes the loss of the metadata.

As soon as an evidential tape has been removed from its recording device, the write-protect mechanism should be activated where available. This is usually in the form of a switch with two positions or a tab that can be removed to prevent the device from switching to record mode. For instance MiniDV cassettes have a switch which can be in one of two positions marked REC and SAVE. Placing the tab in the SAVE position guards the tape from being accidentally erased by over-recording but will not prevent damage or erasure due to careless handling, proximity to magnetic fields or poor storage conditions, etc.

Storage

Whilst it is most likely that digital video tape (e.g. DVCPRO, MiniDV) will have its write protection enabled and be designated as Master, the option exists for a Master to be created on a WORM medium or secure network storage.

If imagery stored on data tape is to be transferred to secure network storage it must be ensured that the data is in a replayable form or that the software required to access it is available and capable of reading the data from its network location. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Network [5e]

Though not common at the time of writing it is likely that direct access to third party networks (e.g. corporate IP based CCTV systems) will be granted to the police. Images could then be retrieved directly from the third party network. The choice of copying retrieved images to a secure network or WORM media for final storage will be a matter for individual force procedure. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper-proof usage logs.

Secure police network [5f]

The term 'secure server' or secure police network should be taken to mean:

An environment, including a security management system, which is accredited to a level of at least 'RESTRICTED' under the Government Protective Marking Scheme (GPMS), in accordance with the ACPO Community Security Policy (CSP). This should be as documented in an associated Accreditation Documentation Set (ADS) and as approved by either the local Force Information Security Officer and/or the National Accreditor for Police Information Systems.

If the data is captured directly onto such a secure server (e.g. ANPR) then it can be designated ‘Master’ in-situ and Working Copies created as required. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Where detailed application specific advice is required see the relevant ACPO guidance documents.

Supplementary protection

There are various media on which images can be captured, both reusable and non-reusable. Irrespective of their nature, early transition from ‘capture’ to ‘defining the Master’ phases is extremely important. The integrity of images needs to be protected at the earliest stages as this reduces the opportunities for challenges at court.

Accidental alteration or erasure could be detected by noting image number sequences and prevented by:

- designating the image file as read only;
- activating the mechanical write protect mechanism;
- transferring to WORM media

Protection can also be achieved by controlling access to the file or media by electronic password and/or controlling the viewing of images by electronic encryption.

The Procedure does not rely on any form of ‘electronic’ protection but neither does it preclude its use. There are several methods for ‘electronically’ verifying the integrity of an image file. Once applied, any change to the pixel values will be detected although the nature and location of the changes may not be indicated.

File integrity techniques

If a ‘hash’ function is applied to an image, a unique numerical value is calculated for the whole image. The number is embedded in the metadata of the image file. A change in pixel value causes the ‘hash’ function value to change. This is the basis for most ‘authentication’ software. Manufacturer specific software for image integrity is becoming increasingly prevalent, as are non-destructive (i.e. fully reversible) editing techniques.

Watermarking

Watermarking describes visibly insignificant changes made to the pixel values to incorporate information which changes if the image file is altered. The watermark may then become visible on the picture or even make it unreadable.

The primary use for watermarking is to protect the intellectual property rights of the photographer or film maker. Its use may lead to claims that the image is not authentic because the pixels have been changed, therefore the use of watermarking is not recommended for image integrity.

Encryption

The image file is encrypted so that the file cannot be opened except with the correct decryption key. This has particular value if images are to be transmitted

to or from remote sites. Loss or corruption of either the key or the data may make files unrecoverable.

The use of electronic protection is mandatory in the digital imaging used for roadside cameras where there is unattended capture, the image is the only evidence of an offence having taken place and the images are transmitted from the roadside to a central facility. Refer to *Home Office and ACPO Traffic, Outline Requirements and Specification for Automated Traffic Enforcement Systems,* S Lewis, PSDB 3/96.

Handling

Images should also be protected from accidental deletion by the careful handling of media. Media should be stored in clean, dry environments and kept away from strong magnetic fields, strong light and chemical contamination.

Some media such as CDs and SmartMedia will be damaged if allowed to become dirty or scratched.

Use

The Master is defined and will be documented as such. It will then be stored securely pending its production (if required) at court as an exhibit. Only in the event of any doubt being cast on the integrity of the images will the Master be viewed.

A Working Copy is usually produced simultaneously, or immediately after the Master is defined. The Working Copy, as its name implies, is the version that will be used for investigation and to assist in the preparation of the prosecution file.

Where it is believed that images relate to any crime or incident pending civil or criminal proceedings they must be retained ensuring compliance with the *Criminal Procedure and Investigations Act 1996, the Data Protection Act 1998* and *ACPO (2006) Guidance on Management of Police Information*.

All use and movement of the Master will be logged in the audit trail. Similarly any significant use, enhancement and distribution of Working Copies should be logged. The aim is to support the presentation of evidence through legal proceedings. All audit trails should be disposed of when the image files and any analogue copies are disposed of.

Where detailed information is required reference should be made to *ACPO (2007) Practice Advice on Police Use of Digital Images*, Section 5.3 Disposal and Section 5.3.2 Disposal of Data and Audit Trail, and/or individual force procedures.

Define Master and produce Working Copy [6]

The core of the Procedure is the production, definition and storage of a Master which can be examined if required by the court to confirm the integrity of the images. The Master should be:

- labelled or named (with due care to the longevity of label and readability of medium);
- stored in a form and manner, with software if required, so that the images may be viewed in the future;
- kept in accordance with exhibit protocol;
- never used, except to make further copies together with appropriate audit trail, or by order of the court to verify integrity.

Force policies should be developed to cater for these requirements.

Image files should be in the same format as:

- received by the force in the case of third party images
- first captured on medium in/or attached to camera;
- as recorded after transmission from camera.

Still images

The first WORM copy is usually the Master.

Video images

Where video is recorded to tape, existing best practice procedures define the original tape recording as the Master. In other cases a Master needs to be defined. This can be done by:

- making two copies simultaneously and defining one as the Master and the other the Working Copy;
- making two copies, consecutively, from the HDD and defining one as the Master and the other the Working Copy;
- making one copy, the Master, and making a Working Copy from that Master.

When video is recorded to a hard disk it can be copied to secure network storage and designated as the Master. Where video sequences are stored on the HDD of a computer with no effective means of downloading the data, the computer may need to be seized in order to safeguard the data until arrangements for download or copy can be made. Any difficulties with obtaining evidential material should be referred to the force TSU or video units. Reference should be made to the *ACPO Good Practice Guide for Computer Based Evidence* and *Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems.*

Produce Working Copies

Working Copies can be in many forms. The files can be copied onto any suitable medium or distributed electronically (if a secure system is in place) for circulation to the investigating officers and CPS. Issues of quality control, security and resource management need to be considered.

Where detailed information is required reference should be made to the *ACPO (2007) Practice Advice on Police Use of Digital Images*, Section 4.3 Transfer of Digital Images to the Crown Prosecution Service and/or individual force procedures.

Document and secure storage of Master [7]

The Master is defined, will be documented as such and retained in secure storage as an exhibit for court purposes.

Local force policies need to be established to ensure that the integrity of the images is maintained throughout the storage, to include the period before, during and after any court proceedings during which the images might be used.

There will be times when the Master may need to be viewed and/or a fresh Working Copy produced. Force policy needs to be developed concerning the actual process of opening the exhibit and any seal that has been used to protect the images. At present this storage is on a physical, separate piece of medium such as a tape or disk. If electronic storage on a computer system is used then equivalent procedures will need to be in place to maintain the integrity of the Master. The location and any access to the Master or movement of the Master should be recorded in the audit trail.

Whatever form the Master takes it is essential to label it adequately, protect it from physical damage and contamination and store it securely. Whether this is a room or locked cabinet it should have a clean dry atmosphere with temperature variations limited to normal room temperatures to prevent condensation. Where long-term storage is required see *Technical Issues Relating to the Storage, Replay and Disposal of Digital Evidential Images*.

Retain as exhibit [8]

The Master should be labelled, protected and stored in accordance with force procedures in order to fulfil statutory requirements.

Audit trails started at the outset of the image capture process should be completed and documented contemporaneously. A similar process may be necessary for those Working Copies that may be produced as evidence. Retention of images should conform to the Data Protection Act 1998, the Criminal Procedure and Investigations Act 1996 and *ACPO (2006) Management of Police Information*. Media containing images should be kept in a suitable environment and catalogued for accessibility.

Produce Working Copies [9]

Once the Master has been defined and stored, all use of images should be from a Working Copy. Bit-for-bit copies should be used (where possible) for further reproduction of additional Working Copies or where precise detailed analysis is to be carried out or when images are to be enhanced.

The Master should never be used, except to produce additional Working Copies when no other Working Copies are available to copy, or by order of the court to establish authenticity. Force procedures will need to detail the circumstances and the relevant processes involved. All actions will need to be entered in the audit trail.

Working Copies produced for the investigation, technical investigation, briefings, circulation, and preparation of prosecution evidence and defence can be in any of the forms described:

- Tapes or digital media in available-equipment form;
- Hard copy stills from still or video cameras;
- Edited video;
- Enhanced still or video.

The copying and distribution of Working Copies should be in accordance with force procedures with appropriate audit trails as required.

The production of copies on media such as CDs, DV tapes and prints requires specialist equipment. The copying of files within a computer is easy and so needs to be disciplined to prevent unnecessary files being produced.

It is not suggested that all Working Copies should require individual audit trails, although certain application specific situations and/or enhancement processes may require audit trails to be maintained for additional Working Copies. Where this is the case records need to be kept contemporaneously.

Where detailed information is required reference should be made to *ACPO (2007) Practice Advice on Police Use of Digital Images*, Section 4 Disclosure and Revelation to the Crown Prosecution Service and/or individual force procedures.

Prepare prosecution file [10]

Officers responsible for file preparation should:

- ensure that the Master is kept in suitable and secure conditions by the police and is made available to the prosecution or defence, upon request;
- liaise with the relevant CPS prosecutor at an early meeting to discuss the processes and capture systems used, where relevant;
- provide the CPS with full information accompanying any evidential digital images, this might include audit trails, maintenance logs, viewing logs and disclosure schedules;
- list and describe any unused and/or unviewed material clearly;
- ensure that viewing logs used for moving images highlight relevant sequences;
- provide the CPS with accurate information about the preferred format for revelation in order to reduce the loss of image quality;
- consider the format in which the image is provided to the CPS in order to facilitate viewing and replay;
- liaise with relevant departments within the CPS to ensure that viewing and replay is possible prior to trial.

Present exhibits for court [11]

All images should be presented so that evidential content is not compromised. Where possible, images should be presented in their native or original format. If there is pertinent material that can only be seen when the image is viewed in digital form then provision should be made for appropriate playback equipment to be provided in court, if these arrangements are not already in place.

It should be understood that images may look different depending on the equipment used. In particular, images viewed on different screens may appear different from one another. An accurate replay facility should be provided wherever possible.

Concerning the presentation of images in court, HOSDB is

- Liaising with the Criminal Justice System;
- Representing the police requirements to these bodies;
- Advising the Police Service on the selection of compatible hardware, software and media to facilitate effective case handling.

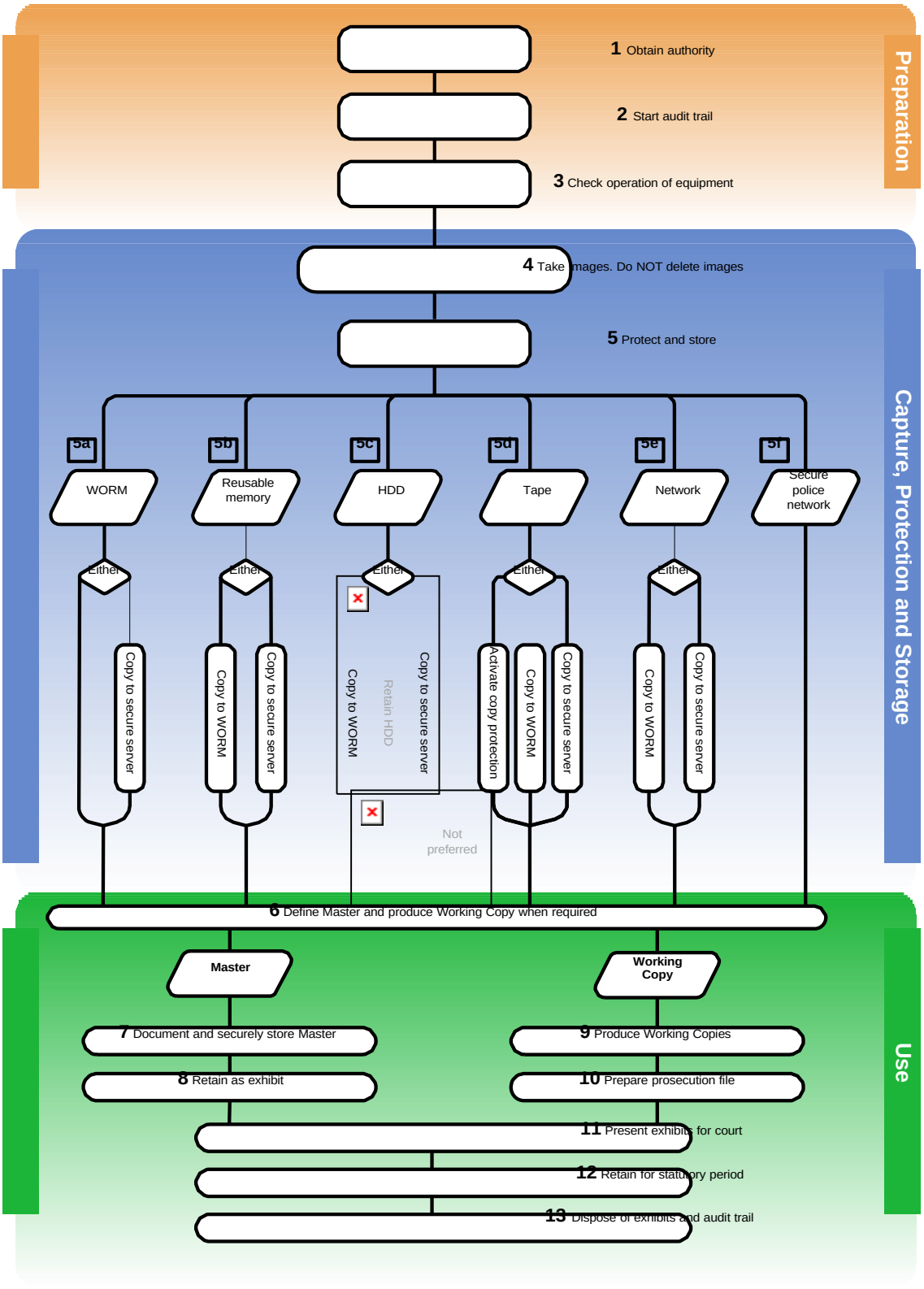
Retention and Disposal [12]

CDs, DVDs, digital tapes etc, are designed for short-to-medium term storage periods. To ensure the integrity of the data the files need to be transferred to new media regularly, possibly as often as every five years, or transferred to professionally managed data management archive systems.

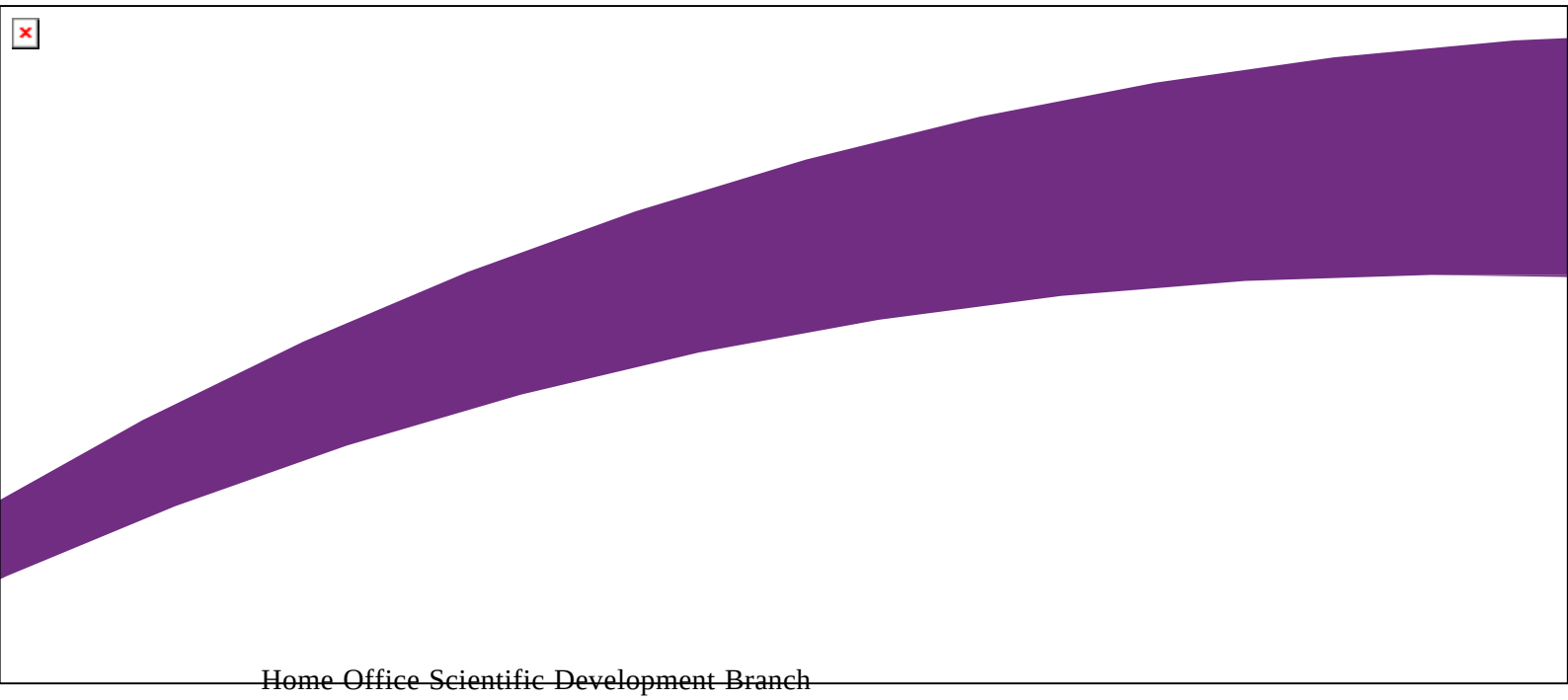
Detailed advice can be found in: *ACPO (2006) Management of Police Information* and *ACPO (2007) Practice Advice on Police Use of Digital Images*, Section 5 Retention, Storage and Disposal of Images.

Dispose of exhibits and complete audit trail [13]

Each force needs to consider mechanisms for the disposal of images and complete audit trails once the statutory periods of retention are completed, in line with the principles of *ACPO (2006) Management of Police Information*.



For further explanation use accompanying notes and refer to force policy.



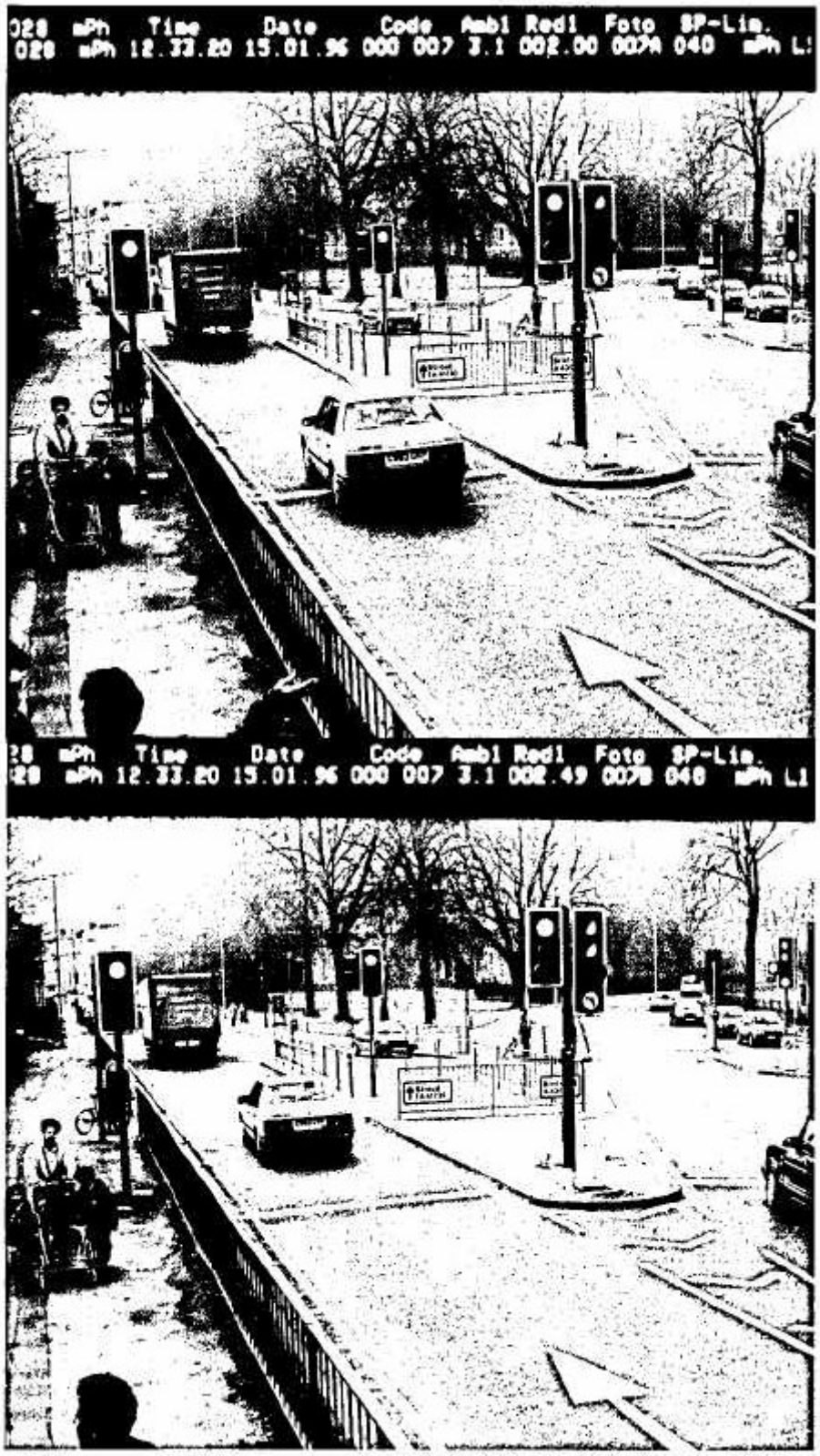
Home Office Scientific Development Branch
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051
Fax: +44 (0)1727 816233
E-mail: hosdb@homeoffice.gsi.gov.uk
Website: http://science.homeoffice.gov.uk/hosdb/

ISBN: 978-1-84726-559-3

Home Office and ACPO Traffic Outline Requirements and Specification for Automatic Traffic Enforcement Systems

Dr S Lewis



POLICE SCIENTIFIC DEVELOPMENT BRANCH

Publication No 3/96

HOME OFFICE
POLICE POLICY
DIRECTORATE

HOME OFFICE AND ACPO TRAFFIC

Outline Requirements And Specification For Automated Traffic Enforcement Systems

S Lewis

3/96

POLICE SCIENTIFIC DEVELOPMENT BRANCH
HOME OFFICE POLICE POLICY DIRECTORATE

HOME OFFICE AND ACPO TRAFFIC

Outline Requirements And Specification For
Automated Traffic Enforcement Systems

S Lewis

FIRST PUBLISHED 1996

Published by:

Home Office
Police Scientific Development Branch
Woodcock Hill
Sandridge, St Albans
Hertfordshire AL4 9HQ
United Kingdom

COVER PHOTOGRAPH
Offence images from a red light camera.

Printed by:

White Crescent Press
Crescent Road
Luton
Bedfordshire

Management Summary

This document provides guidance to industry on Home Office and ACPO requirements for future automated traffic enforcement systems.

The proposed system comprises road side sites equipped with unmanned traffic enforcement equipment which detect and record data to be used as evidence of a traffic offence. The sites are connected over a data network to a central Offence Viewing and Decision System (OVDS). The document specifies standards for the quality of electronic images to be used and the data protection needed to ensure full acceptance of the evidence by the courts. This is of paramount importance. For use over a public data network, data protection modelled on current practice in the financial sector is required.

The OVDS provides an image data base and easy to use facilities for viewing the offences. Its operations, which include vehicle keeper enquiries made to the Police National Computer or DVLA's data base, are listed. The system is required to provide for electronic data transfer to systems used for processing fixed penalty offences.

Contents

Introductions

"Fundamentally, for anyone to be convicted of an offence, the person making the allegation must prove it. Each and every part of the evidential chain must be capable of withstanding vigorous scrutiny.

Technology now allows the opportunity for evidential data to be recorded by mechanical processes, compressed into digitised format and transmitted across communications links. Crucially, adequate protection must exist in those processes to protect the public from any suggestion that data has been corrupted and evidence compromised.

Standards set out in this document, preserve the integrity of the process and enable the public and the courts to be confident in the evidence we adduce".

G R Markham Esq QPM BA (Hons) Assistant Chief
Constable (Operations) Essex Police
Chairman ACPO Traffic
Traffic Enforcement Sub-Committee

"Promoting effective and efficient policing is a key function of the Police Policy Directorate, and nowadays that automatically includes making the best possible use of modern technology. This document fulfils an important need to think ahead in the design of such technology, and so provide industry and other interests with a framework within which to plan development. As head of the Operational Policing Policy Unit, I welcome this document as a co-operative work in which the Police Scientific Development Branch, the Association of Chief Police Officers Traffic Committee, and my Policy Unit have pooled their experience to provide practical advice to guide the development of traffic enforcement technology in the private and public sectors".

Nick Sanderson
Head of Operational Policing Policy Unit Police
Policy Directorate
Home Office

1 INTRODUCTION AND AIMS

1.1 The purpose of this document is to inform and provide guidance to industry on the Home Office and ACPO Traffic Committee's requirements for future automated traffic enforcement systems.

1.2 The Road Traffic Act 1991, which came into force on 1st July 1992, facilitated the use by the police of unmanned equipment for the enforcement of speed and traffic light violations. The equipment has to be type approved by the Home Secretary. It also introduced a conditional offer fixed penalty scheme to allow the police to deal with the offence by post. The Road Traffic Act 1988, Section 172, requires the person keeping a vehicle (or any other person identified as having relevant information), to supply the details of the driver of a vehicle at the time certain road traffic offences were committed. Exceeding the speed limit and failing to conform to red traffic lights are two of those offences.

1.3 To give effect to these new provisions, some police forces, working with their Local Authorities, have begun introducing a variety of automatic enforcement schemes based on local organisation and resources. Most forces are planning the introduction of their own schemes. Consequently the number of offences detected in this way and requiring processing by the police and the courts is likely to grow substantially.

1.4 A steering group of representatives from the ACPO Traffic Standing Sub-Committee on Traffic Enforcement Technology, the Home Office, F8 Policy Division and the Police Scientific Development Branch was formed in 1993 .The group set the following aims for its work:

"While maintaining the quality and acceptability of the evidence to the courts, reduce the cost and increase the throughput for processing fixed penalties from unmanned traffic enforcement equipment through the application of technology, encouragement of best practice and advice to industry."

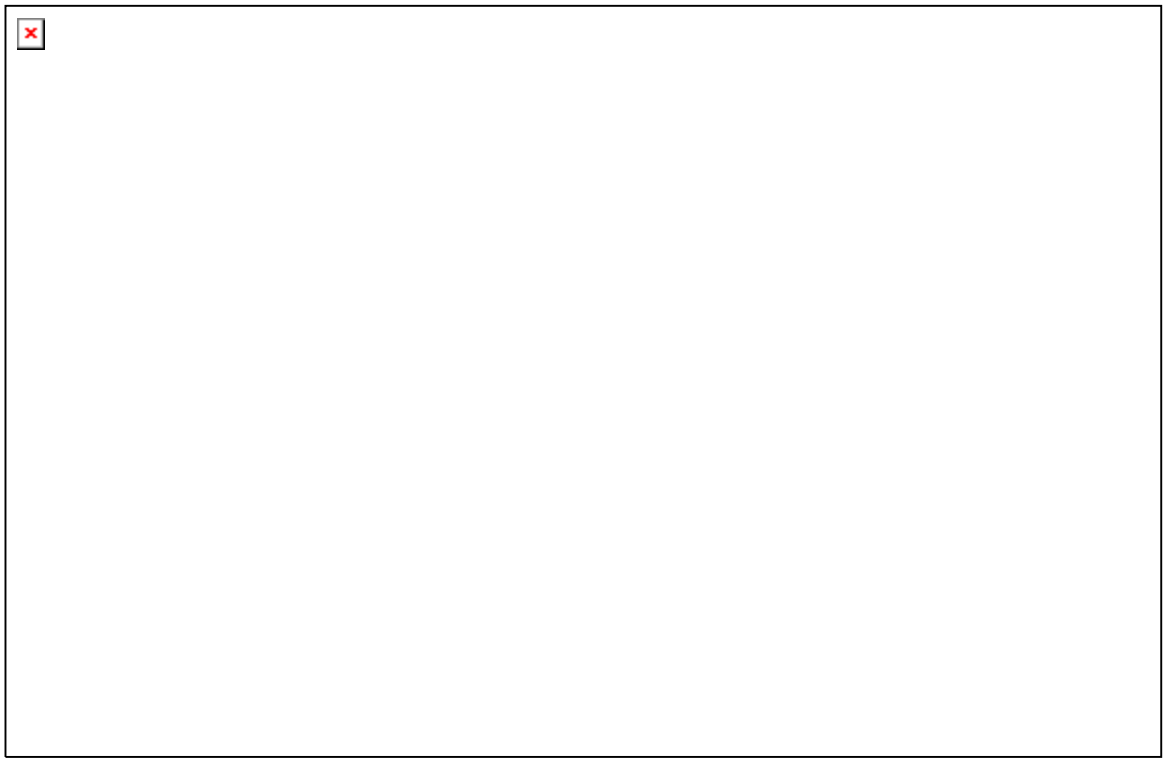
1.5 The group developed a draft of this document whose principles were agreed by the ACPO Traffic Standing Sub-Committee on Traffic Enforcement Technology in September 1993 and by its parent committee, ACPO Traffic, in November 1993. A fundamental requirement for the system is the use of electronic images in place of the conventional photographic film currently used. However the complex issues raised, in particular the standards necessary for maintaining the quality and acceptability of the evidence to the courts, still required detailed and careful consideration. This has now been done and the standards included in this published version.

1.6 While it is a legal requirement for the road side equipment which detects, measures and records the evidence of a traffic offence to have Home Office type approval, this does not extend to the rest of the system or the electronic image standards referred to above. However complete systems and sub-systems will be considered by the ACPO Traffic Standing Sub-Committee on Traffic Enforcement Technology which will consider giving ACPO approval for their operational use.

2 SYSTEM OPERATIONS AND REQUIREMENTS

2.1 The individual system operations and their requirements which, taken together, would provide the basis for an efficient system meeting the aims given in 1.4 above are outlined below. Each may be regarded as a sub-system of the whole system and can be usefully considered as modules from which it may be constructed.

2.2 The proposed traffic enforcement system for meeting the aims of the steering group is shown schematically below. Also shown is the requirement to interface with other systems used for processing fixed penalty offences.



2.3 The traffic enforcement system is for the efficient detection, collection and viewing of evidence from type approved unmanned enforcement equipment located at road side sites. The system is required to support the current equipment approved for the enforcement of speed limits and red traffic light signals and any future type approved equipment.

2.4 The equipment at each mad side site comprises the automatic traffic enforcement equipment which detects, measures and records offences and processing hardware for applying data compression and security to the electronic images it outputs.

2.5 The data network, which may be any private or public network provides for the transmission of the offence data to a central point. This requires standard communications equipment at each site and at the central system. Depending on the -overall system design and the data collection method programmed on the central system, different amounts of data buffering will be required at each site. Data security, which

will need to withstand evidential scrutiny in the courts, shall be automatically managed on the central system including the use of the data network for that purpose.

2.6 However the main functions of the central Offence Viewing & Decision System (OVDS) is to provide an image database for the viewing and storage of offence data and assist the process of identifying the driver.

2.7 Finally the system should provide for the electronic transfer of offence data between the OVDS and existing police systems and a future standard system for the processing of fixed penalty offences. In relation to existing systems this will normally be the force Central Ticket Office (CTO) computer system. However a standard fixed penalty processing system is being developed for use by CTOs and Fixed Penalty Offices (FPOs) (who support the work of the Magistrates' courts) with which the traffic enforcement system will eventually need to be interfaced.

2.8 An important general aim for the system is that it will operate effectively with police officers only undertaking those tasks that need police officers to carry them out such as the viewing and decisions on offences (required by the 1991 Road Traffic Act) and maintaining public support and acceptability for this method of enforcing traffic law. However the provision, servicing and maintenance of the system does not require police officers. This could be undertaken by civilian staff accountable to the police and operating to agreed standards and could be provided under a service level agreement.

2.9 The processing of offences after the police have viewed and made their decisions on the evidence, should also be undertaken by civilian staff using the available fixed penalty processing system. While interaction between the OVDS office and the CTO should be by electronic means as much as possible, they should be co-located to make remaining contact as efficient as possible.

3 OFFENCE DETECTION, MEASUREMENT & RECORDING

3.1 Automatic enforcement equipment

3.1.1 The first operation in the system is to detect automatically, measure and record the occurrence of an offence at mad side sites. For cur[r]ent type approved equipment the operation produces the following:

(a) a pair of images of the scene of the offence taken at a set time interval apart
(b) an image of the offending vehicle's registration number
(c) a record of the location, time and date
and
(d) in the case of a speed offence, an accurate measurement of the vehicle's speed or
(e) in the case of a red light offence, the elapse time since the signal turned red. A speed of the vehicle is also given.

3.1.2 It is of paramount importance that this evidence is of such unquestionable accuracy and quality that it is readily accepted by the courts and public. It is the purpose of the type approval process to ensure this is the case and the requirements for this, including the evidence to be produced, are given in the latest versions of the type approval handbooks published by PSDB. Any enforcement equipment type approved by the Home Secretary for unmanned use may form the basis for this part of the system.

3.2 Image recording and quality

3.2.1 While any medium that can record the evidence with sufficient quality to meet the above requirement may be used, to meet the aims set for this system, the data needs to be recorded and stored in electronic form. The use of electronic images provides the opportunity for reduced staff costs and greater ease of use and is a fundamental requirement for an efficient system. Electronic images are acceptable to ACPO, the Home Office and the Crown Prosecution Service (CPS) if the guidance given below is adhered to.

3.2.2 In general terms, acceptable image quality is that which most people would feel clearly portrayed all the information relevant to proving the offence.

3.2.3 High resolution digital cameras with a resolution near to 1000 by 1500 picture elements or greater may directly replace the photographic cameras in current use and produce images of acceptable quality.

3.2.4 While the cost and availability of digital camera technology with sufficient resolution to capture both the scene of the offence and the vehicle registration number through a single lens is disadvantageous, a complex video image captured using two lenses with different focal lengths may be used. The ratio of the focal lengths should be near to 4:1. The image will then be in two parts, one showing the over all scene and the remainder showing the registration plate with sufficient body work of the vehicle to demonstrate its compatibility with the scene. The images should be in colour. The same date, time and location information should be simultaneously inserted in to both parts or placed along the common boundary between them.

3.3.5 Electronic images may be compressed to reduce theft data capacity using recognised standard methods provided the general requirement given in 3.2.2 is complied with. Images taken from either the high resolution digital camera or the complex video system described above will reliably meet this if compressed between 20:1 and 25:1 using the JPEG compression standard (ref. ISO/IEC 10918-1). This is recommended for use in this system.

4 EVIDENCE COLLECTION AND PROTECTION

4.1 The evidence recorded automatically at the road side is currently manually retrieved for immediate viewing and processing because photographic film is used. Electronic imaging however permits the data to be collected and transmitted automatically with minimal delay over a data network. Data collection must to be done promptly in order to ensure that notices of intended prosecution can be issued within a prescribed time limit of 14 days. For the proposed electronic imaging system, the evidence should be retrieved by electronic transmission over a data network to a central point co-located

with the Central Ticket Office. To provide frequent data collection the system should provide either immediate data transmission or regular (i.e. at least daily) system polling.

4.2 In addition to the frequent transmission of the data back to the central point, the system shall store the data on site using removable Write Once Read Many times (WORM) technology. Capacity to store data for at least 10,000 offences should be provided. Which ever method of data collection and storage is used, sufficient speed of collection and storage capacity shall be provided to ensure no loss of data.

4.3 The integrity and full acceptance of the evidence by the courts 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 courts. Both public and private data networks may be used, but the levels of data protection required are different.

4.4 For a private data net work i.e. one for which it cannot be alleged members of the public can gain access, it is sufficient to apply standard error correction methods to ensure no accidental errors can be introduced during the transmission process. This should be done in the proposed system by using a 16 bit Cyclic Redundancy Check (CRC) in accordance with the CCITT V41 standard for this error correction.

4.5 Normally the requirement will be to transmit the data over a public data network. If the following data protection measures are adhered to, then in principle any public data network, including digital radio networks, may be used. Price and speed will be major determining factors.

4.6 The purpose of the data protection to be applied when public networks are used is to ensure that a defence based on an allegation that the data could be tampered with by anyone accessing the network would be implausible and have no credibility in the courts. The standard data security measures used by major financial institutions for the protection of financial data meet that requirement and this is readily understood by the courts. The process is specified in published international standards (see below) and provided commercially by specialist companies to the financial sector. It is a requirement of the proposed system that data protection as used in the financial sector is applied to the offence data transmitted over a public data network.

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

(1) Authentication
(2) Encryption
(3) Error protection.

4.8 Authentication is the principal element in establishing the integrity of the evidence. A Message Authentication Code (MACS) comprising four 8-bit bytes of data is computed and appended to the image. The MAC is a complex function of a secret 56 bit authentication key. The integrity of a received image is verified when re-computing its MAC using the same key produces the same answer.

4.9 Encryption transforms the image into random data. It ensures the nature of the data is unrecognisable to an unauthorised observer and ensures it is not possible to selectively alter a part of images or even monitor them. The data can only be corrupted blind which would be picked up by the authentication process. Another 56 bit encryption key, chosen to be different from the authentication key, is used for the encryption

4.10 Finally, error protection using the same CRC check referred to above must be used. While the MAC check would also detect any accidental errors introduced during transmission, because it requires error free transmission of all the data before it can be applied, it is not commensurate with efficient transmission. The encrypted data with the MAC appended should be transmitted using the same standard error correction methods given above for transmission over private networks.

4.11 The process implemented at the roadside site, which must be undertaken in the following order, is to:

1 Calculate the MAC of the whole image
2. Encrypt the image
3. Append the MAC to the encrypted image
4. Compute the CRC for each transmission segment
5. Transmit each segment

4.12 At the receiving end on the OVDS the process is to:

1. Check each CRC and request re-transmission when necessary
2. Decrypt the image
3. Recalculate the MAC from the decrypted image
4. Compare this MAC with the transmitted MAC
5. Accept as valid data only if they are the same.
6. Portray image in acceptable format for decision or disposal

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

4.14 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 for both. This shall be the Data Encryption Standard (DES) specified in ANSI X3.92-1981 or NBS FIPS 46.

4.15 The authentication process shall follow the ANSI X9.9 and ISO/IEC 9797 - 1989 standards.

4.16 The encryption process shall use DES with 64 bit Cipher Block Chaining (CBC) specified in ISO/IEC 10116.

4.17 **7** 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. A key management system shall be provided next to or

preferably as part of the OVDS. It shall automatically generate, store, distribute over the data network, synchronise and destroy keys securely. It shall be as transparent to users as possible.

4.18 The keys to be used in the roadside sites shall be sent over the network protected by a method known as triple encryption. Triple encryption uses DES and two 56 bit keys of its own to encrypt the keys to be transmitted. The keys to be sent are first encrypted using one key, and this result "decrypted" using the second key. That result is then encrypted again with the first key. 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.

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

4.20 Where it is necessary to provide for manual data collection, then as much data as possible shall be stored in electronic form on a removable storage medium

4.21 Each site should 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.

5 OFFENCE VIEWING AND KEEPER ENQUIRIES

5.1 The images taken by the automatic enforcement equipment need to be viewed and checked to ensure they provide clear evidence of an offence and whether there are any extenuating circumstances. The pair of images are compared as a further secondary check on the measurements recorded. The number plate of the vehicle used in the offence is read and additional information giving the location, time and date and measured speed or time into red extracted from the image or read from a memory if stored electronically. To provide an additional check that the number plate has been correctly read, the make and colour of the vehicle is noted.

5.2 For each case, an enquiry is currently made on the PNC to obtain the name and address of the keeper of the vehicle and check that the colour and make of vehicle and registration number used are consistent with that record. Normally PNC enquiries are made on terminals connected to standard interfaces known as STIFF links. Where this is currently done PNC enquiries can be a significant constraint on the through put of cases. PNC approved software is available to provide a direct link into the PNC. For the proposed system it shall be possible to make PNC enquiries directly from the OVDS using an approved PNC connection without data being entered more than once. Future opportunities to make enquiries directly on the DVLA computer or through the standard CTO/FPO system may eventually change this requirement.

5.2 It is at this point a police officer makes a provisional decision on whether there is reliable evidence of an offence and what action will be taken .

5.3 For the proposed traffic enforcement system the whole of this operation should be undertaken at a single location next to the force CTO. To the users this should appear as

the main operation carried out on the Offence Viewing and Decision System. The OVDS is required to:

(a) receive and handle the communications for electronically collecting the evidential data from the enforcement equipment sites.

(b) manage and decode the data as necessary.

(c) provide a data base for the storage and retrieval of the evidential data.

(d) provide easy to use facilities for viewing the evidence and comparing image pairs.

(e) check the number plate entered by the operator using Automatic Number Plate Reading software. ANPR shall be used to prompt the operator to confirm their entry whenever a difference is found. The number plate ultimately accepted by the system will be that determined by the operator. The system shall provide for the updating of the number plate recognition algorithm.

(f) automatically handle keeper enquiries on the PNC and alert the operator when the vehicle make and colour are not consistent with the PNC record. Enter the keeper name and address into the data base.

(g) provide for any non routine cases to be flagged by the operator for further review by a designated police officer and retrieval of these cases on request.

(h) provide for electronic transfer of all the data necessary for processing the offence to the CTO computer system and receipt of electronic messages back from the CTO. CTO messages will be linked to the relevant case and the case marked for further review by the appropriate police officer.

(i) provide the option to generate hard copy.

(j) generate a unique OVDS case reference number based on current practice.

5.4 The system shall provide monitoring information that will enable the performance of the checking procedures to be assessed. In particular the system shall log the number of times the operator has been correctly and falsely prompted by the automatic number plate reading system and the colour/model PNC check. This will inform future decisions on extending the automation of the system.

6 IMAGE STORAGE AND ARCHIVING

6.1 The OVDS shall also include facilities for the storage and archiving of evidence in relation to cases which are being or have been processed by the CTO and FPO.

6.2 Facilities for the storage, retrieval, display and hard copy production of all the evidence associated with cases in process on request are required, in particular for proceeding with final summons.

6.3 Images from cases where the processing of the offence has been completed shall only be archived for the minimum time required by the CPS. Write Once Read Many times (WORM) technology is recommended for this purpose.

6.4 An efficient index for extracting images requested by the CTO using the OVDS reference information for the particular offence is required. The CTO shall be responsible for cross referencing between its own unique reference number and the OVDS reference number if they are different. The image shall be decompressed and then be available for use with the facilities for current cases.

7 PROCESSING OF OFFENCES

7.1 The processing of offences should be undertaken by the system used for processing fixed penalties. The work includes the issue of a Notice of Intention to Prosecute and Notice to Owner sent to the keeper within 14 days, followed up by a conditional offer fixed penalty or summons to the driver, endorsement of the driver's licence, collection of the penalty and prosecution in the courts where required.

7.2 The CTO shall process cases in accordance with the provisional decision of the police on how to proceed unless criteria specified by the police for referring cases back to them are met. They shall then refer them back using the electronic messaging facility with the OVDS.

POLICE SCIENTIFIC DEVELOPMENT BRANCH

Woodcock Hill, Sandridge, St. Albans, Hertfordshire AL4 9H0 Telephone: 01727 865051 Fax: 01727 816233

HOME OFFICE POLICE POLICY DIRECTORATE

HOME OFFICE REQUIREMENTS FOR THE PROTECTION OF DIGITAL EVIDENCE FROM TYPE APPROVED AUTOMATIC UNATTENDED TRAFFIC ENFORCEMENT DEVICES.

Dr S R Lewis HOSDB

12th October 2005

1 INTRODUCTION

1.1 Guidance to industry on requirement for automatic traffic enforcement systems was published by the former PSDB (Police Scientific Development Branch), now the HOSDB (Home Office Scientific Development Branch) in 1996(1). Section 4 described the data protection required for protecting digital evidence if operated as an automatic unattended device. The requirements for Home Office type approval are contained in Handbooks published by PSDB, now HOSDB. The requirement for data protection of the evidence is given as:

"For unattended equipment all digital data shall be stored with security codes generated using PSDB published standards for data protection."

The published standards are those referred to above. This document replaces those standards and describes a migration path for devices approved under the previous standards.

1.2 Requirements for the remote recording of digital evidence and remote control of Home Office type approved traffic enforcement devices was published by PSDB(2) in July 2002 and should be read in conjunction with this document.

1.3 The integrity and full acceptance of the evidence by the courts 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 courts. The following data protection is required for devices used for automatic unattended operation.

2 GENERAL REQUIREMENTS

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 in the courts. 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 offence data produced by all devices approved for automatic unattended use.

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.

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

(1) Authentication

(2) Encryption

(3) Error protection.

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 offence data. The MAC is a complex function of a 112 bit, a 128 bit or a 168 bit authentication key. The integrity of a received image and data is verified when re-computing its MAC using the same key produces the same answer.

2.5 Encryption transforms the image into unrecognisable random data. For the encryption, another 112 bit, 128bit or 168 bit encryption key, chosen to be different from the authentication key, shall be used.

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.

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:

1 Calculate the MAC of the whole image

2. Encrypt the image

3. Append the MAC to the encrypted image

4. Compute the CRC for each transmission segment

5. Transmit each segment

2.8 At the receiving end on the ERCU (or if a copy, the OVDS) (see (2)), the process which must be undertaken in the following order, shall be to:

1. Check each CRC and request re-transmission when necessary

2. Decrypt the image

3. Recalculate the MAC from the decrypted image

4. Compare this MAC with the transmitted MAC

5. Accept as valid data only if they are the same.

3. DATA PROTECTION STANDARDS

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

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. The Data Encryption Standard (DES) last specified in FIPS 46-3 was specified in reference 2. From the 1 January 2007, the Advanced Encryption Standard with a 128 bit key specified in FIPS 197 shall be used in all new systems. Existing systems approved using the DES shall be upgraded by the 1st January 2007 to 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 still 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 HOSDB.

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. The previous version of this publication required the process defined in ANSI X9.9 to be used. This corresponds to the RMAC used with DES and a MAC length of 32 bits. From the 1st January 2007 new systems shall use RMAC with AES 128 and a MAC length of 64 bits. Existing systems approved using DES and the process defined in ANSI X9.9 shall move to using RMAC with the AES-128, the 2TDEA or the 3TDEA block cipher on the 1st January 2007. 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 the 1st January 2010 systems still using 2TDEA shall move to using AES 128 or 3TDEA and generate a 64 bit MAC, the 3TDEA systems using a 64bit salt. Beyond the 1 January 2030 all systems will use RMAC with an AES 128 block cipher and generate an 80 bit MAC with a 16bit salt.

3.4 From the 1st January 2007, the encryption process in new systems shall use AES 128 in Cipher Block Chaining (CBC) mode as described in NIST Special Publication SP 800-38A. The previous version of this publication required the use of DES used in the CBC mode. Existing systems approved using DES in CBC mode shall move to using AES 128, 2TDEA or 3TDEA in the CBC mode by the 1st January 2007. On the 1st January 2010, systems still using 2TDEA shall move to using AES 128 or 3TDEA in CBC mode. Beyond 1st January 2030 all systems shall use AES 128 in CBC mode.

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. From the 1st January 2007 all new systems shall generate new encryption and authentication keys for each offence in the road-side equipment. A key management system shall be provided as part of the OVDS. 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.

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. From the 1st January 2007, new 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 may be acceptable if agreed with HOSDB.

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.

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.

(1) "Home Office and ACPO Traffic Outline requirements and specification for automated traffic enforcement systems" Publication No 3/96

(2) "Requirements for the Remote Recording from and Control of Unattended Home Office Type Approved Traffic Enforcement Devices"
Dr S R Lewis, PSDB 25th July 2002