NATIONAL RAIL & UNDERGROUND CLOSED CIRCUIT TELEVISION (CCTV) GUIDANCE DOCUMENT

Version Release – Final 30th November 2010

[Now subject of formal change request procedures – see Appendix 'Seven'

Contact Andy Odell at ATOC andy.odell@atoc.org]

The purpose of this document is to provide guidance regarding the functional, technical and operational requirements of CCTV systems in the railway environment. Note that the document is not a prescriptive standard and what is provided at any given location should be determined on the basis of a risk assessment at that location.

Issued by: National Rail CCTV Steering Group

Date: 30th November 2010

TABLE OF CONTENTS

1. FOREWORD

1.1. Over the last decade CCTV surveillance and the evidence obtained have become increasingly vital tools in the prevention, investigation and detection of crime and terrorism. We have seen significant reductions in crime on the railway and CCTV has played a key role in helping to achieve this outcome and in making the railway safer.

1.2. However, the terrorist attacks on London in July 2005 together with the Haymarket and Glasgow attacks in June 2007 led to an unprecedented demand for access to CCTV recordings as part of the subsequent police investigation. This served to highlight not only the problems inherent in dealing with a multiplicity of different railway CCTV systems but also the general inadequacy of existing systems to support evidential requirements in terms of the quantity, quality and ease and speed of access to recorded CCTV data.

1.3. Following the 2005 attacks a cross industry Group worked with the British Transport Police (BTP) to develop industry guidance on the installation and operation of CCTV. This led to a first issue of the National Railway and Underground CCTV Guidance.

1.4. The 2007 attacks indicated that lessons had not been adequately learned and that more work needed to be undertaken. A national debate sponsored by the Association of Chief Police Officers (ACPO) and Home Office led to work addressing the standards, operation and interoperability of all CCTV. The BTP, as part of its contribution to the national initiative, engaged with the railway community resulting in the setting up of a Railway Industry CCTV Steering Group and a number of industry working groups.

1.5. This Guidance document is the output from the industry working groups. It is intended to build on the earlier work but to give it new impetus and prominence. It is produced with the intention of giving sound practical advice to the operators and users of rail CCTV, to help ensure we learn from our past experiences and that we make the best possible use of our investment in CCTV.

1.6. The guidance is quite deliberately not a standard or a mandate and does not seek to specify exactly what equipment we should use, but rather it sets out an aspiration of where we would like to see CCTV in the rail industry progress. We do not expect the industry to embark on extensive gap analysis work or to incur additional cost, but simply to move towards the best practice guidance contained in this document. Indeed we hope that the document will be organic and evolve as technology and our operating experience advance.

1.7. We hope that you will find the advice sensible and recognise that following the guidance has positive benefits for everyone in that it will ensure we continue to make the railway safer for everyone and maximise the value of our CCTV.

Signed on behalf of:

Andy Pitt, Chairman, Operations Council, Association of Train Operating Companies

ATOC
Association of Train Operating Companies

Paul Crowther, Deputy Chief Constable, British Transport Police

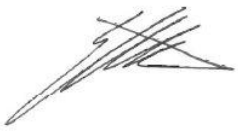
British Transport Police

Robin Gisby, Director Operations & Customer Services, Network Rail

Network Rail

Steve Burton, Director of Community Safety, Enforcement and Policing, Transport for London

Transport for London



2. ABBREVIATIONS

2.1. The following abbreviations appear in this guidance:

ACPO	Association of Chief Police Officers for England, Wales and Northern Ireland
ANPR	Automatic Number Plate Recognition
ATOC	Association of Train Operating Companies
bmp	Bit Map
BSI	British Standards Institute
BTP	British Transport Police
CCTV	Closed Circuit Television
CPNI	Centre for the Protection of National Infrastructure
DfT	Department for Transport
DOO	Driver Only Operation
DVD	Digital Versatile Disk
DVR	Digital Video Recorder
EU	European Union
FTN	Network Rail Fixed Telecom Network
fps	Frames Per Second
HDD	Hard Disk Drive
HMSO	Her Majesty's Stationary Office
HOSDB	Home Office Scientific Development Branch (ex PSDB)
ICC	Integrated Control Centre
ICO	Information Commissioner's Office
ipspc	Images Per Second Per Camera
MPS	Metropolitan Police Service
NR	Network Rail
PSDB	Police Scientific Development Branch
PTZ	Pan Tilt and Zoom
Rotakin	Test target used to measure system quality performance
RAID	Redundant Array of Independent Disks.
RSSB	Rail Safety & Standards Board
SO15	Metropolitan Police Service Counter Terrorist Command

SVHS	Super Video Home System
TOCs	Train Operating Companies
TRANSEC	Transport Security and Contingencies Directorate within the DfT
TfL	Transport For London which includes London Underground (LU), Docklands Light Railway (DLR), London Overground (LO) and Tramlink

3. SCOPE AND STRUCTURE OF DOCUMENT

3.1. This document provides practical guidelines for the selection, specification, operation and use of digital CCTV systems that not only support staff in the effective running and management of their stations, trains and managed car parks but also enhance both the safety and security of the public and staff using the facilities.

3.2. This document supersedes all previous versions.

3.3. Cameras related to security of non-public areas and requirements for other elements of infrastructure e.g. level crossings, are not included in this document. These may be the subject of further documents in due course.

3.4. Also, requirements in respect of Driver Only Operation (DOO) are outside the scope of this document.

3.5. Within the context of this document every consideration has been given to each organisation's obligation[1] under Section 17 of the 1998 Crime and Disorder Act in that:-

"*Without prejudice to any other obligation imposed upon it...exercise its functions with due regard to ...the need to do all it reasonably can to prevent crime and disorder in its area"*

3.6. This guidance document will help operators comply with their legal obligations under the Data Protection Act.

4. INTRODUCTION AND BACKGROUND

4.1. Station, train and station car park based CCTV has been widely deployed by Network Rail (NR), Transport for London (TfL) and the Train Operating Companies (TOCs) as a means of protecting the safety and security of the public and staff; as an aid to police investigations; and as a tool to assist in the general management of the railway environment. CCTV is at the core of the Department of Transport (DfT) / BTP Secure Station Scheme in that it demonstrates that the station operator has taken steps to prevent crime and enhance passenger safety.

4.2. However, given the structure of the industry post-privatisation and the absence of any prescribed national rail and underground industry standards it is inevitable that station, on train and car park based CCTV is characterised by a variety of standalone systems with little or no consistency or compatibility between them.

4.3. The rapid progress of technical developments such as a move from analogue to digital, IP Transmission networks, etc. along with changes to overground TOC franchises,

[1] The Act applies to the police, Local Authorities and TfL. It does not apply to Network Rail or Train Operating Companies

have often meant that such inconsistencies are apparent not just between different station and car park operators but also internally within an individual operator between systems used at different groups of stations or on different classes of rolling stock operated.

4.4. The terrorist attacks on London in July 2005 together with the Haymarket and Glasgow attacks in June 2007 led to an unprecedented demand for access to CCTV recordings as part of the subsequent police investigation. This served to highlight not only the problems inherent in such inconsistencies but also the general inadequacy of existing systems to support such requirements in terms of the quantity, quality and ease and speed of access of recorded CCTV data.

4.5. It is to address these issues and the relevant recommendations of the ACPO/Home Office National CCTV Strategy 2007 that the National Rail CCTV Industry Working Group, comprising representatives from NR, TOCs and TfL in conjunction with the Metropolitan Police Service (SO15), BTP and DfT, has produced this CCTV guidance document to define guidelines for CCTV security systems at all national rail and underground stations, on trains and at managed car parks within Great Britain. The oversight of the rail industry's response to the National CCTV Strategy is driven by the National Rail CCTV Steering Group.

4.6. By following the guidance in this document all national rail and underground station, train and station car park operating companies should move towards achieving a safer and more secure operating environment for both their customers and staff.

4.7. It is envisaged that each station, train and/or station car park operator will produce its own in-house standards using this document as a reference, which will contain full technical and operational specifications specific to its own operational needs.

5. PURPOSE OF CCTV

5.1. CCTV at national rail and underground stations, on trains and at car parks is usefully deployed for a wide variety of collective purposes. These can be broadly grouped as follows but not limited to:

- To deter and prevent crime/terrorist activity
- To detect crime/terrorist activity
- To assist the emergency services
- To investigate crime/terrorist activity
- To investigate staff, public and rail related accidents and incidents
- To provide evidence in criminal and civil proceedings
- To reassure and give confidence to the public and staff
- To meet all statutory requirements and obligations
- To monitor and manage passenger flows
- Crowd control

- Vehicle control[2]
- To aid decisions on train movements, particularly following disruption including contingency management following terrorist activity

5.2. In the vast majority of cases, a station, on train or car park based CCTV system will be intended to address most, if not all, of the above.

6. SPECIFICATION AND SELECTION

Introduction

6.1. This section is based on the Home Office Scientific Development Branch (HOSDB) and Association of Chief Police Officers for England & Wales (ACPO) guidance HOSDB CCTV Operational Requirements Manual 2009 Publication No. 28/09 and the BTP publication "Output requirements from CCTV systems on stations, car parks and trains" v1 dated April 2009. These documents should be read in conjunction with this guidance.

6.2. All data protection and Information Commissioner's Office (ICO) requirements must be adhered to when planning for the recording CCTV images and HOSDB guidance should be considered. The requirements cover all CCTV systems whether they are deployed at a station, car park or on train.

6.3. This document is an aid to meeting the technical specification of a CCTV system based on the operational requirement. The guidance does not specify any one manufacturers' equipment or product. In addition to the system providers, BTP Crime Reduction Officers and specialist BTP CCTV staff can provide free advice and guidance to operators and support their efforts towards achieving Safer Station and Car Park accreditation.

6.4. Before planning, procuring or enhancing the CCTV system a clear understanding should be reached of what the system is required to do and how it should perform. This information should be captured in an operational user requirements document that is generated by interviewing all the stakeholders that propose to use the station, on train or station car park CCTV system. A schematic on how to prepare a CCTV operational requirement specification is provided within HOSDB Publication No. 28/09 mentioned above.

6.5. To realise the maximum benefits of the CCTV systems it is strongly recommended that new installations should be developed with an open protocol technology to allow an interface with other pertinent systems, e.g. links between the system to be installed and those belonging to TfL, NWR, TOCs and local authorities, etc.

6.6. At the time of designing a new or modified CCTV system consideration should be given to the fact there is an aspiration within BTP (subject to further assessment of the costs and benefits) to monitor live images and export recorded images from a remote location such as a BTP facility, a 3rd party control centre or the appropriate ICCs for operational purposes.

[2] Please note that not all operators will use CCTV for vehicle control.

Lighting

6.7. The appropriate British and European Union Standards should be used as guidance to lighting requirements when used in conjunction with CCTV systems[3].

Considerations for on train CCTV systems

6.8. The generic HOSDB document does not specifically cover on train CCTV systems so additional guidance is provided below.

6.9. This guidance does not however cover on train forward or rear facing cameras[4]. A separate document has been produced by the Rail Safety & Standards Board (RSSB) June 2010 (GM/GN2606 Guidance on the Fitment and Functionality of Forward and Rear Facing Cameras on Rolling Stock). For further information about this guidance please contact enquirydesk@rssb.co.uk at RSSB.

6.10. Special consideration should be given to areas of a train that will benefit from surveillance such as doors, vestibule areas, passenger communication devices, luggage racks, disabled facilities and the exit from toilets.

6.11. When specifying an on board CCTV system care should be taken to ensure that the design can cope with the varying light conditions that are inherent to a moving train e.g. going through tunnels and cuttings. If very low emergency light levels can be accommodated in the design this would be useful.

6.12. Viewing screens (if fitted[5]) should be located on trains at positions from which a conductor/guard might be expected to operate doors or provide passenger services.

6.13. Recording equipment should be located in secure locations.

6.14. In the event of an activation of a passenger communication device or emergency door release the guard/conductor[6] should be made aware of the location of the activation by the system. The system should also enable them to view the area at the location of the activation of the passenger communication device / emergency door.

6.15. The system should allow for a member of train crew, from a panel on the train (if provided), to select individual cameras or to scroll automatically through all camera locations on the train and to view live camera images.

6.16. The system should provide an indication to a train control and management system (where fitted) when there is a fault with the system. Faults may be assigned as minor or major.

6.17. The system should be linked to the fire detection system (if fitted), so that in the event of fire detection images from the location of the detection are available in the driving and rear cabs.

6.18. Consideration should be given to the provision of base stations that provide all the functionality that would be features of a station or car park system.

[3] Please refer to BS 5489 part 9 and possibly BS5013.
[4] Please note that not all operators will install forward facing cameras.
[5] Not all operators will have this facility as some trains are operated by one person only.
[6] Not all trains will have a guard/conductor present.

Automatic Number Plate Recognition (ANPR)

6.19. ANPR is not covered in HOSDB documentation and is not in use by all operators. A standard ANPR system installed at a car park allows users to track, identify and monitor moving vehicles for security and safety. The fact that ANPR is mentioned in this guidance does not in any way infer that it should be installed at car parks and controlled areas managed by operators.

6.20. An ANPR system should have as a minimum the capability to store a large volume of vehicle registration numbers and be able to, as a minimum:

- automatically open barriers for known vehicles;
- measure car park stay times;
- identify stolen vehicles; and
- provide statistical reports.

6.21. Each ANPR system should have as a minimum three key elements to provide a fully operational system, namely, Capture, Process and Display.

6.22. **CAPTURE** comprises an ANPR camera that is used to view vehicle number plates and is capable of operating in all weather conditions and when vehicle headlights are pointing towards the camera. Cameras should be mounted at a suitable location to capture a vehicle's number plate as it enters and leaves the car park or controlled area. Where no barrier is fitted the camera should be capable of capturing number plate images at speeds up to 40 MPH.

6.23. If appropriate, and if a security risk assessment deems it a requirement, additional cameras viewing and recording vehicle details such as colour, make, occupants, along with the captured number plate image can be installed at key locations.

6.24. **PROCESS** comprises a computer with a database and pre-installed management software that processes the images from the cameras and then runs an individually pre-configured application. Typically, the system could display messages, operate barriers, check the amount of money available on a pre-paid ticket, etc.

6.25. It is envisaged that the ANPR system processor will be linked via a secure communication link to the DVLA and/or police national computer. Clear operating protocols will have to be defined with all stakeholders when the equipment is installed.

6.26. **DISPLAY** comprises a displayed message on a monitor in the control room should any pre-set condition be breached or the vehicle is identified as stolen or of interest depending on the application. Staff monitoring the car park entrance and exit points should be trained to the appropriate standard to enable them to deal with any situation relating to car parks that they may encounter.

7. RECORDING

Stations and Car Parks CCTV Systems

7.1. Table One below (Station View and Coverage) expresses:

- The desired percentage of floor coverage. This is relevant to areas which have defined floor space such as booking halls, concourses and platforms. It is

recommended that any single "blind spot" should be restricted to an area no greater than 2m high and by 4 m square of floor space. Discussion with the local Crime Reduction Officer will assist in meeting this requirement.

- The quality of image required to support whichever of the four categories of Detect, Observe, Recognise and Identify is specified.
- The desired ipspc (image per second per camera) a camera records at. This is key to producing the desired output.

7.2. Table One below is based on using fixed cameras and the ipspc should be seen as a minimum standard going forward and there is no intention for it to be applied retrospectively. Some Pan Tilt and Zoom (PTZ) cameras may be deployed to augment fixed cameras where there is pro-active monitoring.

TABLE ONE - STATION VIEW AND COVERAGE

Relevant Area of Station	% of Floor Coverage	Image Quality	Images per second per camera (IPSPC)
At risk office doors	n/a	Identify/Recognise	High
Booking / revenue office windows	n/a	Recognise	Medium
Booking hall overview	95	Detect	Medium
Boundary walls / approach roads	90	Detect	Medium
Car Park	95	Detect	Medium/Low
Car Park Entrances & Exits	100	Recognise/Identify	High
Cycle racks, bins & bulk waste containers	100	Recognise	Medium
Left luggage / lost property entrance	n/a	Identify/Recognise	High
Left luggage / lost property overview	95	Detect/Recognise	Medium
Passenger assistance / alarm points	n/a	Recognise	Medium
Platforms overview	90	Detect	Medium/Low
Post boxes	n/a	Recognise	Medium
Public toilet entrances	n/a	Recognise	Medium
Station entrances / exits	n/a	Identify	High
Station frontage / forecourt	95	Detect	Medium
Station over-bridges / stairs / escalators / lifts	100	Recognise/Detect	Medium
Station piazza / concourse overviews	95	Detect	Medium
Station subways / underpasses	100	Recognise	Medium
Taxi ranks	95	Detect/Observe	Medium
Telephone kiosks	n/a	Recognise	Medium

Relevant Area of Station	% of Floor Coverage	Image Quality	Images per second per camera (IPSPC)
Ticket barriers – both sides	n/a	Identify	Medium
Ticket machines / ATMs	n/a	Recognise	Medium
Travel information bureaux overview	95	Detect	Medium
Waiting rooms / shelters	95	Recognise	Medium

Key: High means 8 ipspc and above, Medium means 5 to 7 ipspc and Low means below 5 ipspc.

On Train CCTV Systems

7.3. Table Two below (On Train View and Coverage) is based on using fixed cameras and the ipspc should be seen as a minimum standard going forward and there is no intention for it to be applied retrospectively.

7.4. For on train systems the cameras should minimize the view of the windows and exterior of the train where possible to prevent fast changing scene and light conditions and be located in such a way that each camera is viewed by at least one other.

7.5. The system should ideally be capable of recording for no less than 10 days at the minimum ipspc and image quality relevant to the deployment as shown below.

TABLE TWO - ON TRAIN VIEW AND COVERAGE

Relevant Area of Train	% of Floor Coverage	Image Quality	Images per second per camera (IPSPC)	Target
Carriage entrances and exits	n/a	Identify	High	To capture ID quality images of subjects entering or exiting a carriage.
Carriage seating areas and walkways	n/a	Observe	Medium	To give an overview of activity taking place in these areas.
Train vending counter area	95	Recognise	Medium	To capture activity in this area and recognise a subject at the counter.
Internal cab doors	n/a	Recognise	Medium	To recognise a subject entering or leaving one of these areas.
Toilet doors	n/a	Recognise	Medium	To recognise a subject entering or leaving one of these areas.

Key: High means 8 ipspc and above, Medium means 5 to 7 ipspc and Low means below 5 ipspc.

7.6. In order to allow for the download of large amounts of data, easily accessible removable caddies should be used to enable the entire storage device to be removed quickly and replaced if required without the need for technical expertise.

7.7. An example of the optimum camera positions and fields of view is shown as Appendix 'One'. It is important for the protection of cameras that each camera is within the field of view of another camera.

8. PLAYBACK /VIEWING

Station and Car Parks

8.1. The playback software should:

- have variable speed control, including fast forward and rewind and frame by frame forward and reverse viewing.
- display single and multiple cameras and maintain aspect ratio.
- permit the recording from each camera to be searched by time and date.
- allow printing and/or saving (e.g. .bmp) of individual pictures with time and date.

8.2. It should be possible for operators/authorised persons to playback recorded images from any camera at a station and/or car park based system on the station's and/or car park's own playback facility.

8.3. When playing back images it is essential that the information displayed on the recorded image, such as time, date and camera detail, is identical to that pertaining at the instant of recording the original live image. It is recommended that the time and date signals are generated by a common time source (Atomic Clock) to ensure synchronisation throughout the CCTV system.

On Train Systems

8.4. The system should[7]:

- support viewing of all recorded images on a train or unit via a single diagnostic port (location of port to be agreed) using a laptop computer or other device – preferably Microsoft Windows driven;
- enable the simultaneous viewing of not less than 4 cameras, selected by the operator, from the single diagnostic port on the train.

9. DATA EXPORT AND DATA SEIZURE

9.1. For the purpose of this document DATA EXPORT means the removal of data from the recorder to another device and DATA SEIZURE means the removal of the recording device (unit or complete drive) itself from its normal location.

9.2. The data export system should allow exporting of images to suitable digital storage media e.g. DVD, external HDD, etc. All propriety software required for playback should also be exported onto the storage media by default. Export of a system event log or audit trail should be available along with the pictures to help establish the integrity of the images and system.

[7] Please note that not all operator systems will have an on train reply facility.

9.3. Should a system not export the proprietary software with the images then the supplier of the system should make available to Police, free of charge, any application required to view the images.

9.4. The replay software should allow the investigator to search the pictures quickly, effectively and see all the information contained in the picture and associated with it.

9.5. Consideration should be given to the need for the authorities to seize the recording equipment or elements of it, such as the HDD.

9.6. To ensure a station remains fully operational from a CCTV monitoring and recording perspective should a large and significant seizure occur, it is strongly recommended that the station operator and BTP should undertake a joint security risk assessment for all security designated Category A & B stations. The security risk assessment should cover but not be limited to:-

- The risk of a mass data request being made which affects some/all of the stations managed by the operator at the same time.
- The CCTV system configuration.
- Networking.
- Data access arrangements for BTP (or security services).
- Spares holding supply chain and availability (either held by operator or supplier/maintainer).

9.7. The recommended spares held by the operator or their supplier will be determined by the outcome of the security risk assessments.

10. DOWNLOADING PROCESSES

10.1. This Section describes the ideal processes for downloading (also termed exporting) CCTV images for routine enquiries and major incidents.

10.2. Appropriate processes and procedures[8] should be in place to ensure that the routine download and download for major incidents are fully understood by all staff. System owners should put in place arrangements with the police so that images may be routinely exported in a timely fashion.

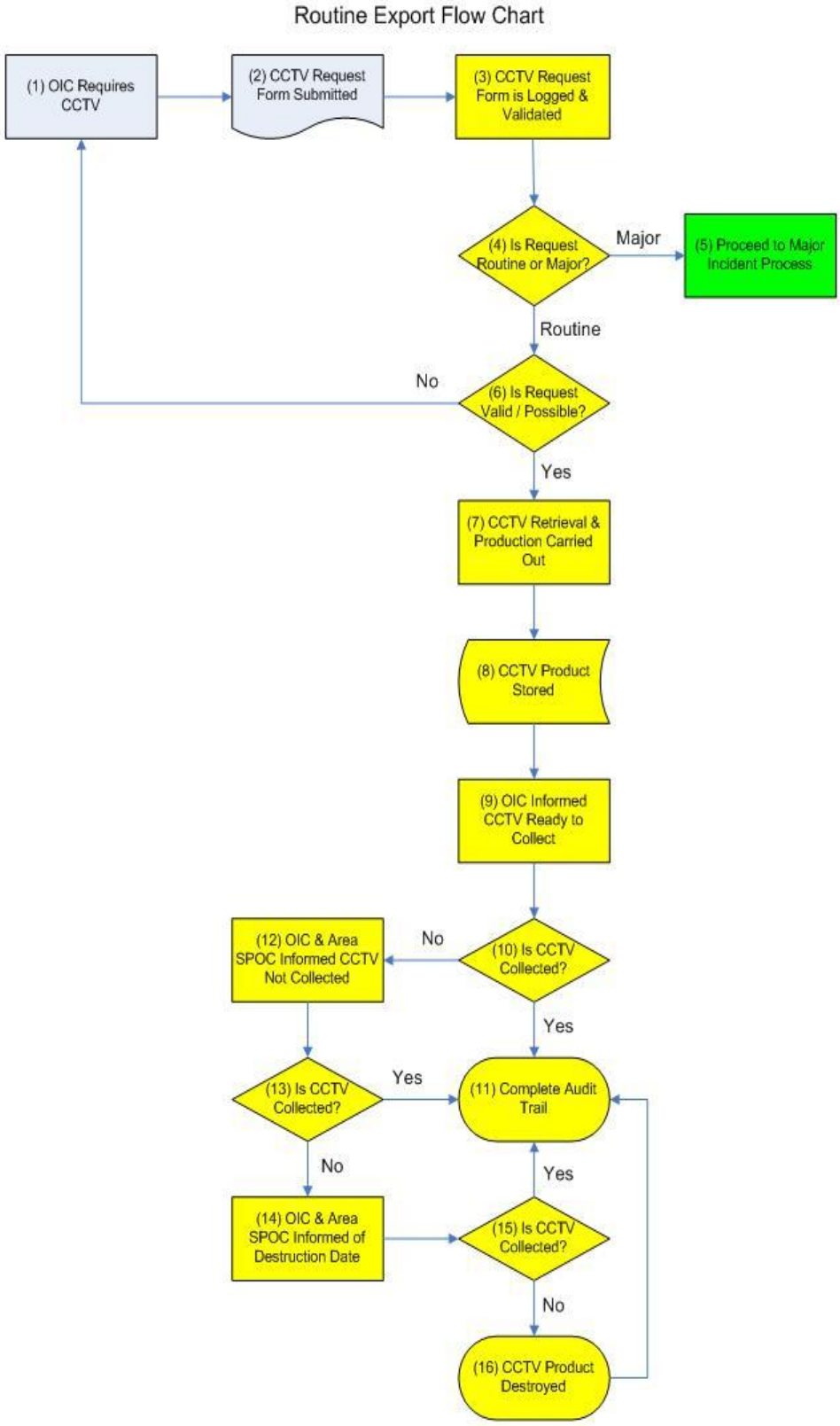
10.3. A key issue for operators is that the requirement to undertake downloads, in the absence of dedicated data profilers, may take staff away from their primary function e.g. the knock on effect on station and/or control room staff.

Routine Downloads

10.4. The flow chart (see Figure One below) outlines the process for exporting CCTV images for routine enquiries; there is a separate process for major incidents. An explanation of each of the boxes (box numbers are shown in brackets) is provided below.

[8] This includes the training and competency of staff.

Figure One – Generic Routine Export Process



10.5. **(1)** CCTV requests may come from a variety of sources such as rail operators themselves (for accidents, incidents or internal discipline enquiries), subject access requests (under DPA) or police forces. The flow chart shows how a request from a British Transport Police Officer may be processed but is easily transferrable to any other person requesting CCTV. The term OIC stands for "Officer in the Case" and is generally who requests CCTV for an incident.

10.6. **(2)** A standard method of requesting data is desirable; email is a good method as it provides its own audit trail for both parties. It should be noted that at times Police Officers might have to make requests verbally over the phone in which case the person receiving the request for CCTV should complete the request form. CCTV Operators should set up a central point where CCTV requests are to be sent (typically control rooms).

10.7. A standard CCTV request form (an example is given at Appendix 'Two') is also advantageous as it provides a standard set of information around which audit trails can be designed and ensures the correct data is retrieved. Information from the request forms can be stored in simple spreadsheet or more complicated database.

10.8. **(3)** When processing CCTV requests thought should be given as to how they will be logged and validated i.e. is the person requesting the data authorised to have it, is the data requested available, is the request reasonable and lawful etc. A method of confirmation and of notifying acceptance or rejection of the request back to its source should be put in place and an audit trail started for each request.

10.9. Each request form received should be awarded a Unique Reference Number (URN). Should the request be valid then this URN should be marked on any disk or tape produced to link the two items. If the request form is rejected for any reason then this should be stated on the form under the "Official (CCTV Staff) Use Only" section in the "Additional Information" box.

10.10. **(4)** DECISION - Is the CCTV request routine (normal daily business) or major (large amount of data required for a major incident / investigation)? This is a decision informed by a CCTV operator's ability to deliver the amount of data required within the required timescales. If **routine** – go to box number 6. If **major** – go to box number 5 - follow the Major Incident Export Process (see below).

10.11. **(5)** Refer to the Mass Export Process for dealing with CCTV requests for large amounts of data to support major incidents / investigations.

10.12. **(6)** DECISION - Is the CCTV request valid / possible? If **yes** – then receipt of the request should be given to the OIC and the data retrieved and produced. Go to box number 7. If **no** – return request to the OIC with details of why the request is not possible. This should still be logged as a request for audit purposes. Go back to box number 1.

10.13. **(7)** CCTV retrieval / production can at times be a complicated technical process. This document only describes the "standard" retrieval / production process i.e. systems set up to export their data via a CD / DVD drive or tape systems where the disk or tape can simply be removed from the recorder.

10.14. Upon receipt of a valid CCTV request the required images should be produced as a "Master Copy". This Master Copy should be capable of being viewed immediately by means of a standard Microsoft Operating System without a software installation

having to take place first (i.e. playback software should be capable of running from the disk or tape containing the images).

10.15. Pictures should be exported in their native file format i.e. the format that they were originally recorded in on the CCTV system. All images should be time date stamped and contain the relevant camera text such as name / location or number.

10.16. With video cassette tapes the master copy will be the original tape, in the case of digital recordings the master copy will be the first cloned copy (on WORM media – **W**rite **O**nce **R**ead **M**any) defined as the master. If a second copy (Working Copy) of digital recordings can be produced then this is highly desirable.

10.17. All CCTV evidence produced should contain a Unique Reference Number (URN) to identify each item (see 10.8 above), as well as being marked with an exhibit number. Typically a master (or working) copy should be marked as such and be sealed in an evidence bag, accompanied by an MG11 witness statement (completed by the person producing the evidence – please see Appendix 'Three'). If the evidence changes hands then the continuity section of the evidence bag should be completed along with a continuity statement.

10.18. Should the retrieval and production processes be carried out by two different people then two separate MG11 Witness Statements should be completed; one MG11 for the initial removal of the data from the system and one for the production of the evidential Master Copy disk. Examples of this would be:

(i) if hard drives are removed from a train by one person, then disks produced from these drives by another person; or

(ii) if data is downloaded from a system on to an external hard drive by one person, and then later transferred to evidential Master Copy disk by another person.

10.19. An example MG11 covering the retrieval or collection of CCTV is shown at Appendix 'Four'. An example MG11 for staff handling or processing CCTV is shown at Appendix 'Five'.

10.20. It is entirely possible that unusual circumstances will arise when the above example MG11s will not be appropriate. Should this prove to be the case then a normal MG11 should be used.

10.21. **(8)** CCTV media of evidential value should be stored securely with a full audit trail kept of any movement. Brief guidelines for storage of both magnetic and optical media are given below[9]:

<u>Optical Media (CDs / DVDs)</u>

10.22. Disks should be stored in a "jewel" case. The recording layer in optical disks can be damaged by light, heat, moisture and a combination of these. Prolonged exposure to moisture allows water to become absorbed into the disk where it may react with the disk components causing failure. Disks should be stored in a dark environment to reduce the risk from light fading.

[9] Further details on storage can be obtained from British Transport Police.

Magnetic Media (Tapes / Hard Drives)

10.23. Magnetic media can be prone to shock due to the mechanical parts within hard drives. Therefore extra care should be taken to prevent damage. Consideration should be given to providing extra padding during transportation.

10.24. Magnetic fields are a concern for magnetic media use and storage. External magnetic fields are most frequently observed near motors and transformers. A separation of a few metres from the source will usually provide sufficient protection. External fields of a more unanticipated nature may be produced by some headphones and microphones or by cabinet latches and magnetised tools.

10.25. **(9)** Upon completion of the CCTV processing the OIC should be informed that the data is ready to collect along with the location, job reference and opening times of the collection point. A timescale for retention of the data should also be given. Best practice would be to agree these timescales corporately with British Transport Police and therefore build them into any process or system.

10.26. **(10)** DECISION - Is CCTV collected (within the agreed timescale)? If **yes** – go to box number 11. If **no** – go to box number 12.

10.27. **(11)** The audit trail should be completed by recording the details of the transaction (time, date, whom released to / by or destroyed by etc) for continuity of evidence and Data Protection Act (DPA) purposes.

10.28. **(12)** The OIC and (by way of escalation) the relevant Area DCI or Single Point of Contact (SPOC) should be informed that the data still awaits collection. BTP area SPOCs will be set up to manage the non-collection of CCTV.

10.29. **(13)** DECISION - Is CCTV collected (within the agreed timescale)? If **yes** – go to box number 11. If **no** – go to box number 14.

10.30. **(14)** The OIC and area SPOC should be informed that a date has been set for destruction of the data due to the non-collection within agreed timescales.

10.31. **(15)** DECISION - Is CCTV collected (before the date set for destruction)? If **yes** – go to box number 11. If **no** – go to box number 16. Operators have different policies over how long they will retain CCTV images which are not collected; for some this is as little as one month. CCTV requesters should make sure that they are aware of the policy of the operator holding the image(s).

10.32. **(16)** CCTV data should be securely destroyed. Go to box 11.

Major Incident Downloads

Definition

10.33. CCTV system operators can normally deal with "routine" requests for data as part of their daily business. There is no common definition for what is a major incident download. There are however factors that would make a download request deemed to be major as opposed to routine and these are:

- The volume of data that is being requested
- The time frame within which that the data requester would like it to be produced
- The logistics around getting access to the data that may be spread across a large geographic area

- The technical infrastructure in place that could enable immediate live viewing as an alternative to a download
- The availability of TOC staff (or other contractors) who would undertake the downloading
- The operational impact of the incident on the operator who is to provide the data

10.34. Depending on individual circumstances it will be up to each operator, in conjunction with the BTP, to determine if a CCTV data request is to be treated as routine or major.

Introduction

10.35. As a result of the London July 2005 and the June 2007 Haymarket / Glasgow terrorist attacks, the rail industry was faced with requests to Mass Export data from its CCTV systems, in some cases from all cameras up to 31 days of recording. Lessons learned from such events and more recent incidents, have highlighted a need for both procedural and technical measures to be put in place by the Security Service, British Transport Police (BTP) and Rail CCTV Operators, in order that any future incidents of this nature can be more efficiently dealt with.

10.36. BTP will endeavour to ensure that major incident CCTV recovery is done in a focussed manner, intelligence led where possible. This approach should lead to more targeted requests being made for CCTV images. It should be acknowledged however that when intelligence is not available following a major incident then large requests for CCTV images may still be necessary.

10.37. It is recommended that all rail operators work with BTP to produce their own internal Major Incident download procedures. An offer of BTP assistance to develop these procedures was set out in a letter from the Deputy Chief Constable to TOCs in April 2010. These procedures should align with the guidance process and procedures contained within this document to effectively deliver a combined (common) process that can be carried out following a major incident. The current BTP procedure and a draft process flow have been included to aid this process.

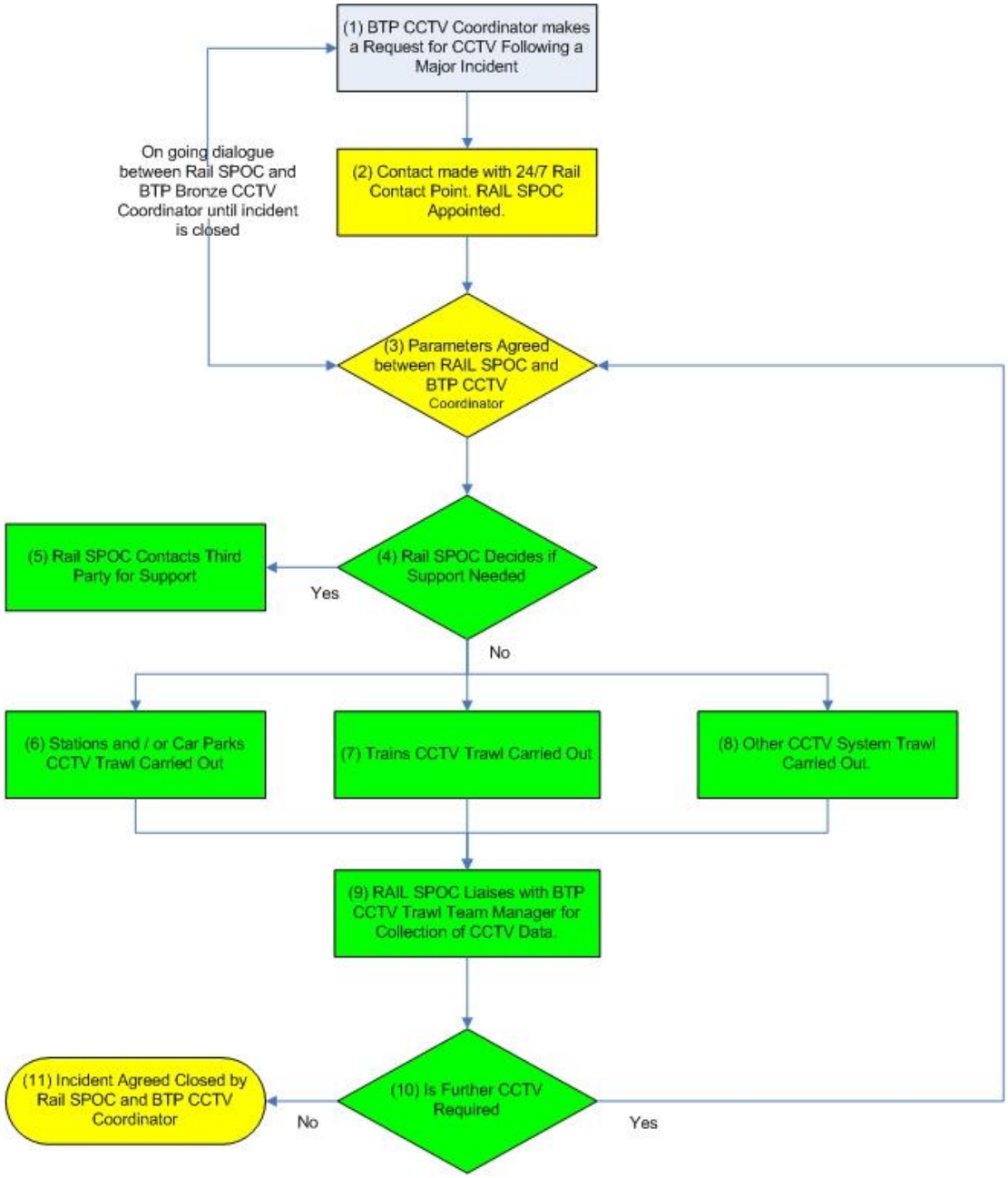
Major Incident Procedural Measures

10.38. Once rail operators have developed their own Major Incident procedures, this should lessen the impact on CCTV system owners and improve the effectiveness of the police investigation. This process will require effective communication and cooperation between all parties, BTP will need to ensure that all CCTV requests are absolutely necessary and that all efforts have been made (via the Senior Investigating Officer) to rationalise the request through viewing the required images where possible, therefore minimising the extraction process

Rail Company Process Map

10.39. To aid rail operators in developing their own internal process for a Major Incident download a draft template detailing the basic high level process flow is included below (see Figure Two). BTP will work with any rail operator to support the development of their own Major Incident download procedures.

Figure Two – Generic Routine Export Process



Role Definitions

BTP CCTV Coordinator

10.40. The role of BTP CCTV Coordinator is to liaise with the Senior Investigating Officer to agree the CCTV trawl parameters, liaise with the Rail SPOC to ascertain whether or not the parameters are realistic (and review them if needed), and to ensure that Area CCTV Trawl Team Managers are appropriately briefed as to what their specific trawl area responsibilities are.

24/7 Rail Contact Point

10.41. Rail companies should determine where their 24/7 point of contact is for Police in order for communications to be directed there in the first instance. This would normally be the TOC control room.

Rail SPOC (Single Point of Contact)

10.42. The Rail SPOC will have their own internal process to follow during a Major CCTV Trawl, however, the interface between them and the BTP CCTV Coordinator is key to the success of the trawl. They will be responsible for agreeing the parameters with BTP CCTV Coordinator and also working with the (Police) Area CCTV Trawl Team Managers to ensure the required data is produced and collected in a timely fashion.

Area CCTV Trawl Team Manager

10.43. BTP will appoint an Area CCTV Trawl Team Manager to manage the Police teams collecting CCTV for the investigation. They will be responsible for liaison at ground level to ensure all data requested is collected paying particular attention to evidential integrity.

Processes / Decisions (Box #)

10.44. **(1)** British Transport Police (BTP) will appoint a BTP CCTV Coordinator to manage all Major CCTV Trawls from a Police perspective. This person will liaise with the rail companies (CCTV system owners) and the BTP CCTV Trawl Teams. This person will make the initial request for CCTV to the 24/7 Rail Contact Point.

10.45. **(2)** Initial Police contact will be made with the designated 24/7 Rail Contact Point by the BTP CCTV Coordinator, who will expect to be given a Single Point of Contact to deal with going forward. At this stage the Rail SPOC should be determined as one individual to aid clear communication lines. Although the Rail SPOC may change should a Major CCTV Trawl last for an extended period of time, it should only be one person at any one time acting as the SPOC.

10.46. **(3)** The Rail SPOC and BTP CCTV Coordinator should agree the trawl parameters at this stage, this included locations where CCTV is required from, the time periods required, the urgency of the request and any priority areas.

10.47. **(4)** The Rail SPOC should consider at this stage how they will resource the provision of CCTV data to the Police. If third party support is required go to box 5, if not, then proceed to boxes 6, 7 and 8.

10.48. **(5)** Should third party support be required i.e. regular CCTV staff are either not available of cannot provide the required resource, the Rail SPOC should make contact with their support company to enquire about extra resources to help with the trawl.

10.49. **(6, 7 & 8)** The Rail SPOC should coordinate the retrieval and production of CCTV data from the locations required, this could be from stations, trains, car parks or a combination of all.

10.50. (**9**) BTP will appoint an Area CCTV Trawl Team Manager for each rail company involved in the trawl. These Managers will make contact with the Rail SPOCs to agree collection locations for CCTV and manage the process of getting all CCTV requested collected and delivered to the required location to support the investigation.

10.51. **(10)** If further CCTV is required (and this is a dynamic process as the answer may change throughout the duration of an investigation) go to box 3, if not go to box 11.

10.52. **(11)** Once all CCTV required has been collected and delivered to support the investigation, the Rail SPOC and BTP CCTV Coordinator should formally agree the trawl is at an end and communicate this to the relevant parties within their own organisations.

Scenario Testing the New Mass Export Process

10.53. In order to test any new procedure a number of scenarios have been set out below. These scenarios may be compared against the proposed Mass Export process to help flush out any issues there may be with delivering each scenario. Any issues should be recorded and discussed with British Transport Police. Timescales for delivering each scenario should also be recorded by the rail company to help inform decision-making during a major investigation.

Scenario 1

10.54. A CCTV request to view historic footage of (potentially) all cameras from 10 (typical) stations on a line of route for a period of 2 hours. This review needs to take place immediately and there are five investigating officers available to view the data.

Scenario 2

10.55. A CCTV request for all pinch point cameras (doorways and barrier lines) from 10 (typical) stations on a line of route for a period of 2 hours. This data is required to be produced as evidential exhibits within 24 hours.

Scenario 3

10.56. A CCTV request for all cameras from 10 (typical) stations on a line of route for a period of 2 hours. This data is required to be produced as evidential exhibits within 72 hours.

Scenario 4

10.57. A CCTV request for all cameras from 10 (typical) stations on a line of route for a period of 48 hours. This data is required to be produced as evidential exhibits ASAP.

Scenario 5

10.58. A CCTV request for all cameras from 10 (typical) stations on a line of route for the entire retention period data is stored. This data is required to be produced as evidential exhibits ASAP (this may require removal of hard drives).

Scenario 6

10.59. A CCTV request to view all historic footage of all cameras from a specific train[10]. This review needs to take place immediately.

Scenario 7

10.60. A CCTV request for all cameras from all trains stopping[11] at one given station within a one-hour window. This data is required to be produced as evidential exhibits within 24 hours. This request could involve multiple operators and each operator is expected to provide data for their trains only.

Scenario 8

10.61. A CCTV request for all cameras from all trains that have arrived at or departed from a given station within a two-hour window. This data is required to be produced as evidential exhibits within 72 hours. Please note that this could involve multiple operators.

Mass Export Technical Measures

10.62. It is estimated that there are around forty different digital CCTV systems currently in use within the rail industry. Before technical solutions to Mass Export can be developed we need to better understand the systems that are in place. BTP is developing a CCTV asset database (on behalf of the Industry) to capture both the technical and contact information for each system. This database will be used to support effective mass export of CCTV data and provide a starting point from which to agree the best way forward and develop the necessary technical solutions.

10.63. The difficulty with differing digital systems revolves around the following:

1. Retrieval from differing systems requires specialist knowledge, equipment, and information from the system owner.
2. Replay of images is not always immediately possible due to proprietary formats of video used.
3. Retrieval of images from digital systems can be very labour intensive.

[10] Where there is more than one unit then train means all the combined units.
[11] This does not include non stopping trains.

10.64. The rail industry should ensure that any technical solutions developed are considered and addressed in any new designs, and wherever practical retrofit systems. At this stage there are a number of possible considerations, which may be capable of implementation straight away. These considerations are laid out in the next section of this document.

Possible Considerations – Stations

Consideration 1 Pinch Point cameras on first DVR

10.65. There are cameras throughout stations that are referred to as Pinch Point cameras that capture key areas of the station where people have to pass through e.g. entrances, gate-lines and platforms. All pinch point cameras are configured onto a single DVR (ideally DVR 1)

10.66. In a Mass Export the spares that the rail operator keeps could be used to replace this one DVR rather than expecting to replace an entire system. Again the rail operators (or another source) would potentially need to replace hard drives spares if required.

10.67. Cost would include the reconfiguration/design costs for each system, plus replacement of spares if removed.

Consideration 2 Mirrored hard drives for Pinch Point cameras

10.68. As above, based on the Pinch Point cameras, if these cameras were identified, per station, they could be recorded onto a single hard drive, which could be removed as requested. This would give BTP the main areas of the station which typically is what they require for major incidents.

10.69. Other cameras are typically for operational or crime and disorder purposes, not major incidents such as terrorist activities.

10.70. Initial discussions with manufacturers suggest that this solution is feasible. Rail operators would need to purchase replacements if removed but the replacements would be minimised by prioritising the required Camera views.

Consideration 3 Provide hard drive capacity for more than the main retention period

10.71. The hard drives could be replaced with larger storage capacity hard drives to allow the rail operators retention periods to be locked ensuring that it is not recorded over. This would allow a period of additional time to export the data without affecting the retention the agreed retention period.

10.72. As hard drive technology has progressed since the rail operators designed these systems, they are now able to install larger capacity hard drives into the same DVR's e.g. instead of 250GB drives, they can replace them with 500GB drives.

Consideration 4 Procure / call off appropriate spares

10.73. Provide appropriate number of spares for all hard drives, seeking cost efficiency through collaborative procurement arrangements.

Consideration 5 Export data over a Network

10.74. If a suitable network was provided, data could be accessed remotely and exported over the network. This would allow data to be exported to a remote location on demand.

10.75. A network of large storage drives would need to be provided for this option, however this option would also deliver additional benefits e.g. better incident managing as recorded data could be played back remotely on demand and live data could be provided to multiple control centres which could be essential for the Olympics.

Consideration 6 Data Warehouse / Backup

10.76. Off site central backup storage could be provided which would routinely back up data from each station to a central storage facility. Several companies already provide this service however the above Consideration 6) would also need to be implemented.

10.77. Data Warehouse should not be confused with central recording. Data Warehouse gives the opportunity to ring fence / view and retrieve data in a timely manner without affecting the original recordings.

10.78. Please note that none of the considerations outlined above are standalone solutions and they will require a combination of options to provide robust solutions to the Mass Export challenge.

Possible Considerations – Trains

Consideration 1 Rail operators procure / call off appropriate spares

10.79. Trains record for typically 72 hours only. Therefore data needs to be removed quickly to ensure the data is not recorded over. Due to space restrictions it is difficult to add additional equipment.

10.80. An appropriate level of spare hard drives is a simple solution to Mass Export. As rail operators currently have limited trains with digital recording systems, appropriate spares would not cost too much at this time.

10.81. Trained resources would also be required to export and replace the hard drives within the trains. It is likely that as more rolling stock has CCTV systems introduced, more data will be lost, as resources would be stretched to complete the exporting.

Consideration 2 Wireless downloading / remote network

10.82. This option would have a remote download function so that on entrance into the depot/siding the data on the train hard drive downloads either wireless of remotely to a server held on site.

10.83. This would require further development by the rail operators to deliver and potentially could only be networked on new rolling stock.

11. NETWORKING & CONNECTIVITY

11.1. Having remote access to CCTV data is of benefit to operators, BTP and third parties and supports the development of new and more efficient CCTV management processes. These include, but are not limited to:

- Remote management of stations
- Live operational management
- Events management
- Incident / Response management
- Post incident investigations (access to and exporting of recorded data)
- Intelligence gathering
- Minimisation of disruption during incidents
- Improved capability for crowd management
- More efficient CCTV retrieval

11.2. If it is possible to extract CCTV footage across a network, further efficiencies are made. It is no longer necessary to physically collect CCTV data and it can allow a faster conclusion to cases.

11.3. There are significant advantages to CCTV system owners if systems are interconnected. These are normally driven by the desire for a Crime & Disorder Reduction Partnership / Community Safety Partnership to reduce crime and disorder and promote public safety. The most common arrangements that already exist involve connectivity between station and local authority systems but this could be extended to provide access to the BTP. Where such arrangements are considered it is important that, as part of the system configuration and management, agreement is reached on camera / image control via a hierarchy arrangement to ensure proper camera control is prioritised between system users.

11.4. Further advice on securing CCTV networks can be found on the Centre for the Protection of National Infrastructure (CPNI) website www.cpni.gov.uk in the section entitled 'Protecting your assets'.

11.5. It is possible to network and monitor on train CCTV remotely and view live images, including by means of a wireless download system that will allow CCTV data to be transferred whilst the train is in the depot /sidings overnight. However this will require the appropriate level of infrastructure to be in place at all relevant depots. If the depot/siding is also networked to a CCTV control centre, it would be possible for CCTV to be extracted and shared efficiently. Automatic downloading to a central storage by GPRS is also an option for consideration.

11.6. Please see Appendix 'Six' for more detailed information about networking and connectivity.

12. SYSTEM MANAGEMENT & MAINTENANCE

12.1. Access to the system and recorded images should be controlled to prevent tampering or unauthorised viewing.

12.2. A record should be kept of who has accessed the system and when. Further information on this can be found in the BSI document Code of Practice for Legal Admissibility of Information Stored electronically the Data Protection Act 1998 and from local BTP Crime Reduction Officers.

12.3. Processes and procedures should be in place to cover day-to-day operation of the CCTV system. Further information may be found in the BSI document CCTV Management and Operation: Code of practice, ICO's CCTV Codes of Practice and HOSDB's Storage, Replay and Disposal of Digital Evidential Images – 53/07 V1.00 November 2007

12.4. The above mentioned CCTV Code of Practice makes certain suggestions as to the size of signs and where they should be sited.

12.5. By following the Code of Practice, a suitable maintenance regime can be established to ensure the maximum lifetime of equipment, effective image recording and continued system control.

13. FURTHER ADVICE

13.1. For further advice please contact:

ATOC, Police & Security Liaison Officer	020 7841 8165
British Transport Police Crime Reduction & CCTV Dept	020 7830 8994
Transport for London CCTV	020 7027 8489
Network Rail Senior Technology Engineer (SISS & CCTV)	020 7557 8589

14. USEFUL LINKS

14.1. Outlined below are some useful links.

- ATOC – http://www.atoc.org/
- British Transport Police - http://www.btp.police.uk/
- Centre for Protection of National Infrastructure (CPNI) http://www.cpni.gov.uk/protectingassets.aspx
- Data Protection - http://www.ico.gov.uk/what_we_cover/data_protection.aspx
- Department of Transport (Security) – http://www.dft.gov.uk/pgr/security
- HOSDB - http://scienceandresearch.homeoffice.gov.uk/hosdb/
- Information Commissioner's Office - http://www.ico.gov.uk/

- Security Industry Authority - http://www.the-sia.org.uk/home

15. REFERENCE DOCUMENTATION

15.1. The below reference documentation has been used in the creation of this document:

Source	Title
BSI	Code of Practice for Legal Admissibility of Information Stored electronically - BIP0008-1:2004 CCTV Management and Operation: Code of Practice
BTP	British Transport Police – Output requirements from CCTV systems on stations car parks and trains V 1.0 April 2009.
CPNI/Internet	Centre for the Protection of National Infrastructure: Protecting Your Assets
HMSO/Internet	Data Protection Act 1998
HOSDB/Internet	CCTV Operational Requirements Manual 2009 Publication No. 28/09 Digital Imaging Procedure V2.1 November 2007 No. 58/07 Storage, Replay and Disposal of Digital Evidential Images – 53/07 V1.00 November 2007
ICO/Internet	Information Commissioner's CCTV Code of Practice revised edition 2008
HMSO/Internet	ACPO/Home Office National CCTV Strategy – October 2007
HMSO/Internet	Section 17 of The 1998 Crime & Disorder Act

16. OWNERSHIP & REVIEW

16.1. This document is owned by the National Rail and Underground CCTV Steering Group. To make contact with the Steering Group please email the BTP's CCTV Programme Manager Superintendent Peter Rowe Peter.Rowe@btp.pnn.police.uk

16.2. There is a formal change request procedure in place. Should you wish to request a change please email in the first instance ATOC's Police & Security Liaison Officer Mr. Andy Odell andy.odell@atoc.org

16.3. A template change request form is attached marked Appendix 'Seven'.

16.4. The Steering Group meets quarterly and it has determined that unless otherwise necessary a formal review of this guidance document will take place in November 2011.

17. APPENDICES

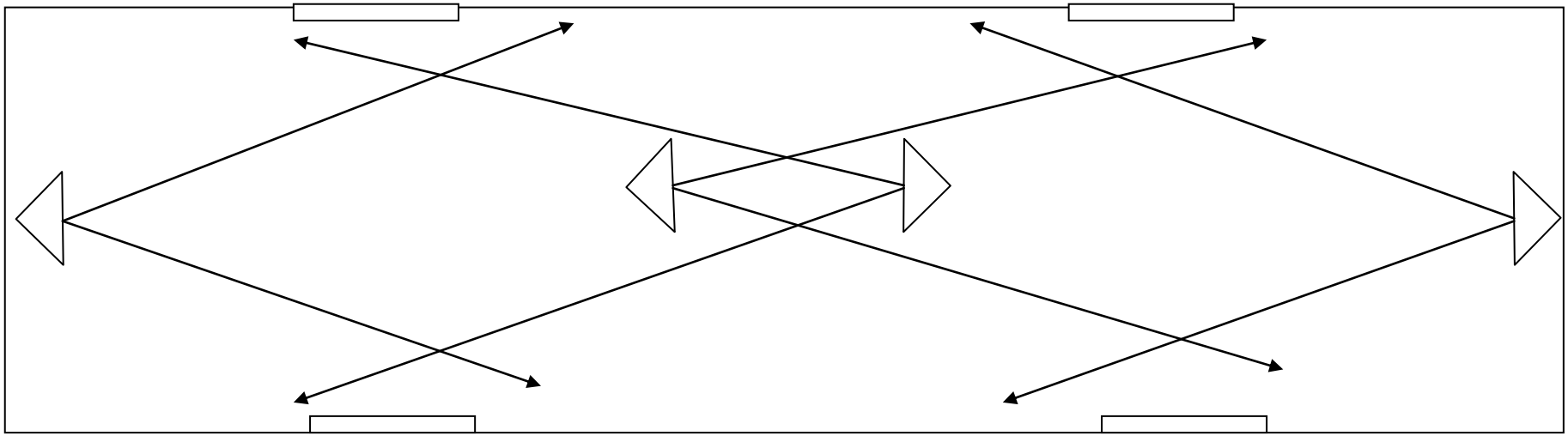
17.1. The following Appendices are referred to in this guidance:

Appendix ‘One’	Optimum on Train Camera Positions and Fields of View
Appendix ‘Two’	Standard CCTV1 Request for CCTV images
Appendix ‘Three’	MG11 CCTV Producing Evidence
Appendix ‘Four’	MG11 CCTV Retrieval/Collection
Appendix ‘Five’	MG11 CCTV Handling/Processing
Appendix ‘Six’	Explanation of Networking
Appendix ‘Seven’	Template Change Request Form

Appendix 'One'

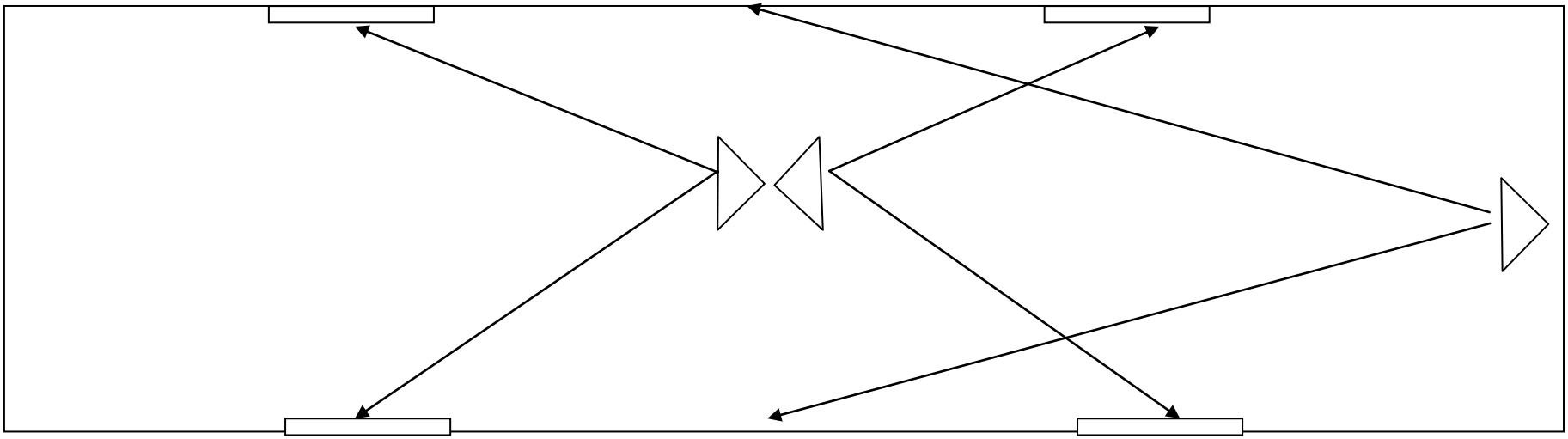
Optimum on Train Camera Positions and Fields of View

Camera Lenses will need to be tested in a unit. It is likely that 16mm or 12 mm focal length will provide the optimum field of view. Arrow heads indicate the centre of each camera field of view. Focus rings must be capable of locking to combat vibration.



Alternative THREE Camera Positions and Fields of View

Camera Lenses will need to be tested in a unit. It is likely that 8mm or 6 mm focal length will provide the optimum field of view. Arrow heads indicate the centre of each camera field of view. Focus rings must be capable of locking to combat vibration.



Appendix 'Two'

Standard CCTV1 Request for CCTV Images

This has been reproduced as a separate document.

Appendix 'Three'

MG11 CCTV Producing Evidence

This has been reproduced as a separate document.

Additional Explanatory Note for completion of this MG11

The Production of Master/Working Copy images and exhibits may cover remote downloads. When completing the FULL LOCATION within the statement operatives should show the full address (which could also include trains, stations, etc.). A brief explanation as to how any Master/Working Copy was created will also assist any interested parties.

Appendix 'Four'

MG11 CCTV Retrieval/Collection

This has been reproduced as a separate document.

Additional Explanatory Note for completion of this MG11

To be used when taking possession (and ownership) of all the various media by which CCTV images can be obtained i.e. VHS, Digital, Hard Drives, Memory Drive and Remote Downloads, etc.

Appendix 'Five'

MG11 CCTV Handling/Processing

This has been reproduced as a separate document.

Appendix 'Six'

NETWORKING & CONNECTIVITY

1. Introduction

1.1 This Appendix is intended to provide guidance for CCTV connectivity. Please also see Section Eleven above.

1.2 Digital systems are able to provide live and recorded remote viewing feeds to any connected CCTV user and the ability to extract recorded data to remote locations.

1.3 As CCTV data is digitally stored on hard drives, there is a level of computer competency required to access and transfer (copy) the recorded data onto a removable storage device, such as DVDs or USB Hard Drives.

1.4 To perform the CCTV transfer task locally can be extremely time consuming and logistically difficult. The user is required to gain access to the CCTV provider's hardware and remain with the system whilst the transfer is conducted. If a connectivity network with sufficient bandwidth is in place, this task can be performed remotely. Even if sufficient bandwidth for extraction is not available CCTV connectivity remains a benefit as it allows the CCTV user to better pinpoint the required CCTV footage thereby minimising the required transfer time.

1.5 A CCTV network provides significant benefits to both operational users and 3rd party users. The following are high level benefits (not in any priority order) to both the rail industry and Police authorities:

- **Minimise disruption during incidents such as on line fatalities and line side incidents**

  If an online fatality occurs, a connectivity network will allow Police and railway operational staff to assess the incident more efficiently, this will minimise any necessary line closure which will in turn reduce costs to the rail operator[12].

- **Improved capability for crowd management and control**

  The ability to remotely view CCTV images provides Rail operational staff and BTP with a better perception of overcrowding on stations. This will allow operational staff or event management teams to more efficiently manage and disperse overcrowding, reducing risk to passengers and rail staff. In turn this will reduce any delays due to platform safety.

- **Enhanced support for Major Events (New Years Eve, major sporting events, football matches)**

  Remote CCTV images allow event management teams to control and supervise major events more efficiently. The ability to remotely view known hot spots or flash points and proactively manage the event is extremely important. Remote CCTV also allows the event manager to get a true feel for the event not reliant on interpretation or opinion from on the ground staff or officers.

[12] Station based CCTV systems do support the investigation of fatalities by BTP in addition to forward facing cameras.

- **Monitor and control trespassing on Rail Industry Property**

  With networked CCTV cameras it is possible to remotely view known areas of trespass. Cameras allow Rail industry staff and Police officers to monitor record and apprehend trespassers. This is done without the need to patrol potentially dangerous areas.

- **Improved day to day management of stations and non crime incidents**

  Networked CCTV provides many opportunities for the rail industry to streamline processes and either reduce resource costs or enable resources to perform other tasks. Gate lines, platforms and help points can be monitored remotely from a single location.

- **Workforce health & safety**

  The ability to view potential incidents or risks proactively can create a safer working environment for Rail industry staff. If stations are monitored from a central location and have sufficient coverage it is possible to spot potential hazards such as litter and spillages.

- **More efficient CCTV retrieval**

  The ability to review footage remotely prior to download or even extract CCTV footage across a network is a big efficiency saving for both rail operators and police officers.

1.6 Historically, CCTV requests have been inefficient and in some cases larger than necessary. This has been cost prohibitive to all parties. If more informed and accurate CCTV requests are made the following can be achieved:

- Reduced retrieval time (Rail industry employees or Police officers)
- Less paper work regarding access to stations and request logging
- Minimisation of media storage requirements - more accurate requests allow better and more efficient use of DVDs, USB hard drives and any other types of storage media.

2 What is Network Connectivity?

2.1 Network connectivity is the term or phrase used within this guidance when CCTV systems are linked together via a network (see paragraph 9.3 below).

3 What is a Network?

3.1 A network is a series of points or nodes interconnected by communication paths. Networks can also interconnect with other networks and contain sub networks.

3.2 They can be characterised in terms of spatial distance as local area networks (LANs) and wide area networks (WANs). Each type of network has some specific considerations.

3.3 CCTV networks are traditionally analogue point-to-point switch circuits, or increasingly commonly digital internet protocol (IP) based circuits, often referred to as Ethernet networks. As Ethernet becomes more common in the CCTV domain it is

increasingly important to ensure that networks are designed and constructed accordingly.

3.4 More information on Ethernet can be found by researching the IEEE 802.3 standards.

4 Compression

4.1 Video compression refers to reducing the quantity of data used to represent digital video images. Video compression removes information in exchange for a smaller file size. Increasing compression leads to the ability to store longer periods on the storage device, but at the expense of sacrificing some of the detail in the images.

4.2 This trade-off must be considered when attempting to balance image quality and recording time on a DVR. Compression also allows data or images to be moved around a connectivity network using less bandwidth, this is both a cost saving and a functional benefit where high levels of bandwidth are not available.

4.3 It is recommended that live operator viewing facilities have a picture resolution of at least 704 x 576 pixels (4CIF) at 12.5 frames per second.

4.4 For further details please refer to the HOSDB's CCTV Operational Requirements Manual 2009 - Publication Number 28/09.

5 Protocol & Compatibility Considerations

5.1 One of the main issues and potential risks with regard to connectivity is the introduction of many different proprietary protocols. This can cause compatibility issues with regard to video playback for recorded image review.

5.2 CCTV systems often utilise proprietary methods for controlling cameras, connecting to cameras and transporting CCTV footage either live or recorded.

5.3 CCTV systems also frequently store CCTV footage in proprietary formats, making it difficult to share CCTV footage with 3rd parties.

5.4 Proprietary formats or protocols often require the use of specialist software usually only available under license from a single manufacturer. The alternative to proprietary formats or protocols is open formats or protocols. These are protocols that are generally free to use, or have a very low cost to implement. Sharing with and connecting to 3rd parties is generally easier and cheaper than implementing proprietary standards due to the documentation available to integrators, and transfer of knowledge about the deployment of open standards around the network / CCTV user communities.

5.5 It is recommended that each CCTV owner maintains open-protocol/format systems to maximise the potential for connectivity, and to ensure that 3rd parties, especially security agencies such as the BTP and other police forces, can promptly and efficiently process any CCTV footage.

6 Bandwidth Considerations

6.1 Bandwidth is a major consideration for any CCTV network which is reliant on the use of the network or part of network.

6.2 For view only facilities such as control rooms and event management rooms, the image can be compressed or encoded which will reduce the necessary network bandwidth.

6.3 Where evidential images are required it is necessary to authenticate the image with no loss of picture quality, this would generally mean that larger video files are being moved around the network. This can be extremely bandwidth intensive.

6.4 As CCTV networks tend towards IP solutions it is essential that any CCTV owner understands the total bandwidth requirements for their systems. Failure to provide adequate bandwidth could result in no CCTV footage being available to view or record.

6.5 Bandwidth should be considered in terms of:

- What is the peak bit rate going from each camera to the recording platform?
- What is the total bandwidth a single user will consume in a normal view session?
- Will this change if activity being observed by the CCTV cameras becomes operationally important?
- What is the maximum number of viewers using the CCTV network at one time?
- What is the usage profile for any 3rd party viewer of live CCTV footage?
- What is the usage profile for any 3rd party viewer of recorded CCTV footage?

6.6 Live and recorded CCTV viewing should be considered separately in most cases as each has separate bandwidth requirements on the network.

6.7 Transfer of large volumes of data can be very demanding on a network.

6.8 As most of these issues are not found in analogue CCTV networks (which can be considered as having a constant and sufficient bandwidth to successfully deliver CCTV video), their criticality for digital networks may be easily overlooked by those without previous experience of them.

6.9 It is recommended that any CCTV system owner audits their own use of CCTV and the requirements of 3rd parties when specifying any CCTV network to ensure sufficient bandwidth can be provided.

7 Latency

7.1 Latency occurs when the bandwidth of the transmission channel is insufficient for the volume of data that is being applied to it, and should be low in a well-designed system. There are number of possible remedies for latency – increase the available bandwidth, reduce the data volume (or a combination of both) and use different network protocols. It is recommended that the end to end latency is below 200ms. When control of a PTZ Camera is necessary, higher levels of latency may be acceptable for other uses.

8 Security Considerations

8.1 It is essential that any CCTV network is suitably secure. Depending on the criticality of the network or the sensitivity of the footage, various security requirements may need to be followed.

8.2 In general a layered approach to securing a CCTV network should be followed, focusing on the need to secure any hardware (physical security) as well as securing the information (electronic security).

8.3 If suitable security is not provided, the integrity of any CCTV footage can be brought into questions, as well as its availability compromised.

Physical Security

8.4 If an attacker has physical access to a computer, router, switch, firewall, or other device, security options are extremely limited. With this in mind it is important to control all technical and user areas.

Electronic Security

8.5 A technology aware attacker may be able to penetrate a network and gain access to CCTV footage or other corporate information (depending on the design of the network). It is therefore essential that the CCTV network is constructed in such a way that access can be controlled and audited by approved personnel only. If there is a requirement to connect to a government owned network there is generally a technical approach to securing network access that can be tested by any inspection body to ensure external systems are not compromised.

8.6 Further advice on securing CCTV networks can be found on the Centre for the Protection of National Infrastructure (CPNI) website www.cpni.gov.uk in the section entitled 'Protecting your assets'.

9 Connectivity for Stations

9.1 It is recommended that rail stations be connected to central CCTV hubs or control centres which allow both Train operators and BTP to view live and / or view and interrogate recorded images. This is typically achieved by connecting all available station systems to a central control centre and linking this to the most accessible BTP CCTV facility.

10 Connectivity for Trains

10.1 At present the collection of CCTV from trains is almost exclusively administered by manual collection of either tapes or hard drives. This can be time consuming, costly and render the train recorder inoperable whilst the data retrieval is being performed.

10.2 Please also see paragraph 11.5 in the main text.

11 Connectivity for Car Parks

11.1 Typically a Car Park System is separate from the Station System and would require independent connectivity; there may be benefits in combining the Station and Car Park systems to allow a single access point to any wider CCTV network. All of the issues addressed in section 9 are relevant to Car Parks.

Appendix 'Seven'

Template Change Request Form

NATIONAL RAIL & UNDERGROUND

CLOSED CIRCUIT TELEVISION (CCTV) GUIDANCE DOCUMENT

From (Full Name):_____ Date: _____

Contact Email _____ Tel:_____

Please use the below table to set out the proposed changes to the guidance document.

1. Please separate each change using the numbered boxes.
2. 'Para No.' refers to the current and latest version of the guidance document. Please check with Andy Odell that you are referring to the latest version. For example, this is the version released in November 2010.
3. Under 'Detail of Change' please set out your proposed change to the wording, format, etc.
4. Under 'Reason' it would be very helpful if you could provide as much background information as possible, including any links to other reports, documents, etc.

No.	Para No.	Detail of Change	Reason
1			
2			
3			
4			
5			
6			
Etc.			

When completed please email this form to Andy.Odell@atoc.org

Appendix A - Request for CCTV Data

POLICE OFFICER / STAFF DETAILS

Crime Ref | NSPIS Ref | Other Ref

Rank | Police Number | Surname | Forename

Force Area | Dept. | Request Date | Other Agency

CCTV TIME & DATE REQUIRED

Start Date | Start Time | End Date | End Time

Incident Type | TOC | Priority Status

CCTV From (Tick One): Train | Station | Other

TRAIN REQUIREMENTS

Line of Route | Head Code (e.g. 1Y23) | Unit No(s) (e.g. 122-311)

Section/s of Train Required / Carriage Number(s)

STATION REQUIREMENTS

Station

Cameras / Area Required

OTHER PREMISES REQUIREMENTS

Exact Location

ADDITIONAL INFORMATION

Additional Information (e.g. descriptions)

Important Note: One form must be submitted for each separate location. Requests for CCTV from each train, station and other place must be treated as individual requests.

WITNESS STATEMENT

CJ Act 1967, s.9; MC Act 1980, ss.5A (3) (a) and 5B; Criminal Procedure Rules 2005, Rule 27.1

Statement of:	**URN**				

Age if under 18: (if over 18 insert 'over 18') Occupation:

This statement (consisting of page(s) each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it, anything which I know to be false, or do not believe to be true.

Signature…….. ..... Date

Tick if witness evidence is visually recorded ☐ *(supply witness details)*

Production of Master / Working Copy Images and Exhibits

I am NAME

I am employed as

Working for NAME OF COMPANY / POLICE AREA

On DAY DATE TIME

I received from - FULL NAME AND TITLE

ORGANISATION

A request to secure CCTV from FULL LOCATION

For DAY DATE TIME(S)

On DAY DATE TIME

I checked the time of the images against the MSF Signal (formerly the Rugby Clock) and found the following discrepancy

I created (for disks) / produced (for tapes) a Master Copy and / or Working Copy from camera No(s)

Signature…… Signature witnessed by:

Continuation of Statement of

On DAY DATE TIME

I handed to - FULL NAME AND TITLE

ORGANISATION

The following items (full description and quantity) which were placed in property bags/jewel cases and sealed.
I produce the exhibits shown below:

Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number

Please note if you have additional Exhibit Description / Exhibit Number / Seal Number items to include, see the last page of this document

Signature…… Signature witnessed by:

Witness contact details

Home address Postcode

Home telephone No Work telephone No:

Mobile/Pager No E-mail address:

Preferred means of contact *(specify details)*:

Best time of contact *(specify details)*:

Male / Female click here Date and place of birth

Former name Ethnicity Code (16 + 1) click here

Religion / Belief *(Specify)*

Dates of Witness Non-Availability:

Witness care

a) Is the witness willing to attend court? Yes ☐ No ☐ If 'No', include reason(s) on form **MG6**.

b) What can be done to ensure attendance?

c) Does the witness require a Special Measures Assessment as a vulnerable or intimidated witness? Yes ☐ No ☐
If 'Yes' submit **MG2** with file.

d) Does the witness have any particular needs? Yes ☐ No ☐

If 'Yes' what are they? (Disability, healthcare, childcare, transport, language difficulties, visually impaired, restricted mobility or other concerns?)

Witness Consent (for witness completion)

a) The Victim Personal Statement scheme (victims only) has been explained to me: Yes ☐ No ☐

b) I have been given the Victim Personal Statement leaflet Yes ☐ No ☐

c) I have been given the leaflet "Giving a witness statement to the police – what happens next? Yes ☐ No ☐

d) I consent to police having access to my medical record(s) in relation to this matter (obtained in accordance with local practice) Yes ☐ No ☐ N/A ☐

e) I consent to my medical record in relation to this matter being disclosed to the defence Yes ☐ No ☐ N/A ☐

f) I consent to the statement being disclosed for the purposes of civil proceedings if applicable, e.g. child care proceedings, CICA Yes ☐ No ☐

g) The information recorded above will be disclosed to the Witness Service so that they can offer help and support, unless you ask them not to. Tick this box to **decline** their services ☐

Signature of witness PRINT NAME

Signature of parent/guardian/appropriate adult PRINT NAME

Address and telephone number if different from above

Statement taken by (print name): Station

Time and place statement taken

Continuation of Statement of

The following items (full description and quantity) which were placed in property bags/jewel cases and sealed. I produce the exhibits shown below:

Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number
Exhibit Description	Exhibit Number	Seal Number

Signature………………………………………………….. Signature witnessed by

WITNESS STATEMENT

CJ Act 1967, s.9; MC Act 1980, ss.5A (3) (a) and 5B; Criminal Procedure Rules 2005, Rule 27.1

Statement of:	**URN**				

Age if under 18: (if over 18 insert 'over 18') Occupation:

This statement (consisting of page(s) each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it, anything which I know to be false, or do not believe to be true.

Signature…….. ..... Date

Tick if witness evidence is visually recorded ☐ *(supply witness details)*

Collection / Retrieval of CCTV

I am NAME

I am employed as

Working for NAME OF COMPANY / POLICE AREA

On DAY DATE TIME

I visited FULL ADDRESS

To collect / retrieve CCTV recorded on

DAY DATE TIME(S)

Covering location

In relation to NSPIS Incident Number or CRIME Number

OTHER Reference

I took possession (and ownership) of the following items from

Full name and title / CCTV System

Exhibit / Item Description Exhibit / Item No Seal No

Signature…….. Signature witnessed by

Continuation of Statement of:

Signature…….. Signature witnessed by

Witness contact details

Home address Postcode

Home telephone No Work telephone No:

Mobile/Pager No E-mail address:

Preferred means of contact *(specify details*:

Best time of contact *(specify details)*

Male / Female click here Date and place of birth

Former name Ethnicity Code (16 + 1) click here

Religion / Belief *(Specify)*

Dates of Witness Non-Availability:

Witness care

a) Is the witness willing to attend court? Yes ☐ No ☐ If 'No', include reason(s) on form **MG6**.

b) What can be done to ensure attendance?

c) Does the witness require a Special Measures Assessment as a vulnerable or intimidated witness? Yes ☐ No ☐
If 'Yes' submit **MG2** with file.

d) Does the witness have any particular needs? Yes ☐ No ☐

If 'Yes' what are they? (Disability, healthcare, childcare, transport, language difficulties, visually impaired, restricted mobility or other concerns?)

Witness Consent (for witness completion)

a) The Victim Personal Statement scheme (victims only) has been explained to me	Yes	☐		No	☐	
b) I have been given the Victim Personal Statement leaflet	Yes	☐		No	☐	
c) I have been given the leaflet "Giving a witness statement to the police – what happens next?	Yes	☐		No	☐	
d) I consent to police having access to my medical record(s) in relation to this matter (obtained in accordance with local practice)	Yes	☐	No	☐	N/A	☐
e) I consent to my medical record in relation to this matter being disclosed to the defence	Yes	☐	No	☐	N/A	☐
f) I consent to the statement being disclosed for the purposes of civil proceedings if applicable, e.g. child care proceedings, CICA	Yes	☐		No	☐	
g) The information recorded above will be disclosed to the Witness Service so that they can offer help and support, unless you ask them not to. Tick this box to **decline** their services						☐

Signature of witness PRINT NAME

Signature of parent/guardian/appropriate adult PRINT NAME

Address and telephone number if different from above

Statement taken by (print name) Station

Time and place statement taken

WITNESS STATEMENT

CJ Act 1967, s.9; MC Act 1980, ss.5A (3) (a) and 5B; Criminal Procedure Rules 2005, Rule 27.1

Statement of:	**URN**				

Age if under 18: (if over 18 insert 'over 18') Occupation:

This statement (consisting of page(s) each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it, anything which I know to be false, or do not believe to be true.

Signature…….. ..... Date

Tick if witness evidence is visually recorded ☐ *(supply witness details)*

CCTV Handling & Processing

I am NAME

I am employed as

Working for NAME OF COMPANY / POLICE AREA

On DAY DATE TIME

I opened ☐ PROPERTY BAG ☐ SEAL REF NUMBER

And removed ☐ VIDEO TAPE ☐ DISK ☐ OTHER REF NUMBER

In the presence of

I carried out the following processes

☐ VIDEO EDITING ☐ DUPLICATION ☐ STILL IMAGE PRODUCTION ☐ OTHER

I then produced the following exhibits

Signature…….....Signature witnessed by

Continuation of Statement of

Signature…….....Signature witnessed by

Witness contact details

Home address Postcode

Home telephone No Work telephone No:

Mobile/Pager No E-mail address:

Preferred means of contact *(specify details)*:

Best time of contact *(specify details)*:

Male / Female click here Date and place of birth

Former name Ethnicity Code (16 + 1) click here

Religion / Belief *(Specify)*

Dates of Witness Non-Availability:

Witness care

a) Is the witness willing to attend court? Yes ☐ No ☐ If 'No', include reason(s) on form **MG6**.

b) What can be done to ensure attendance?

c) Does the witness require a Special Measures Assessment as a vulnerable or intimidated witness? Yes ☐ No ☐
If 'Yes' submit **MG2** with file.

d) Does the witness have any particular needs? Yes ☐ No ☐

If 'Yes' what are they? (Disability, healthcare, childcare, transport, language difficulties, visually impaired, restricted mobility or other concerns?)

Witness Consent (for witness completion)

a) The Victim Personal Statement scheme (victims only) has been explained to me: Yes ☐ No ☐

b) I have been given the Victim Personal Statement leaflet Yes ☐ No ☐

c) I have been given the leaflet "Giving a witness statement to the police – what happens next? Yes ☐ No ☐

d) I consent to police having access to my medical record(s) in relation to this matter (obtained in accordance with local practice) Yes ☐ No ☐ N/A ☐

e) I consent to my medical record in relation to this matter being disclosed to the defence Yes ☐ No ☐ N/A ☐

f) I consent to the statement being disclosed for the purposes of civil proceedings if applicable, e.g. child care proceedings, CICA Yes ☐ No ☐

g) The information recorded above will be disclosed to the Witness Service so that they can offer help and support, unless you ask them not to. Tick this box to **decline** their services ☐

Signature of witness PRINT NAME

Signature of parent/guardian/appropriate adult PRINT NAME

Address and telephone number if different from above

Statement taken by (print name): Station

Time and place statement taken