NATIONAL CCTV STRATEGY

OCTOBER 2007

GRAEME GERRARD

GARRY PARKINS

IAN CUNNINGHAM

WAYNE JONES

SAMANTHA HILL

SARAH DOUGLAS

Acknowledgements

The Joint Home Office ACPO team would like to express their thanks to all those involved in contributing towards the drafting of this document

The front cover photograph is reproduced with permission from www.doktorjon.co.uk © www.doktorjon.co.uk

CONTENTS

FOREWORD

The United Kingdom is generally recognised as a leading user of Closed Circuit Television (CCTV) for community safety and crime investigation purposes. We regularly see examples of where it has been used to make our streets safer, reduce the fear of crime and detect serious offences. The use of CCTV in the support of terrorist investigations in the UK has led to considerable worldwide interest, with many countries now following us in developing CCTV infrastructures.

CCTV enjoys considerable public support and it is important that this is maintained. This report has identified the significant benefits associated with CCTV, but also highlights the potential improvements that can be made to existing systems. Although the current CCTV infrastructure is very good, it could be much better if it was effectively coordinated and there is a direction that all users could follow in terms of future developments.

The Home Office continues to be in favour of technical developments that will improve the effectiveness of CCTV, but we need to ensure that any system adopted will be effective. The review upon which this report is based highlights among a number of things the problems faced using images for evidential purposes in the Criminal Justice System (CJS). It should be our collective aim and responsibility to ensure that, as well as the need to keep up with technical developments in the industry as a whole, improvements in provision remain consistent with the requirements of the CJS and with the needs of the Court Service in particular.

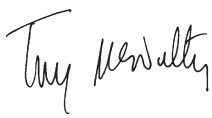
The report looks at the attention being paid to improvements in the technical aspects of CCTV development, the potential benefits and impact of digital recording systems, rapidly evolving technology, and the legal background to the operation of CCTV. It also highlights the constant need to observe data protection, privacy and human rights legislation. Recognising data protection and privacy rights in the operation of all systems is not only important because the law requires us to do so, but also that it is right that we should do so, with concerns about surveillance so apparent in our everyday lives.

I see CCTV as an important tool in the Government's crime-fighting strategy.

The review upon which this report is based highlights some of the problems faced by many of those who operate and manage CCTV systems. The need for standards, better training, improved partnership working and more coordinated use of new technology will ensure that we get the best out of new and existing CCTV systems.

I very much welcome this report. I am grateful to the joint Home Office and ACPO team involved in this important piece of work and for setting out the way forward clearly and concisely. The recommendations are wide-ranging and will require immense efforts on behalf of everyone involved in continuing to making CCTV effective. At the end of the day, if the public were to lose confidence in CCTV as a beneficial influence, we risk losing a very valuable tool in the battle against crime and disorder.

I look forward to seeing the continued development of CCTV following this review and in particular the work of the National CCTV Strategy Programme Board.



TONY MCNULTY
Minister of State for Security,
Counter Terrorism and Police and Ministerial Adviser on Parliamentary Affairs

EXECUTIVE SUMMARY

Closed circuit television (CCTV) plays a significant role in protecting the public and assisting the police in the investigation of crime. In many ways, we have led the world from its early introduction in the 1970s to the massive growth in CCTV installation and use in the 1990s.

The Government has invested heavily in local authority-operated CCTV schemes and most town centres benefit from CCTV cameras. Although we have more CCTV than many other countries, most is privately owned and operated by the commercial sector and covers areas such as retail establishments and shopping malls.

CCTV has been instrumental in helping the police to identify and bring to justice those involved in all aspects of criminality, perhaps the most notable being serious crime and terrorist incidents. CCTV in the UK enjoys significant public support and year on year fear of crime surveys states that the public feels safer due to the presence of CCTV.

The contribution CCTV has made in protecting the public and assisting the police to investigate crime has occurred despite CCTV systems being developed in a piecemeal fashion with little strategic direction, control or regulation. This approach has failed to maximise the potential of our CCTV infrastructure and many involved in its operation and management felt there remained a pressing need to examine existing standards, procedures, training and methods of operation. In addition, as local authorities, the police and criminal justice agencies face the challenges associated with the move from VHS technology to digitally recorded images, the lack of a co-ordinated approach to CCTV development poses significant risks in terms of compatibility of systems, cost of accessing the images and the potential loss of operational effectiveness. Recognising the current concerns and both the risks and potential opportunities that CCTV can bring, a report was submitted by the Association of Chief Police Officers (ACPO) lead on CCTV to the Home Office recommending that there was now an urgent need for the development of a national strategy that would ensure the effective development of the public space CCTV infrastructure. The report was endorsed by the thenCrime Reduction Delivery Board in September 2005.

This strategy is the culmination of work undertaken by a small joint ACPO/Home Office project team, supported by a wide range of stakeholders involved in the use and management of CCTV.

This report is broadly based on the following 10 themes and examines each issue in detail.

- The need for standards in all aspects of CCTV;
- The need for clear guidelines on registration, inspection and enforcement;
- Training of all personnel;
- The police use of CCTV footage and evidence
- Storage / Volume / Archiving / Retention issues
- The need for CCTV Networks – Live & Stored
- Equipping, resourcing and standardisation within the CJS
- Emerging Technologies / Changing Threats / New & Changing Priorities
- Partnership Working
- Financial and Resource management.

The 44 recommendations proposed within this report represent a significant effort for all agencies involved in CCTV. Progress in these areas is extremely important if we are to realise the full potential of CCTV across a varied range of uses and continue to receive the support of the public.

The next stage of this work will be in the form of an implementation phase which will prioritise and develop the recommendations and establish the future strategic direction. In order to do this we have established a multi agency team that represents key stakeholders and an overarching Programme Board that will co-ordinate the activity and ensures the cooperation and agreement that is vital if the Strategy is to be implemented successfully.

CHAPTER 1 : INTRODUCTION

1.1. BACKGROUND TO CCTV IN THE UK

For many years, Closed Circuit Television (CCTV) has been instrumental in identifying and bringing to justice those involved in all aspects of criminality, perhaps most notable of these being serious crime and terrorist incidents. From the IRA terrorist campaign in the 1990s and the Brixton nail bomber in 1999, to the terrorist incidents in London in July 2005, CCTV released to the public led to early identification of suspects and played an important role in the subsequent prosecutions.

Recent successes in the capture of assailants in a number of high profile cases as a result CCTV and its subsequent link to automatic number plate recognition (ANPR) is yet another example of their value in serious crime investigations.

The origins of CCTV provision for public space in this country lie in the early 1980s. Since then the use of CCTV systems has expanded gradually but significantly. The earliest systems were funded in a small number of cases by the police or local businesses, but in the majority of cases by local authorities through what were then known as City Challenge or Safer Cities Initiatives.

Subsequent Government funding took the form of the CCTV Challenge Competition between 1994 and 1999, under which £38.5 million was made available for some 585 schemes nationwide.

In turn, between 1999 and 2003, major investment was made in public space CCTV through the Home Office-funded Crime Reduction Programme (CRP). A total of £170 million of capital funding was made available to local authorities following a bidding process. As a result of this funding, more than 680 CCTV schemes were installed in town centres and other public spaces. The end of the Crime Reduction Programme signalled the end of a dedicated central funding regime for public space CCTV. However, local areas continued to have access to Home Office grant monies in the form of general funding for crime reduction through funding streams such as Communities Against Drugs (CAD), Safer Communities Initiative (SCI), the Building Safer Communities Fund (BSCF) and the current joint Home Office/ Department for Communities and Local Government initiative, the Safer Stronger Communities Fund (SSCF), as well as wider funding opportunities, for example that given by the Department for Communities and Local Government (DCLG) under arrangements for neighbourhood renewal and similar schemes.

The CRP represented the biggest ever single investment in CCTV and extended its coverage and use. It was a key part of the Government's programme to tackle and reduce crime and disorder.

CCTV has been thought to be an effective tool, particularly as an aid to detection, and when used as part of a wider crime reduction strategy. It has a good track record and the CRP initiative was designed to help reduce the unacceptably high crime rates in some areas. The Government gave priority to bids to support the regeneration of housing estates with high crime rates, making a real difference to the quality of life of the people who lived on those estates. CCTV for car parks seeking Secured Car Park status was also a priority.

CRP funding was also available for CCTV in town or city centres, including improvements and extensions to existing schemes, and for other crime "hot-spots", such as access to community, commercial and transport facilities. Crime and Disorder Reduction Partnerships (CDRPs) were asked to play a key role in helping to decide where CCTV could be most effectively used. As part of the application process, bidders were required to set realistic and achievable crime reduction targets which demonstrated the impact CCTV could have when deployed as part of a wider strategy.

As a result of this huge investment, most public space CCTV is now owned, monitored and managed by local authorities, many of whom have procured different systems at different times and with a range of different specifications, leading to a mix of schemes across the country. Although the Government has invested heavily in public space CCTV schemes, so too have local authorities and local partnerships. Local authorities also continue to carry much of the burden for the ongoing costs of running and maintaining their schemes.

In addition to the police, there are many other uses and users of CCTV, such as benefit fraud investigators, insurance companies and solicitors. In addition CCTV evidence is also passed onto local authority officers – highways enforcement officers, dog wardens, health safety and licensing and the Environment Agency. Local authority Emergency Planning Teams and the London Fire Brigade have also used recordings of incidents for training purposes.

It should also be remembered that while there exists a large number of local authority operated CCTV cameras, it is a very small proportion of the nation's CCTV provision, since the vast majority are commercially owned.

The effectiveness of CCTV systems therefore varies significantly across the country and there is a wide variance in terms of coverage, monitoring, quality of images, uses and therefore the impact that CCTV can have on local crime and disorder. Similarly, there is considerable variance in the way police forces utilise CCTV and whether the product of surveillance cameras is effectively integrated into the policing function.

The introduction of digital CCTV systems could provide opportunities for real benefits if the technology is harnessed correctly. However, it has also created a new set of difficulties.

Improving the quality of CCTV images will support the development of current, complimentary technologies such as Automatic Number Plate Recognition (ANPR) and future technologies such as facial recognition.

1.2. BACKGROUND TO THE REVIEW

Given the difficulties associated with the diverse state of CCTV coverage referred to above, the Association of Chief Police Officers (ACPO) recognised the need to address the various problems. In April 2005, the ACPO CCTV/Video Working Group submitted a paper to the Home Office suggesting that there was a need to develop a strategy for the future development of public space CCTV. The strategy would need to determine a programme of activity that should be undertaken in order to maximise the operational effectiveness of the country's current CCTV infrastructure.

The terrorist incidents in London in July 2005 also highlighted the effectiveness of CCTV as an aid to investigation but also identified issues in relation to the lack of integration, quality of images and the

difficulties associated in retrieving digitally recorded footage.

The ACPO paper was presented to the then Home Office Crime Reduction Delivery Board (CRDB) in the autumn of 2005. The paper identified the need for a multi-agency approach to be taken in order to seek the views and support of the many agencies that have an interest in the development of public space CCTV.

The CRDB unanimously supported the proposals, and established a project team to review the use of CCTV nationally, and to take forward work on developing the strategy that was so badly needed. The Home Office and ACPO jointly committed to form a joint ACPO/Home Office project team.

The terms of reference for the project agreed by the CRDB were:

- To review the current CCTV infrastructure to establish its effectiveness in terms of crime and disorder reduction and detection; and
- Through consultation with various agencies, to develop a strategy that improves the effective use of CCTV in terms of crime and disorder reduction and detection, taking into account developing technology and threats.

1.3. REVIEW METHODOLOGY

Work on the project began in mid-January 2006.

A series of workshops were held to understand the current CCTV infrastructure, its use and where the main issues and problems lie from the perspective of key stakeholders and interested parties. The workshops were an opportunity for users of CCTV and stakeholders to air their experiences and views on current public space CCTV.

The workshops were organised to bring similarly interested groups together as part of the consultation. These included representatives from the following stakeholder groups:

- Serious crime, transport, government departments, the criminal justice system, technology and town centre CCTV groups.

The team also held consultation exercises at the ACPO/HOSDB CCTV conference and met with the PCMA/LCMG (town centre CCTV managers).

In addition, the review team:

- Presented and took questions at the Thinking Strategically about CCTV Conference (March 2006), the CCTV Users Group Conference (April 2006, October 2006 and April 2007) and the Local Authority CCTV conference (July 2007) .
- Held a number of smaller meetings with the Information Commissioner's Office (ICO), ACPO Digital Imaging Project Board, ACPO ANPR, CCTV User Group, Public CCTV Managers Association (PCMA), town centre managers and other interested parties.

During the review, the National Policing Improvement Agency (NPIA) was in the process of being established. From April 2007 the NPIA took on work from existing policing organisations including

Centrex and PITO and some parts of the Home Office. They additionally work with the Police Service on new areas of activity, including large scale work programmes which affect all forces.

From the evidence gathering sessions, the issues identified soon began to fit into ten broad groups:

- The need for standards in all aspects of CCTV;
- The need for clear guidelines on registration, inspection and enforcement;
- Training of all personnel;
- The police use of CCTV;
- Storage / Volume / Archiving / Retention issues;
- The need for CCTV Networks – Live & Stored;
- Equipping, resourcing and standardisation within the CJS;
- Emerging Technologies / Changing Threats / New & Changing Priorities;
- Partnership Working; and
- Financial and resource management.

These ten issues form the basis for the chapters in this report.

Finally, during the course of 2007, the strategy in draft form was sent out to a number of stakeholders for comment and a programme board has been created to take forward the recommendations

CHAPTER 2 : STANDARDS

2.1. INTRODUCTION

Closed circuit television cameras are an increasing feature of our daily lives. There is an ongoing debate over how effective CCTV is in reducing and preventing crime, but one thing is certain, its deployment is commonplace in a variety of areas to which members of the public have free access.

At the outset of the installation of CCTV there was no statutory basis for systematic legal control of CCTV surveillance over public areas until 1 March 2000 when the Data Protection Act 1998 came into force. The definitions in this Act are broader than those of the Data Protection Act 1984 and so more readily cover the processing of images of individuals caught by CCTV cameras than the previous legislation. The same enforceable information handling standards that previously applied to those processing personal data on computer now cover CCTV.

There remains no statutory or legal obstacle to installing a CCTV camera or system, and it is open to anyone to do so, provided they meet the requirements of the Data Protection Act 1998. Chapter 3 discusses DPA issues in greater detail.

It became clear at every workshop, conference and meeting held as part of the Review's evidence-gathering phase that there was a need for clear and transparent standards in every aspect of CCTV provision.

The standards, which must be met if the requirements of the Data Protection Act 1998 (DPA) are to be satisfied, are based on the eight data protection principles which are:

- fairly and lawfully processed.
- processed for limited purposes and not in any manner incompatible with those purposes.
- adequate, relevant and not excessive;
- accurate.
- not kept for longer than is necessary.
- processed in accordance with individuals' rights.
- secure.
- not transferred to countries without adequate protection.

2.2. KEY ISSUES

It became evident during the consultation that the issues relating to the inadequacy of standards could be categorised as follows:

2.2.1. INCOMPATIBLE SYSTEMS

In the pre-digital (analogue) era, international standards (such as PAL and the de facto VHS) have provided a certain degree of compatibility in camera resolutions, their output specifications, transmission standards,

and recordings. Whilst there were differences, for example, in how different CCTV manufacturers controlled and recorded multiple cameras by use of proprietary codes, those problems were largely overcome. With the emergence of digital CCTV systems which are likely to fully replace existing analogue CCTV systems in the next few years and the rapid convergence of IT and television, the situation has taken a turn for the worse.

The CCTV industry is at the forefront of implementing emerging technologies and is constantly developing new digital CCTV systems by using the very latest technology and adapting it to their needs. The results have been a myriad of largely incompatible systems that in the main adhere to no common or open standards. This results in largely proprietary systems and recordings.

With hundreds of international manufacturers, offering thousands of different products to the CCTV industry, purchasers, system designers and police and other CJS users are faced with many issues. Some of these include the fact that purchasers and system designers have identified that digital cameras from one manufacturer may not be compatible with other manufacturers' recording systems. This restricts their ability to pick and choose different system components without being tied in to one manufacturer.

Police and CJS users have difficulty in playing back CCTV footage from the many proprietary recording formats. The police service is employing specialist technical staff to recover and process digital CCTV footage, but the CJS often has difficulty playing back in these formats. Currently, the measures used to overcome this are conversion to other standard formats (in most cases VHS). This is time consuming, can result in a reduction of quality, integrity and contravenes the intended practice laid out in the Home Office Scientific Development Branch (HOSDB) Digital Imaging Procedures.

2.2.2. PICTURE QUALITY

The quality of images recorded by CCTV systems varies considerably. Anecdotal evidence suggests that over 80% of the CCTV footage supplied to the police is far from ideal, especially if it is being used for primary identification or identities are unknown and identification is being sought, for instance, by media release.

A series of guidance documents from HOSDB issued throughout the 1990s recommended minimum performance guidance according to the different tasks for which CCTV images may be required. The recommendations are referred to in many publications including British Standards and ICO advice. The recommendations introduced the "Rotakin" - a device to test the quality of the displayed image. The guidance was intended mainly for live CCTV monitoring, and did not adequately address the recommended quality of recordings, or how to test the systems to ensure that the recorded images were fit for purpose. It is widely accepted that the Rotakin test needs to be updated for use with digital CCTV systems.

There are also concerns that the documents in the series are not more widely used, especially by small CCTV users. Some maintain that they are difficult to read, their advice is out of date and they were written in a pre-digital era. There are now many more variables that affect quality such as resolution of the image, amount and types of compression.

2.2.3. OPERATIONAL REQUIREMENTS

Several related HOSDB documents have been produced which address the operational requirements of a CCTV system; the most requested of these being the HOSDB Operational Requirements Manual 17/94.

It is felt the advice did not go far enough in exploring the reasons for installing CCTV in the first instance, establishing the exact purpose of the CCTV system and individual cameras, and how the critical success of the system could be measured. (HOSDB has recently updated the Operational Manual 17/94 with a publicly released draft available from the HOSDB website)

2.2.4. FIT FOR SEVERAL PURPOSES

Increasingly, CCTV systems are now being used for a variety of purposes.

In town centre CCTV schemes, in addition to crime and disorder uses, cameras are increasingly being used for parking and bus lane enforcement. Whilst in many circumstances additional cameras are being installed, in some cases the cameras' initial purpose has been changed or they are required to perform a number of additional and conflicting tasks. Some existing cameras originally installed for detecting crime are now being positioned to monitor a bus lane and record vehicle number plates. Whilst the cameras are being used in this way, it seems unlikely that they will then be used proactively to patrol the area and detect crime. Current installed cameras cannot perform these two functions at the same time.

The London Councils' (ALG) Camera Sharing Group has done a lot of work in establishing protocols and enabling camera sharing between local authority, Transport for London (TfL) and other agencies. Whilst it makes good financial sense to share cameras, and a good example of a partnership approach, particular care and attention should be given to ensure that cameras installed for crime and disorder are not diverted to other uses. Although it is more acceptable, for instance, to use TfL enforcement cameras for crime and disorder when they are not being used for their intended purpose, the cameras cannot be used for two different purposes at the same time, without some conflict and a reduction in their effectiveness.

There is also a conflict between the pro-active and post incident investigation use of CCTV. Town centre operators use the cameras pro-actively to search for suspicious behaviour, certain types of activity, or in response to intelligence or ongoing incidents communicated to them by police or other parties. This real time pro-active use of the cameras is at the heart of the CCTV operator's role. Unfortunately, this often frustrates investigators reviewing CCTV. If an incident was not captured initially, the roaming cameras, and distant shots are unable to provide secondary evidence/intelligence, by providing a good quality continuous recording at set locations or choke points in the vicinity of the crime. This results in investigating officers having to trawl nearby addresses and subsequently relying on external CCTV cameras from commercial premises. CCTV in this instance was never expected to provide the quality of images required for police investigations.

In other situations, such as transport hubs, shopping centres, shops, public houses and clubs, the role of CCTV cameras is widened even further. Often the primary role is not the detection and prevention of crime. The purpose of the CCTV scheme may be to monitor crowds, slips, trips and falls and staff crime. Often there is a public expectation that these systems are being installed for their safety, but the CCTV may not be of sufficient quality for police to use in criminal investigations.

2.2.5. COVERAGE/DEPLOYMENT

A commonly-used estimate for the number of cameras operational in the UK is that generated in a study by Michael McCahill and Clive Norris in 2002. This provided what has been regarded by many as the best estimate figure of around 4.2 million cameras. In London, it is estimated that on average, an individual may be recorded by over 300 different cameras in any given day. However, the evidence from police

investigations does not suggest such extensive coverage. This may be for a combination of reasons, including: the figures are wrong; there is excessive coverage in some areas and insufficient in others; the quality of the images recorded by the cameras are not fit for purpose; the police are not able to make best use of the cameras and the resources required in retrieving and reviewing them is excessive for the resources available.

It is established that crime patterns change. Much of the CCTV was installed in the 1990s, and any analysis of the siting of cameras may not still be relevant today.

Increasingly, temporary cameras are being deployed. There is little evidence to suggest whether crime mapping analytical tools and the National Intelligence Model (NIM) are being consistently used to determine the most effective deployment of CCTV cameras.

Considerable improvements in the effectiveness of CCTV can be obtained if actively monitored town centre CCTV schemes extend their monitoring services to other CCTV systems already in public areas such as railway/tube stations, shopping centres and other areas of public activity. This is particularly important when these systems are not being actively monitored, and the areas are being used for criminality or are being used as an escape beyond the range of the actively monitored CCTV systems. But equally savings can be made within the partnerships and the ability to communicate in real time directly to police through their existing channels should be advantageous to all concerned.

Understandably, this has resource implications, and if these systems are to be monitored effectively, more resources and financing will be required. Equally, partners will have to be confident as to effectiveness of the arrangement and it will have to be carefully assessed as being adequately resourced, effective and value for money.

2.2.6. BUSINESS PROCESSES

Research has shown a vast range in the quality and usefulness of the business processes employed across all of those involved in CCTV. This includes standard working practices; standard job profiles; standard interfaces / protocols with other agencies; the use of standard performance indicators; evidence to support business cases, and indications of success. This was particularly noticeable in the differences between police forces, local government, and the interfaces between them. This has led to a fragmented approach across the country. Best practices have not been built upon and there have been strained or less effective interfaces.

2.2.7. CRADLE TO GRAVE (CAMERA TO ARCHIVE)

An important theme that emerged throughout the consultation was the need for a joined up end–to-end process, i.e.: “camera to archive”.

There was little evidence to suggest that the whole life-cycle of CCTV was always considered at every stage. For example, in many circumstances those purchasing systems failed to consider how the CCTV would be used, including how it would be retrieved and played back by the police, or how straightforward it would be for playback in court, and ultimately how it would be archived to enable it to be played back in ten or more years’ time.

Other examples included failing to take advantage of complementary works, which could reduce the overall cost of CCTV. This included influencing building design and licensing/ legislation requirements,

low cost variations on large infrastructure projects, such as the digging up of roads, laying conduit for CCTV or large scale IT projects which could tie in with digital CCTV, transmission, and storage etc.

2.3. CONCLUSION

The following conclusions were arrived at following consultation with key stakeholders:

- Incompatible systems have led to the police employing specialist technical staff to recover and process digital CCTV footage. The CJS has difficulty playing back these proprietary formats.
- The picture quality of images obtained from CCTV systems varies considerably and is often far from ideal, especially if it is being used for primary identification of a suspect and identification is being sought.
- HOSDB operational guidance documentation was fairly dated and difficult to read but it is currently being reviewed and brought up to date.
- CCTV cameras are increasingly being used for potentially conflicting roles, which results in them becoming less effective for crime and disorder purposes. Until a viable technical solution is found, consideration should be given to supplementing existing pan-tilt-zoom (PTZ) cameras with fixed cameras capable of continually providing good quality images for post investigation use, and if and when they are justified, dedicated cameras installed for non crime detection use, thus allowing the original PTZ cameras to be used for their original pro-active surveillance use.
- There is a vast difference and variance in the quality and usefulness of the business processes employed across the CCTV landscape.
- We cannot say with any certainty how accurate previous estimates of camera numbers are. Efforts are ongoing to ascertain numbers through consultation with local authorities, but there is a good deal of uncertainty about the extent of provision nationally. This uncertainty extends to where the cameras are, if they are deployed and covering the correct areas, if the images they produce are fit for purpose and whether they are being used effectively by the police. This in itself is a major problem and one which requires a clear, transparent strategy that will be central to delivering a strategy for the short-to-medium term. Without a better understanding of the degree of coverage, or a clearer and supported end to end process, future guidance around common standards in all the areas of concern above, will fall far short of what is required to ensure a meaningful strategic direction.
- Increased CCTV effectiveness can be achieved if actively monitored town centre CCTV schemes are also encouraged to monitor existing CCTV systems in other largely public areas such as railway/tube stations and where possible onboard CCTV in buses, tube and train carriages, extending to shopping centres, football stadiums, arenas, thus becoming the de-facto hub for public space CCTV. It should be the aim that such monitoring be carried out in a fully co-ordinated way.

2.4. RECOMMENDATIONS

R 2.1. Establish digital CCTV standards. Agreement would have to be reached between police, CJS and public space CCTV operators. One way would be for the stakeholders to agree on a standard digital video format that they will accept. To achieve this, it would be appropriate to establish a technical standards group within the stakeholders / governance group.

R 2.2. Setting of standards more generally by the stakeholders. There would be merit in seeking to influence national and international CCTV standards. It is proposed that one of the ways of achieving this would be through the involvement of national and international standards setting bodies, and seeking collaborative working with industry and national and international police agencies and organisations

R 2.3 Continue the review of the Home Office HOSDB Operational Requirements (OR) Manual. Work on this is currently underway . (HOSDB have recently updated the Operational Manual 17/94 with a publicly released draft available from the HOSDB website) it is expected that the completed manual will: give guidance on recommended minimum image quality, be more user friendly, and give guidance on how to test the systems once they have been installed.

R 2.4. Review the location and purpose of all CCTV cameras. Owners of systems should undertake a review of all the CCTV cameras in public space use, detailing their purpose and establishing if they are fit for that purpose.

R 2.5. Establish a mechanism such as a Governance Body to ensure that there is the correct balance between cameras being used for police / crime use and other uses. This refers to the structure we have to set up with the key stakeholders and detailed in the chapter on Partnership Working.

R 2.6. The current installed camera base of Pan-Tilt-Zoom (PTZ) camera technology cannot be used by a variety of users for different purposes simultaneously. Therefore, there is a need to establish the technical requirements and possible technical advancements that would allow multiple purpose use whilst maintaining fitness for purpose but also reducing the cost.

R 2.7. Clear recommendations on what is required from CCTV systems if they are to be used by the police for investigation, detection and prosecution of criminal cases is needed. There is a role here for forces, in conjunction with the Crown Prosecution Service (CPS).

R 2.8. In order to scope the issue of coverage across the country, consideration should be given to mapping out where the cameras are in order to produce a holistic analysis, identifying any weaknesses in the coverage, [profile the coverage against the National Intelligence Model (NIM) and National threat assessment models such as known crime spots, anti-terrorism / serious crime, intelligence, and specific targets of a financial or strategic importance]. To have strategic value, this would need to be a national exercise. Future deployment should be in accordance with NIM principles.

R 2.9. Local CCTV owners should consider the value in gathering best practice and job profiles, prepare standard local operating procedure/guidance documents, complete with generic role profiles, preferred Key Performance Indicators, model business cases, and process and stakeholder mapping/interfaces. Any documents associated with this work would in practice serve to supplement and complement the advice currently being prepared by the NPIA on

CCTV & imaging best practice for police. Consideration should be given to this work being conducted as a standalone project when implementing the strategy.

R 2.10. Better strategic guidance and governance is needed overall and consideration needs to be given to establishing a process for developing such guidance and better avenues of dissemination and cascading of best practice, from central Government, through the police and local authorities.

R 2.11. Better inter government department co-operation and local government working would be in the best interests of all who operate CCTV for public safety and for those who rely on CCTV for evidential purposes leading to conviction, including the police and CPS.

R 2.12. Extend the remit of town centre CCTV schemes to monitor railway, tube stations, and where possible onboard CCTV from buses, tube and train carriages. Extending to shopping centres, football stadiums, arenas and other areas of public convenience thus creating a hub for public space CCTV. This should be co-ordinated by partnerships at a local authority level.

CHAPTER 3 : REGISTRATION / INSPECTION / ENFORCEMENT

3.1. INTRODUCTION

The Data Protection Act 1998 (DPA) is the principal legislation that impacts on the operation of public space CCTV systems. Legal issues relating to the use of CCTV and with regard to matters of privacy and data protection and human rights legislation are handled by the Information Commissioner's Office (ICO). The ICO, as the regulatory body, has overall responsibility for data protection issues. Within this, the Information Commissioner has legislative authority to inspect CCTV systems, including those used for crime reduction and community safety, to ensure that they are fit for purpose under the DPA.

3.1.1. THE DATA PROTECTION ACT 1998 (DPA)

In terms of compliance with the DPA, the Information Commissioner must enforce the principles within the DPA around personal data and its fair processing, proper data control, accuracy of personal information, and the duration and retention of personal data.

A further aspect of the DPA is that it allows the Information Commissioner to produce, where appropriate, codes of practice providing guidance in connection with the legislation. It was determined that, because of the increasing and widespread use of video surveillance systems, a code of practice covering this field would be beneficial.

The Information Commissioner published a CCTV Code of Practice in July 2000, containing a number of recommendations regarding his interpretation of the Act in relation to CCTV.

The code, as produced, deals with surveillance in areas to which the public have largely free and unrestricted access (for example town centres and large shopping complexes) because there was a particular concern about a lack of regulation and central guidance in this area.

The Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place. It sets out the standards that must be met if the requirements of the l998 Act are to be complied with.

The Information Commissioner has the power to issue enforcement notices where he considers that there has been a breach of one or more of the Data Protection principles. An enforcement notice would set out the remedial action that the Commissioner requires to ensure future compliance with the requirements of the Act. In the case of CCTV, the Information Commissioner will take into account the extent to which the users of such surveillance equipment have complied with the CCTV Code of Practice when determining whether they have met their legal obligations when exercising his powers of enforcement.

Although the Data Protection Act 1998 covers other uses of CCTV this Code addresses the area of widest concern. Many of its provisions are relevant to other uses of CCTV.

However, this Code is now being revised, as certain principles contained within it no longer fit the emerging technologies.

There are some existing standards that have been developed by representatives of CCTV system operators and, more particularly, the British Standards Institute (BSI). But while such standards are helpful, they are not legally enforceable.

The changes in data protection legislation meant that for the first time legally enforceable standards were applied to the collection and processing of images relating to individuals.

3.2. KEY ISSUES

A number of important issues were highlighted during the course of consultation with stakeholders. These included:

- Lack of direction regarding registration and provision of new or existing systems;
- The DPA does not require CCTV systems to be registered – this is considered to be at the heart of all the problems associated with the extent of provision, the types of technology across the piece, and the regulation of schemes more generally;
- The Information Commissioner currently has no legal authority to enforce the Code of Practice;
- No effective systems for registration of CCTV are in place. These would, if effective, include types of system, purpose and coverage etc;
- Cameras that are poorly maintained and not fit for purpose;
- Lack of regulation governing the use of private CCTV systems;
- Failure by many local authorities to link CCTV into their general planning considerations;
- Procurement processes are piecemeal and often do not lead to or provide systems that are fit for purpose either technologically or otherwise – this is often compounded by inadequate direction or management;
- Inadequate and often unclear formal advice on replacement of existing systems and what principles they need to adhere to for registration etc;
- Scheme procurement and installation not driven by user requirements but by the industry/salesmen;
- No central register of CCTV systems nationwide;
- Significant issues around licensing (a Security Industry Authority (SIA) responsibility) and the Information Commissioner's lack of resource to enforce every public space system;
- Lack of clarity about the role of the Surveillance Commissioners under RIPA;
- Problems arise from the fact that the Information Commissioner cannot enforce inspection; however, he can encourage users to deploy best practice, i.e.: signing up to an informal code of accreditation issued by a third party;
- The Information Commissioner regulates the way in which personal data is "processed", but not the cameras themselves. This is regarded by many as inadequate.
- The licensing and registration process is fraught with difficulties, particularly over exemptions and compliance with notification.
- There are questions surrounding whether or not systems installed can be seen to be 'fit for purpose'-

there is no standard method of quality assuring new or established systems, or for policing them, and this is seen as counterproductive;

- There are many additional issues regarding standards of retention, systems, siting and positioning. These can be considered under a general 'standards' issue where a system of enforcement is needed to ensure standards are being complied with.

3.3. CONCLUSIONS

It was evident from the review team's consultation that there was widespread concern about the inadequacies of current legislation in place to address the shortcomings around enforcement.

In particular, the DPA does not confer sufficient regulatory powers on the Information Commissioner to ensure compliance with the registration and licensing processes, as well as change of use. Without appropriate and effective legislation, conferring adequate powers on the relevant regulatory bodies, this will remain and the situation will not improve.

3.4. RECOMMENDATIONS

R 3.1. The role of the Information Commissioner needs to include greater powers to enforce licensing requirements of systems and people and needs to be clearer;

R 3.2. Consideration needs to be given by the Home Office to the creation of appropriate legislation to tighten the regulatory deficiencies where these are shown to be a problem. This should in practice entail the development of more legislative powers to inspect CCTV systems; consideration should also be given to whether or not there is a need for any new legislation to tackle invasion of privacy with regard to both public and private CCTV – the latter remains a grey area in many respects;

R 3.3. From the perspective of the Information Commissioner, there needs to be greater understanding by all about the issues around public protection in the context of the DPA and the Human Rights Act;

R 3.4. Better use should be made of existing legislation (the DPA) to drive up standards across the industry and the use of public space CCTV;

R 3.5. CCTV should be considered in planning regulations and licensing, therefore satisfying inspection, regulation and enforcement by capturing CCTV within the licensing laws that currently exist.

R 3.6. A system of registration is needed and an initial step towards this would be to create a database listing all CCTV schemes. Such a database would provide information such as location of cameras, their coverage, their intended purpose, equipment details, details of the registration with the DPA, owners' details. This would enable an authority charged with inspection to quickly and accurately identify non-compliant systems and take action to enforce compliance.

R 3.7. Develop a mechanism to allow CCTV standards to be enforced.

CHAPTER 4 : TRAINING

4.1. INTRODUCTION

The use of CCTV in the police service as an evidential tool has grown significantly over the past 10 years, and today provides a higher percentage of investigative evidence than any other form. Possibly, due to its easy accessibility in the form of analogue tapes, the need to provide officers with the skills to retrieve and compile the evidence has not historically been an issue. However, the increasing use of digital CCTV has changed a fairly simple task into one of complexity, which requires technical knowledge, technical skills and understanding.

It is critical that the standards of training and associated procedures are complementary, thus ensuring the chain of evidence from capture right through to the court hearing is to the highest standard.

In addition to the police service, the users and operators of the systems are also an important link in the evidence chain, and the skills mentioned above should also apply to all associated with CCTV.

4.2. KEY ISSUES

There is inadequate training for all staff engaged in CCTV. There are currently no uniform training standards that apply to all CCTV staff. The SIA Licence requirement for CCTV training addresses minimum training requirements for those public CCTV operators that require a SIA Licence and the Skills for Security National Occupational Standards goes further in raising standards in CCTV operators and security consultants. The lack of uniformity though is leading to a disparity between the skills ranges of staff. It has been identified that the proper training for all users of CCTV is crucial to its successful deployment and effective use. A system can be rendered ineffective if the system user is unsure how to fully use the system, and of what relevance the images might be. Further, the inadequate, and, in many respects, total lack of training for operators means that some systems and software applications installed in the control rooms are seldom or never used. It is clear that in many cases, CCTV is not being used to its full advantage.

4.2.1. SIA LICENSING

The Security Industry Authority (SIA) licensing regime which came into effect on 20 March 2006 has made it illegal to work as a public space CCTV operator without an SIA licence. The licensing requirement applies to contracted-in staff only and has had the effect of imposing a training requirement on all front-line staff. The licence requires that staff are trained to the right level. The SIA licence requirement has had the effect of raising training standards. This will help to achieve minimum standards for CCTV operators, but the licence remit is perhaps not as wide as is necessary to raise standards across the board. The requirement does not extend to police officers; during consultation, it was evident that police officers, who are dealing with CCTV footage and working closely with control rooms, receive no formal CCTV training. The partnership between control room staff and police officers is an important one, which needs to be built upon, to create a more joined up approach to CCTV. The partnership between CCTV control rooms and the police is key in the successful deployment and gathering of evidence.

It is evident from consultation with practitioners and users that there is confusion around who falls within the 'licensable' remit. For example, police staff are not specifically included and it is not clear if they fall under a broader category of police who are then exempt from the licensing requirement. If it does not apply to police staff, this will lead to further skills and training gaps. Another issue is that the SIA only 'recommend' that the licensing extends to in-house staff. Although some CCTV control rooms have taken the approach to train all staff to the SIA license standard, this is not obligatory and so the level of training and skills will differ from one control room to the other, depending on individual control room initiatives and funding. Finally, the SIA licensing does not extend to cover the installers of the CCTV systems, and although this function has been identified as being a key one in the roles associated with CCTV, the SIA has no influence over installers and in the short term will not be able to extend its boundaries to include installers without further legislation.

4.2.2. CCTV MANAGERS

All levels of CCTV users need to undergo some form of training. It was pointed out to the review team that town centre CCTV managers may not have come from a CCTV background. They may not therefore be aware of the training issues and needs, which in turn create a disparity in the resources and training opportunities that are open to CCTV staff from one control room to another.

4.2.3. LENGTH OF TRAINING

Another question raised is the length of training required. Often an operator of CCTV might only be using the equipment for two hours a day. This raises the question of whether such operators need to be trained to the same level as a full time user.

4.3. CONCLUSIONS

It is clear from the previously detailed issues that there is a need for a uniform and comprehensive set of standards for training of all those involved in the use of CCTV; from operators to the police to the courts. It is equally clear that we have a golden opportunity now to develop a multi-agency approach. The provision of such a programme will lead to a wide understanding of the needs and issues for each role, and aid progress towards partnership working. Effective training will also make better use of CCTV.

The SIA has made a move towards raising minimum standards. However, it is clear that there are gaps left by the licensing requirement that must be filled. The fact that the police are exempt from this requirement leaves a real training gap, especially within the police service. Similarly, general opinion is that all staff need to be trained, from operators through to management. Currently, it is only the operators of the system who require a licence.

There are a variety of different bodies currently working on training and developing training standards. There is a need to bring these groups together and evaluate their findings and proposals.

In order to raise standards and provide a consistent use of CCTV, a detailed end to end process needs to be articulated and made clear to all those working in the field. There needs to be a focus on detailing each profile, laying down the areas of development and identify how each profile ties in with the wider end to end process.

There is a need to include an appropriate level of training in the current legislation surrounding CCTV (e.g. Data Protection Act, RIPA, Human Rights Act, and Freedom of Information Act). This is one of the areas to be covered by the SIA licensing requirement, but there is concern over the uniformity of training standards across the different providers of training for the SIA licence.

4.4. RECOMMENDATIONS

R 4.1. With regard to operator licensing, there is a need for further clarification from the SIA as to the requirement and how far the remit extends. There should be a full and comprehensive list of those roles that are not covered by the licensing requirement, and consideration given to how to fill these.

R 4.2. Ultimately, there is a need to set down minimum requirements, alongside those set down for SIA licensing. In the short term, it is advisable to encourage CCTV schemes to extend the SIA licensing requirements to all those working in the CCTV environment as an example of good practice.

R 4.3. In the long term what is needed is a fully comprehensive and inclusive accredited training programme. It is recommended that the National CCTV Strategy Project Team work closely with the ACPO CCTV Training Working Group, who are currently looking at developing a training programme in conjunction with Skills for Security, Skills for Justice, NPIA and stakeholders such as the police and CCTV Town Centre Managers. The end result should be a training strategy that can be adopted as part of the wider CCTV strategy. There is also a need to consider who might accommodate the responsibility for a National Training Strategy and whether a higher authority or board should be set up to coordinate the provision of such training (e.g. ACPO, Home Office, Local Forces etc.) to local level.

R 4.4. Once a training programme and standards have been agreed and put in place, it is proposed that there needs to be a method of dissemination of ideas and issues to all users of CCTV. It has been suggested that a national forum, where members can discuss the topic be set up, to provide closer partnership working (see also chapter on Partnership Working). This will provide a way of disseminating information on training to local level, and creating better communication between CCTV partners.

CHAPTER 5 : POLICE USE OF CCTV

5.1. INTRODUCTION

A number of research projects have been undertaken into the effectiveness of public space CCTV, whilst this research has been useful in determining the crime prevention and deterrent effects of the technology, little formal research has been undertaken to establish the impact that CCTV has on the investigation of crime. Those examining the issue therefore have to rely on limited research and anecdotal evidence provided by operational police officers.

Despite the lack of formal research evidence, there appears little doubt that the police service utilises CCTV images in the investigative process and has had considerable success in doing so. High profile cases have reinforced the investigative benefits of CCTV which not only assist police officers in the identification of offenders but also help to establish the nature, location and time of the crime.

The extent of the country's public space CCTV coverage presents the police service and those agencies with responsibility for public safety with significant opportunities to deter offenders, identify crimes in progress, monitor the activities of suspects and provide evidence to support the prosecution process. The principle of public space CCTV surveillance has general public support allowing coverage to be extended as and when the operational case justifies its expansion.

5.2. KEY ISSUES

5.2.1. VOLUME AND CAPACITY

When CCTV was initially introduced into the UK, images were recorded onto VHS tapes and replayed using technology that was relatively easy to use. Although the quality of the images often left a lot to be desired, police officers had little difficulty in obtaining the relevant VHS tape and viewing the evidence at the police station.

The proliferation of CCTV systems, whilst presenting the police with evidence gathering opportunities, also raised issues in terms of their capacity to recover the evidence and review the tapes to establish whether they contained relevant evidence. In cases of serious crime where investigative costs are significant, the financial overhead relating to the recovery and examination of CCTV is not so great. In high volume, less serious crime where the police have insufficient resources to undertake extensive investigations, the financial overhead relating to CCTV recovery and examination is proportionately greater. This is particularly so if the recovered CCTV image is of poor quality and adds nothing to the investigative process. Unfortunately, police officers cannot tell whether the CCTV is of no evidential value until they have recovered and viewed it. Finally, almost all the footage recovered by the police, whether it is of use or not, has to be retained by the police until after the trial and in many instances for several years afterwards.

The CCTV expansion programmes outlined in the introduction provided funding to greatly increase the number of CCTV cameras in UK towns and cities. Placing thousands of cameras on the streets, each with the capacity to constantly monitor the local environment was bound to increase the workload of the police.

Unfortunately, whilst funding was made available for cameras, no additional funding was provided to the police to enable them to increase their capacity to recover and view CCTV images or to respond to live incidents that were being monitored by CCTV operators. Inevitably, the police have been unable to respond to all incidents viewed by CCTV cameras and have been forced to prioritise the incidents they attend.

5.2.2. DIGITALLY RECORDED CCTV

Digitally recorded CCTV systems have presented the police service with additional challenges. The absence of standardisation in relation to down load formats has resulted in the development of hundreds of different systems, many requiring unique software to download the image into a viewable format. Recovery of some forms of digitally recorded CCTV has become a specialist function requiring specific technical skills. This has significantly increased the cost of CCTV image recovery making it prohibitively expensive in some cases. Many forces have failed to develop the capability and capacity to recover digitally recorded images resulting in evidence being lost.

Additional cost occurs as a result of the CPS and Courts being unable to receive digital images in the format recovered by the police. It is not unusual for a digitally recorded image captured on a DVD or CD to be copied onto a VHS tape so that it can be viewed by criminal justice agencies.

In addition to the complexity associated with the recovery of digitally recorded images, the cost of storing the images has resulted in many system administrators reducing the amount of time the images are retained before being over recorded. This creates further operational difficulties for the police as they have less time in which to recover the images. Copying a digitally recorded image to an analogue format is not only costly but also reduces the quality of the image.

Despite the current difficulties experienced, digitally recorded CCTV does present significant operational advantages if properly managed. The ability to move images electronically and utilise automatic searching techniques has the potential to increase operational effectiveness and reduce the time currently spent recovering CCTV images. A co-ordinated approach to the developing technology will allow the police service to make greater use of the technical benefits associated with digitally recorded CCTV.

5.2.3. STRUCTURES AND RESOURCES

Where specialist resources have been made available, it is often the case that the individuals concerned face significant demands on their time as digitally recorded CCTV images become more common. Many have to prioritise the work that they are asked to do, resulting in some images being over written before they can be recovered.

The police service as a whole has yet to establish the most appropriate way of managing the specialist staff required to undertake this role. Where dedicated staff have been provided, there is little commonality in the way they are organised with staff variously working under the umbrella of Technical Support Units, Computer Crime units, High Tech Crime Units or stand alone teams of CCTV Retrieval and Intelligence Officers. This lack of standardisation makes it difficult to co-ordinate activity across the police service and identify best practice. By contrast, there is a high degree of standardisation in relation to the recovery and analysis of the more traditional forms of identification evidence such as fingerprints and DNA with well established Forensic Investigations teams in every UK Police Force.

The amount of money invested in the recovery and analysis of fingerprints and DNA is substantial and contrasts significantly with the resources invested in the recovery and analysis of CCTV evidence. Every force has a number of trained Crime Scene Investigators (CSIs) and additional funding was provided by the Home Office to develop every force's capacity to recover and analyse DNA from volume crime scenes.

There is a need for the police service to determine the most appropriate model for managing the recovery and analysis of CCTV evidence. Consistency of approach will allow for national standards to be developed and applied and will assist in determining the skills and training required to support those who undertake the role. Whether CCTV recovery and analysis becomes another forensic discipline or sits within a High Tech Crime Unit has yet to be determined. However, without an appropriate model of delivery and management structure, the recovery and analysis of CCTV is likely to remain an ad hoc function that is under resourced and consequently less operationally effective.

5.2.4. TRAINING

CCTV has yet to feature in the National Competency Framework. Although this is being addressed, it illustrates that the retrieval and compilation of CCTV evidence is still not a recognised 'practice' and not incorporated into officers' roles.

The lack of a standardised approach to the recovery and analysis of CCTV images has meant that there is no recognised training regime for those engaged in the activity. The Home Office Scientific Development Branch (HOSDB) and Metropolitan Police Service have recently run six training courses in the recovery of digitally recorded CCTV evidence and this has allowed for the development of a cadre of officers who can be called upon to assist any force with the large scale recovery of CCTV evidence. However, the HOSDB is not a training organisation and should not have the responsibility for training officers to undertake this function. There is an urgent need to develop an accredited training course for those engaged in the recovery and analysis of digitally recorded CCTV evidence.

NPIA as the central provider of police training currently provides training for a range of forensic disciplines including Technical Support and High Tech Computer Units and Crime Scene Investigators (CSIs). In addition to training delivery and design they develop new techniques and keep pace with new technology. In relation to CCTV no such 'home' exists and it is not recognised as a forensic discipline despite it becoming an increasingly complex specialist area.

5.2.5. PERFORMANCE STANDARDS

Forensic Investigation Units are subject to national performance measures and inspection by Her Majesty's Inspectorate of Constabulary (HMIC). The Home Office Police Standards Unit collects and publishes performance data relating to the recovery of DNA and fingerprints, the recovery rates of each CSI and the contribution this evidence makes to the successful detection of crime. There is nothing similar in relation to CCTV evidence. Lack of standards, measurement and inspection exacerbates its standing against other forensic disciplines. Without any quantifiable data its success as an investigation tool remains, to a great extent, unknown, which severely affects the investment forces are prepared to contribute in terms of its development.

It is likely that the police service is missing significant investigative opportunities by not investing sufficient resources in the recovery, analysis and Investigation of CCTV evidence. Research needs to be undertaken to establish the relative benefits of fingerprint and DNA recovery, analysis and investigation in comparison

with CCTV recovery, analysis and investigation. In the absence of additional resources, there may be a strong business case to realign some staff currently engaged in traditional crime scene evidence investigation and use them to investigate CCTV evidence.

5.2.6. INTEGRATION INTO THE POLICING FUNCTION

Most public space CCTV systems are owned and managed by local authorities. Whilst this arrangement ensures the cameras are locally managed and monitored, difficulties arise if there is poor co-operation and communication between the CCTV monitoring staff and the police officers who are required to respond to the images. Those forces that provide police radio communications (Airwave), share local intelligence and provide feedback regarding the usefulness of the images enjoy more productive relationships with the CCTV operators and ensures that the CCTV system is more closely integrated into the policing function.

There is a need to develop a consistent approach to issues such as intelligence sharing protocols, the use of Airwave radio communications and the involvement of the CCTV monitoring staff in the intelligence gathering requirements of the local police area.

Currently, there is a lack of consistency of approach in the manner in which police forces co-operate with local town centre CCTV systems. Invariably, it is left to the local police commander to determine whether intelligence is shared and how closely the CCTV system is aligned to the policing function. This lack of a corporate approach has often been criticised by town centre CCTV Managers who face a variable approach dependent on local determination. In addition, continued investment in terms of monitoring costs, systems upgrade and expansion can only be justified if the CCTV system is seen as effective. In the absence of feedback from local police commanders, it is often difficult to determine whether the local town centre CCTV system is performing adequately and justifies the expense associated with it. Adequate feedback as to the operational usefulness of CCTV images is required if local investment in CCTV is to be maintained

Whilst we have mainly focused on the CCTV recovery, analysis and town centre CCTV liaison, there are many other roles within the police service that are also closely associated with CCTV. These include crime prevention advisors, specialist CCTV Investigators, crime analysts, intelligence officers, CCTV librarians and a host of others. In many ways, the police service has not recognised the need to develop these roles with specialist CCTV training, promotion of national role profiles or greater integration between the various roles affecting the CCTV chain.

One example of greater integration between CCTV investigations and crime prevention is that, unlike the traditional crime scene evidence, the quality and usefulness of future CCTV evidence can be dramatically improved by feeding back the results of CCTV investigation to the crime prevention officers through to the system owners, thus correcting defects in current systems, improving the quality of the CCTV installation, and improving future evidence.

Similarly, although the advantages of specialist CCTV investigators have been recognised for many years, and the Management of Volume Crime Advice 2004, recommends dedicated specialist CCTV investigators integrated into the Volume Crime Management Model, there is little evidence of widespread adoption of these measures.

5.2.7. SERIOUS AND ORGANISED CRIME AND TERRORISM

The current CCTV structure has been based around volume crime that occurs mainly in town centre and urban areas, determined by localised crime and disorder issues. The majority of cameras have not been placed in positions which may be required for the prevention and detection of serious and organised crime and counter terrorism. This is not to say that the current camera infrastructure does not assist, because it clearly does. The use of CCTV in the post incident analysis of the London bombings are but one example of their value. Consideration needs, however, to be given to strategically placing cameras in areas which would probably not accord with local crime and disorder strategies but would be of significant value to pre and post major crime investigations.

CCTV coverage of key economic sites across the UK also needs to be identified and addressed. Clearly the majority of industrial sites are not covered by town centre CCTV systems and therefore the development and control of such systems will need to be considered.

CCTV has played an important role in the prevention and investigation of terrorist incidents and a range of tactical options have been developed to ensure that the current CCTV infrastructure is used to maximum effect. There will be a need to take into account the current tactical options and additional ones that are likely to be developed as different technologies are used to complement CCTV systems. The recovery of large quantities of CCTV material presents all police forces with a challenge in terms of both the collection and analysis of the images. Processing and analytical examination of CCTV images for counter terrorism investigations has improved considerably in recent years and with the formation of a dedicated CCTV investigation team within the Counter Terrorist Command has the potential to improve further. A cadre of specialist personnel trained in the recovery of CCTV images is now available on a mutual aid basis to police forces to assist in CCTV recovery operations. Although the image retrieval cadre was developed for terrorist investigations, it has been used to good effect in major crime investigations. Consideration needs to be given to extending the assistance available so that it covers the viewing and analysis of the CCTV in addition to its recovery.

Consultation has taken place with the Counter Terrorist Command of the Metropolitan Police (SO15), the Security Services, Home Office Terrorist Protection Unit, Home Office Scientific Development Branch, Serious and Organised Crime Agency and individuals representing elements of the national transport infrastructure to consider the future use of CCTV in counter terrorist operations. National security considerations prevent a detailed description of their requirements appearing in this document.

5.2.8. IDENTIFICATION TECHNOLOGIES

Development of digitally recorded CCTV will enable identification technology to be used in conjunction with town centre CCTV cameras and as a consequence improve the effectiveness of the camera infrastructure. ANPR is a good example of camera technology being used in this way.

5.3. CONCLUSION

The development of CCTV in the UK has resulted in a public space CCTV surveillance infrastructure that is the envy of many police forces around the world. The operational benefits of such a system are considerable, especially in the investigation of crime.

The proliferation of CCTV systems, whilst presenting the police with evidence gathering opportunities,

has raised issues in terms of their capacity to recover the images and review the tapes to establish whether they contain evidence. The development of digitally recorded CCTV evidence, whilst offering potential opportunities, has added a degree of complexity to the issue of image retrieval and presented further challenges to the police service.

The development of the technology has outpaced the ability of the police service to respond to the operational opportunities. The lack of a national strategy or a co-ordinated approach to the development of CCTV has led to an ad hoc response that is less than adequate and fails to maximise the significant potential afforded by CCTV.

The police service needs to review its approach to CCTV and establish the operational processes and management structure that will ensure it makes better use of CCTV's surveillance capacity. Performance standards will produce quantifiable data allowing the effectiveness of CCTV evidence to be judged and integration of CCTV into the policing function will allow for intelligence to be shared with those responsible for monitoring the images.

5.4. RECOMMENDATIONS

R 5.1. Image retention periods should be standardised and should relate to the operational purpose of the CCTV system.

R 5.2. The Crown Prosecution Service and Court Service should develop the capacity to view digitally recorded CCTV evidence

R 5.3. The police service needs to develop an organisational model for managing the recovery, analysis and investigation of CCTV evidence. The model should be resourced appropriately.

R 5.4. The specialist nature of CCTV evidence recovery, analysis and investigation should be recognised and appropriate training developed.

R 5.5. The police service needs to review its internal operational processes and management structure. In effect, it needs to determine 'ownership' within each force for CCTV and consider its links to existing forensic disciplines and its future training and development requirements.

R 5.6. Performance standards similar to those that support other forms of crime scene evidence should be developed in relation to CCTV recovery and analysis.

R 5.7. Research should be undertaken to determine the relative benefits of fingerprint and DNA in comparison with CCTV.

R 5.8. Protocols should be developed allowing the use of Airwave radio in Town Centre CCTV Control Rooms and the sharing of intelligence between the police and Town Centre CCTV monitoring staff.

R 5.9. Protocols should be developed that require the police to provide feedback to Town Centre CCTV Managers as to the operational usefulness of CCTV images.

R 5.10. The police service needs to consider the development of a CCTV capability to support serious and organised crime, counter terrorism and the protection of key economic sites across the UK.

R 5.11. The effectiveness of the CCTV Image Retrieval Cadre should be further enhanced by the provision of regular training, the development of standardised procedures and the identification of suitably qualified individuals who can provide the Senior Investigating Officer with expert advice relating to the management of large scale CCTV recovery operations.

R 5.12. A cadre of personnel, available on a mutual aid basis and trained in the analysis and viewing of CCTV images, should be developed to assist forces with the examination of large volumes of CCTV material recovered during major crime and terrorist operations.

CHAPTER 6 : STORAGE / VOLUME / ARCHIVING / RETENTION

6.1. INTRODUCTION

It has long been accepted that CCTV recordings should routinely be kept between 28 and 31 days before being re-recorded over. This time period allowed the police the opportunity to recover CCTV evidence and respond to lines of enquiry that were not known at the time the incident was reported. It also assisted with the video tape recycling procedure and ensured that the tape would not be used, day in, day out.

Since the introduction of digital CCTV systems, some system owners have moved away from the 28 and 31 days figure, to periods as short as 14 days. This has resulted in significant resource implications for police, as they struggle to collect the digital CCTV before the footage is overwritten. This is extremely important in terrorist investigations, where extended periods of between 14 and 31 days, are often required.

The police have therefore re-iterated their need for 31 days of storage in the digital CCTV era, with the proviso that the recording quality should not be reduced or compromised, which could result in the recordings not meeting the fit for purpose criterion. The Information Commissioner supports the view that, as 31 days was the recommended period when VHS systems were employed, it should then follow that 31 days should remain the recommended period when digital CCTV systems are employed.

The volume of storage required on this scale understandably brings with it many problems. Analogue CCTV systems require large amounts of VHS tapes, which have to be securely stored in appropriate conditions (for instance within certain temperature and humidity limits).

Large scale digital CCTV systems require due consideration of the specialist housing of the equipment racks and hard disk storage, as the digital CCTV recording equipment creates additional noise and cooling requirements beyond those of their analogue counterparts.

Some large CCTV schemes may have several thousand video tapes in circulation or several thousand gigabytes of hard disk storage in use. Up to this point, these are self contained systems and managed by the CCTV operators.

There are significant problems when the recordings are required for evidence. In the first instance, once it is known that the footage needs to be secured, a decision needs to be made on the quantity required, which can vary between a few minutes, a few hours, a few days or a few weeks. In serious and terrorist offences, police may need large amounts of data to be secured as they may be unsure at early stages as to what may be relevant. Sometimes the amount of video secured is affected by disclosure rules.

In order to protect the footage in analogue recordings, VHS tapes are removed, stored and replaced by new tapes. In digital systems the material is exported from the system. Whilst most events can be exported to CD and DVD, problems arise as to playback throughout the CJS. Larger periods of time required for major/serious incidents and in the extreme terrorist incidents, expose the difficulties associated with digital systems, which either require long exports from the systems or the swapping out of hard disks or complete systems.

The problems in viewing this material throughout the CJS have been highlighted in other chapters. Other procedural and logistical problems exist as to who should be responsible for storing the recordings throughout the varying stages of the CJS process. It is important to ensure that the material is stored securely, and accessible when required, and the material is disposed of when it is no longer required.

Town centre CCTV managers have reported that large amounts of material have been put aside and apparently never used by the police and CJS. This raises concerns that may be missed opportunities in detecting crime, or lack of feedback as to the progression of the investigation and notification that the material is no longer required.

On some occasions, such as cold cases and trials undergoing appeals, CCTV material has to be archived for a number of years. The need therefore to carefully plan and resource future archiving capability is crucial to the continuing storage and rapidly increasing volume of CCTV data.

Increasingly, concerns have been raised as to how the CCTV material will be played back in 10-20 years time. It is not known what the physical state of the media will be at that future point. In addition, the rate of technological change and proprietary nature of digital CCTV material will also affect the ability to play back the material. It may well be impossible to find the correct software and hardware to do so.

6.2. KEY ISSUES

- It has been seen that there is a large disparity between systems, on the way that storage, archiving and retention is handled. Questions surrounding storage concentrate on what to store, how to store, and how long to store. Currently, there remain large variations in standards with differing lengths of periods of retention and differing formats. An agreed standard must be reached, based on sound technical advice.
- How long images are to be stored for will depend entirely on how long the evidence is needed in the opinion of the police and the CPS.
- Degradation – material kept in its original format is subject to problems with degradation. Conditions of storage need to be agreed to keep degradation to the minimum, even when storage conditions are optimised, there is considerable uncertainty as to the durability of most digital media (including CD/DVD) over the long term.
- Retrieval – when images are stored, there are problems associated with accessibility and retrieval at a later date. Linked with this is the need to develop better systems whereby access to data/images is faster and simpler, such as the electronic retrieval of images.
- When data is stored, consideration must be paid to data protection and audit issues. When a request for access to data is made, there needs to be a system of control and audit, in order to protect the images and the requestor.
- CCTV systems are not necessarily designed with the police in mind, and therefore the way that images are managed might conflict with police views on storage and archiving.

6.3. CONCLUSIONS

Serious concerns have been raised about the best methods of dealing with the huge amounts of CCTV material retained, used, stored and archived within the CJS. Existing methods of removing/exporting material to CD, DVD and hard disk, are not consistent with other methods of handling data. Non standard proprietary formats will be difficult to play back in future years.

6.4. RECOMMENDATIONS

R 6.1. The police service needs to be provided with CCTV retention and disclosure guidance. The NPIA are currently working on a document that offers guidance on the police use of digital images. It is hoped that this will go some way in addressing these issues. HOSDB should provide technical advice and guidance on the best approaches for the short, medium or long term (including archiving) solutions to the access and storage of CCTV.

R 6.2. CCTV operators, police and CJS agencies should determine respective roles and responsibilities in the short and long term retention (including archiving) of CCTV material.

R 6.3. Complete "camera to archive" network access and data archiving methods need to be evaluated.

CHAPTER 7 : CCTV NETWORKS – LIVE AND STORED

7.1. INTRODUCTION

Most CCTV installations in the UK are monitored and recorded locally.

Whilst some larger systems may have several hundred cameras, they are still usually monitored and recorded in the town centre CCTV control room.

In some cases, limited camera views from town centre CCTV systems on individual incident by incident demand are transmitted live to the nearest police BCU control rooms (and in some instances their main/major control rooms). Such transmissions are very useful in the deployment of police to an ongoing incident.

Only in a few of the more recent installations is there remote access to previously recorded (stored) video. Consequently, on almost every occasion where police need to view CCTV material, they first have to attend the venue, Most town Centre CCTV control rooms provide facilities for officers to view the material, but for large/serious investigations and for the occasions where there are no viewing facilities the police have to seize the data, and then find a method to view the data and/or have it converted to another format (currently VHS). This is all prior to assessing if the CCTV has even captured the event, or if it is of significant value to warrant its retrieval. This is a resource hungry process, and for the reasons discussed in other chapters, one that the police are increasingly ill equipped to deal with.

The delays and difficulties outlined above need not arise if the live and stored CCTV systems were networked and the CCTV material was easily accessible. This would make CCTV usage equivalent to most people's experiences of access to other forms of information held on their local network or via the Internet; an indispensable requirement of modern day working. Appropriate access and permissions restrictions will need to be developed relating to the access of the images.

Whilst it has always been possible to connect individual CCTV systems together, it is only recently that this has started to happen in earnest, due to digital CCTV systems (based on IT technology) naturally lending themselves to being connected to each other over networks. Up until now the barriers that existed included the capability of the IT networks to handle the large amounts of data that is required to display CCTV effectively. With improvements in technology, the costs continue to fall, making it increasingly viable to connect CCTV systems together.

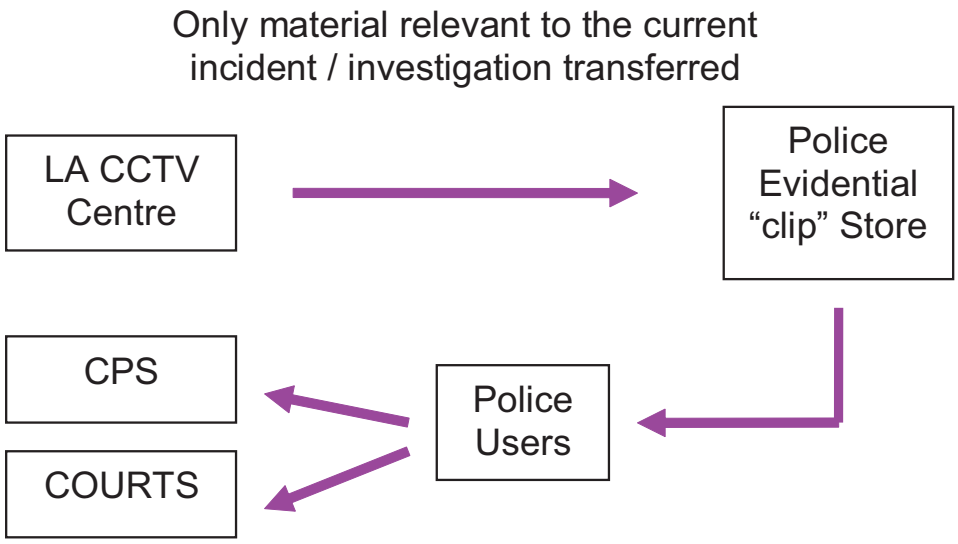
The first systems to do so have been commercial, where large companies want to monitor their entire organisation from a central location, or commercial premises and have subscribed to remote monitoring companies

7.2. KEY ISSUES

There are many advantages to connecting individual CCTV systems together;

- Police have immediate access to live and recorded CCTV material and the police can use the more extensive live CCTV to help inform their decisions as a live situation develops.
- In the event of a recent crime being reported the police can begin to remotely investigate by replaying the stored CCTV whilst deploying their officers on the ground.
- Advances in police communications could lead to CCTV images being passed to the police on the ground via mobile data so they had a clearer description of who they were looking for.
- When suspects have been arrested the CCTV would be more easily available and could be played back using a standard PC in the interview room. This would reduce the number of occasions when suspects had to be bailed as the CCTV material had not been collected or available in a viewable format.
- CPS or defence solicitors could log on to the network using their own pc's and view the material, thus eliminating the need for multiple copies being made and held, and finding facilities to play them. Finally, the material could be played back over the network in Court

An example of a CCTV Network



Consideration needs to be given to the expansion of the networks to include CCTV from shopping centres, transport and commercial CCTV schemes.

Consideration should also be given to the police, with the consent of individual users having limited and prescribed network access to smaller CCTV systems, to allow them to investigate crimes carried out against those users, in their own premises, such as investigating a robbery at a local shop, or a burglary at a commercial premises.

Whilst there are always likely to be some privacy concerns, these should be addressed within existing laws, appropriate codes of practices, and regular review and assessment, overseen by the existing Information and Surveillance Commissioners.

Security, access and audit trails need to be stringent and continuing management scrutiny of the security, access and audit trails will be essential.

The topology and infrastructure of such a network needs careful planning, and will be most cost effective if it makes use of existing networks, such as the Police National Network (PNN) network and Criminal Justice networks. Whilst initial enquiries with the Police Information Technology Organisation (PITO) were encouraging, both the National Police Improvements Authority (NPIA) which has now subsumed PITO and CJIT will need to ensure that CCTV is included in their future network planning and strategies.

It will take some time to build up an extensive CCTV network. However consideration must be given to setting up, in quicker time, a skeleton infrastructure and a strategic network of CCTV cameras to assist in the policing of key economic sites and the investigation of major and terrorist incidents.

It is hoped, in future, as technology is developed, that such a network will allow the use of automated search techniques (i.e. face recognition) and can be integrated with other systems such as ANPR, and police despatch systems to further increase the effectiveness of CCTV.

7.3. CONCLUSION

Access to live and stored video will allow police to view footage of initial incidents as they despatch officers. This will greatly speed up post incident investigation and facilitate the use of CCTV during interviews and will allow easy access by the CJS and playback in court. After all, this is the way all other forms of data are effectively accessed and managed. This will significantly increase the effectiveness of CCTV, and reduce the technical complexities of collection, playback, delays incurred and associated costs.

7.4. RECOMMENDATIONS

R 7.1. Establish the basic network infrastructure, security and access rights and permissions by working with NPIA, CJIT and local authorities.

R 7.2. Establish the effectiveness through running pilots. A pilot is currently running in Crewe.

R 7.3. Determine the strategic network required.

R 7.4. Facilitate the connection of digital CCTV systems to the network.

CHAPTER 8 : FACILITIES IN THE CJS

8.1. INTRODUCTION

CCTV is a very valuable tool that can be used to gather evidence of crime and anti-social behaviour and can be used in legal proceedings to take action against the perpetrators. CCTV footage can and does form a major part of police evidence leading to prosecutions in court.

For prosecutors CCTV footage has proved to be vital evidence in securing convictions in a variety of cases, from car theft, and street thefts to terrorist incidents. However, there are deficiencies in the capability of technology in courts across the country, and a diverse and variable level of technological readiness, particularly in the provision of CCTV/video of evidence at trial.

The presentation of CCTV evidence at the majority of courts continues to be a problem.

One group trying to improve the current situation is the CJS Audio/Visual Strategy Group, made up of senior representatives of various CJS agencies. This group is committed to the development of audio-visual (AV) technology with the aim of ensuring the compatibility and inter-operability of systems.

Notwithstanding the ongoing work within the group, it has a difficult task. The current assessment of the degree to which the courts were geared up to present CCTV/video evidence in a professional and technologically sound way indicate that the CPS, along with HM Court Service, and the CJS as a whole, has not kept pace with the technological advancement in CCTV. More importantly, they have in place generally inadequate and less than up-to-date playback systems and procedures. It is clear that advancements in digital media for recording and playback generally have changed the face of the CCTV industry dramatically since 2001.

Where current technology has been made available, it is not apparent that the courts are making best use of that technology.

It is clear to all that image quality is only as good as the technology used to record it, and in the case of the CJS, to play it back in court.

The CJS Audio/Visual Strategy Group has been leading on the Video in the CJS component of the CJS Comprehensive Spending Review. The purpose of the review was to identify further investments and reforms necessary to equip the UK for the global challenges of the decade ahead.

8.2. KEY ISSUES

Consultations were held with representatives from the Court Service, CPS and Operation Emerald. Operation Emerald consists of staff from the CPS London and the Metropolitan Police working together to improve the capital's Criminal Justice System (CJS). One initiative identified that the increased use of CCTV evidence in the CJS was causing delays and contributing to ineffective trials. The following issues affect the successful preparation and presentation of CCTV evidence in magistrates and Crown courts:

- Inadequate and outdated playback facilities in many courts.
- Little or no guidance has been issued to court staff on the operation of technology and its maintenance; nor is the standard of training acceptable in general terms.
- Disclosure and evidence continuity rules are complex resulting in a misunderstanding in many areas of the CJS and leading to cracked and ineffective trials.
- The Court Service is failing to show all the CCTV evidence presented, because some courts lack the technology to play footage. This was highlighted in a recent National Audit Office (NAO) Report. A snapshot of unsuccessful cases presented at court were analysed. 6 out of 167 unsuccessful cases were dropped or dismissed in the UK because courts, CPS offices and defence solicitors used only VHS video equipment and did not have the correct equipment to play back the digital CCTV recordings. The NAO report confirmed that: "In order for a case to progress the police are required to obtain the evidence, arrange for it to be reformatted and provide copies for the Crown Prosecution Service and the defence" and that "this evidence needs to be available with the full file as it is often conclusive, leading either to early guilty pleas or to early dismissals, thus avoiding the additional costs of a trial".
- Organisations provide CCTV footage to police in a wide range of formats. This includes VHS, DVD, VHS multiplex recordings or proprietary digital recordings, all of which require the appropriate software and hardware to play back.
- Where the CCTV evidence is admissible, and the technology is available to play the images, a guilty plea is often forthcoming from a defendant. On these occasions it is unusual for CCTV evidence to be played in courts, even though the images would provide the court with evidence to assist in sentencing.

8.3. CONCLUSIONS

All the above could have serious repercussions for the credibility of CCTV evidence if it is not properly addressed. There is a lack of a clear end-to-end procedure. Users generally and the courts more specifically, require up-to-date guidance on best practice and minimum standards

8.4. RECOMMENDATIONS

R 8.1. Continuing consultation with the Ministry of Justice/CJS with a view to agreeing central government guidance (HO/ICO/OCJR) on minimum standards for playback systems and training of court staff.

R 8.2. Better communication between CPS and the police on the video evidence required or desired in specific cases.

R 8.3. Ongoing need for the HO to join up its work with the CJS Audio/Visual Strategy Working Group and the Operation Emerald team to bring together in a concise and clear way the actions it needs to carry out in order for improvements to be made.

R 8.4. Continue to work with the CPS more generally to ensure there is clear guidance to court staff on the requirements of video evidence at court.

R 8.5. A more joined up process, technically and procedurally. CCTV recordings should be more readily available within the CJS. Examples of joined up processes include a small pilot in Crewe, exploring the movement of images electronically throughout the CJS

R 8.6. Support initiatives in the more effective presentation of CCTV evidence in court.

R 8.7. In the event of a guilty plea, consideration should be given to playing CCTV evidence in court where this may assist the court in determining an appropriate sentence.

CHAPTER 9 : CHANGE - EMERGING TECHNOLOGIES / CHANGING THREATS / NEW AND CHANGING PRIORITIES

9.1. INTRODUCTION

We have already established that in the relatively recent history of CCTV in the UK, the underlying technology has changed dramatically. The introduction of digital CCTV systems has posed a great number of problems, initially with their acceptability, now with compatibility, retrieval and playback. Alternatively, this has also opened up a raft of new uses and possibilities. Whilst the strategy document is now trying to address these issues and harness the possibilities of the current technologies, during the course of the Review's consultation it was felt that without an element in the strategy that addressed how to deal in the future with change, there would always be an element of playing 'catch up'.

Change is not just restricted to technological change and emerging technologies. There are new threats to the public that CCTV could and should address and the new and changing local policing and disorder priorities in which CCTV plays an important role.

9.2. KEY ISSUES

9.2.1. CCTV EMERGING TECHNOLOGIES AND TECHNIQUES

The thrust of the current technological change within the CCTV market includes automated analysis, technology convergence, and integrated systems.

Whilst the basic mechanisms and principles of CCTV are understood and have been in operation for many years, the search continues for the panacea of CCTV; systems capable of Automated Picture Analysis, Person Identification, and Behavioural Analysis. Research still continues, and some applications have emerged, with limited success.

Increasingly, CCTV technologies converge with IT technologies and in current digital CCTV systems we witness many instances of CCTV treated similarly to how we treat other forms of computer data. As the technology/infrastructure is developed further and it becomes more affordable, even more possibilities will emerge that revolutionise the use of CCTV (based on technologies such as high resolution cameras, lower cost higher capacity storage, lower cost higher bandwidth internet, wireless data transmission methods and searching techniques).

The greater convergence also allows once separated systems to be integrated. For example:

- Alarm systems connected to CCTV cameras.
- Town centre cameras connected to ANPR systems.
- Shop cameras to Electronic Point of Sale (EPOS) systems.
- Internal building cameras connected to building access control systems.
- Transport system cameras to travel cards and CBRN detectors to CCTV cameras.

Such integrated systems dramatically improve the effectiveness of CCTV systems, as actions can be triggered by associated events and post event CCTV images can be quickly searched against other events/ data (not as now by viewing hours of CCTV material). Integrated systems significantly increase the capacity to undertake public surveillance and therefore needs to be carefully controlled by Information and Surveillance Commissioners' guidance.

9.2.2. CHANGING THREATS

Unrelated to changes in technology has been the change in the threat, caused by serious, organised crime and terrorism to the country. CCTV has in the past proved an effective measure in investigating these crimes but by no means as effective or efficient as it could have been. It has always been time consuming and expensive, and often does not deliver consistently good quality images.

Currently the planning and siting of CCTV cameras has been to predominately deal with local volume crime. If we are to deal more effectively with serious, organised crime and terrorism, different operational requirements are needed, for example:

- cameras, sited in accordance with the National Intelligence Model (NIM) assessments, National Threat assessments and the location of high risk targets.
- specialist training of operators such as to recognise hostile reconnaissance.
- appropriate security levels for the staff and transmission of images.
- a network to establish the national two way flow of intelligence and images, before, during and post-incident.

9.2.3. NEW AND CHANGING PRIORITIES

Generally crime changes as a result of many factors, including the location, the type and the people who carry out the crime. It is influenced by seasonal variations and changes in the law. Local priorities similarly change, for example to reduce certain crime types, such as burglary, street crime, car theft, etc, for which CCTV is an important operational tool. To be at its most effective CCTV should also be able to adapt to crime changes. It is important that operators and police adapt their provision and use to the current priorities. The location of the cameras is important, and more should be done to ensure that the cameras can be easily re-deployable so that they are operating in the crime hot-spots.

Equally more should be done to maximise their effectiveness in detecting certain types of crime, and provide good quality images of the crime, allowing perpetrators to be identified. Two-way flow of intelligence between the police and the local operators of the cameras is critical to the effectiveness of CCTV.

Changes in the local environment and infrastructure can also have an impact on crime. New buildings, change of use, and licensing applications can all impact on local crime, requiring a change in the operational requirements of a CCTV system.

9.2.4. OLYMPICS 2012

The 2012 Olympics will present a significant opportunity for partner agencies to 'join up' their thinking in the positioning and networking of cameras across London and the UK.

The magnitude of the event and subsequent planning will provide the impetus for setting standards and the need for greater integration of CCTV systems.

9.3. CONCLUSIONS

There is a need to harness and guide research, evaluate and improve the effectiveness of current technologies, spearhead the use of CCTV in different and imaginative ways. We must influence manufacturers and standards organisations to produce systems based on the users' requirement, create standards, allowing interoperability of products, and data. Our existing CCTV infrastructure has to be improved so that it can adequately tackle serious, organised crime and terrorism and we must improve the responsiveness of CCTV to tackle changes in local crime and local priorities.

9.4. RECOMMENDATIONS

R 9.1. Establish a structure/body that promotes a greater relationship/ partnership between the universities, manufacturers and users (see chapter on Partnership Working).

R 9.2. Establish close ties with Information and Surveillance Commissioners.

R 9.3. Help develop digital CCTV standards, with national and international government agencies and manufacturers.

R 9.4. Use National Threat Assessments and develop other tools and initiatives to increase the effectiveness of CCTV in managing and reducing the threat to serious, organised crime and terrorism.

R 9.5. Create an effective cross country strategic CCTV network to facilitate the two way flow of intelligence and images, to manage and reduce the national threat to serious, organised crime and terrorism.

R 9.6. Promote the use of the National Intelligence Model and establish other tools and practices to improve the responsiveness of CCTV to changes in local crime and local priorities.

CHAPTER 10 : PARTNERSHIP WORKING

10.1. INTRODUCTION

The number of parties that have a vested interest in CCTV is extensive; from the police, Crime and Disorder Reduction Partnerships to government departments and agencies, transport, industry, the CJS, the Information Commissioner, local government and private individuals. From early on in the evidence gathering process, it was clear that engagement between these groups is desirable and essential to improving the effective use of CCTV. This chapter therefore, ties in closely with other chapters such as those on Standards, Networking and Training.

There exist some real shortcomings in the effectiveness of working relationships between CCTV stakeholders. There is evidence of some groups working closely with each other and this has led to efficient partnership working and cooperation. Conversely, we have also seen groups working in isolation, even where agendas and aims are common amongst agents, leading to either the duplication of work and resources or gaps in development. The issues highlighted below are a good indication of the importance and scale of the developments that need to take place among partners in order to coordinate the effective use of CCTV.

10.2. KEY ISSUES

- There appears to be a general lack of adequate cooperation and communication between some CCTV stakeholders and partners. We have seen evidence of strong partnerships being formed among some small groups, but this is not a general practice, even though it is agreed as vital by all engaged in the evidence gathering process. This is illustrated by the critical relationship between the police and the CCTV control rooms. It is clear that in some cases, where CCTV has been identified as playing a vital role in the fight against crime, and time and resources have been invested in its development, local authorities and the police have centred on building strong relationships. This has increased the effectiveness of CCTV as an investigative tool. This is not, however, a general affiliation, as disparity can be witnessed from one control room to another. The role of the police was identified as being crucial to the success of a CCTV partnership, and the desire for the police to cooperate further with the control room is paramount.
- There is a need for a multi-agency approach to CCTV, but this extends further than simply public bodies and local authorities. The private sector, industry and manufacturers also need to be engaged, to create a complete and comprehensive partnership as a large number of CCTV schemes are privately operated. Ignoring this number of schemes will leave a gap in the partnership chain. As the industry grows, and technology develops, there is a desire by CCTV managers to be kept abreast of developments and innovations by liaising with the private sector, to provide an integrated service.
- A joined up approach may also lead to a conflict of interests between certain stakeholders. A local authority may have agendas that differ from that of the police or the CJS. It seems that local authorities may be diversifying camera use for revenue generation. This is likely to conflict with the purpose of crime reduction, which the police are keen to see take priority. Demands of different users may be large and time consuming, and it is clear for example that local authorities are not exclusively using CCTV for

crime reduction purposes. Many systems were not originally designed for policing purposes and there might be difficulty in identifying common aims for all partners.

- Primacy and priority issues; when such a conflict of interest occurs, the question is who or what takes priority. An example would be if there is a police operation centred on local criminality, consideration needs to be given as to which agency's purpose takes priority.
- The issue of funding and bearing the running costs for the system has also been seen to cause some concern for CCTV Town Centre managers. The systems are set up and controlled by local authorities; however CCTV benefits a wide range of groups, including the police and the wider CJS. CCTV impacts significantly on community safety which is a statutory obligation for a number of agencies. There is therefore a desire for contribution towards the running costs from areas other than local government funding.
- When identifying partners and stakeholders, attention needs to be paid to what level of access to images and recording systems partners may have. Protocols need to be developed that cover issues such as access and control, management, ownership and the provision of images to third parties this ties in closely with the chapters on Networking and Emerging Technology, where it is possible to view images over the internet.
- Effective partnerships will require common technical provision arising from agreed standards. This would enable partners to communicate via a common medium, allowing the transfer of images to each other. This is an essential point in the continual pursuit for networking across the CCTV systems. Other chapters in this report discuss how networking and common standards could be a possibility for the future.
- CCTV is being increasingly identified as having a part to play in local and national crime reduction. On a local scale, there are few CCTV managers who are members of Crime and Disorder Reduction Partnerships (CDRPs). Since CDRPs develop and implement strategies for tackling crime and disorder on a local level, membership of the CCTV manager is regarded as crucial to raising the profile of CCTV and including it in longer term crime initiatives.

10.3. CONCLUSIONS

From the evidence gathered, it is clear that communication, cooperation and engagement are the key to creating a CCTV partnership. It is vital to identify all stakeholders and make them aware of the CCTV work being carried out in the area. The National Strategy review has largely achieved this through its engagement with stakeholders and by creating awareness of the developments of CCTV for the present and the future.

A number of the issues raised centred on the role of the police in such a partnership. The police are seen as a crucial link in the chain, and attention should be paid to creating stronger links between the local police station and the CCTV control room.

Overarching all the issues of access, networking, user groups and targets and agendas is the issue of where the responsibility for CCTV should lie nationally. Currently, there is no single model with responsibility for developing the integrated use of CCTV at either local or national level. It was agreed by most, that a strategic direction is needed to ensure the coordinated growth of CCTV.

10.4. RECOMMENDATIONS

R R 10.1. In order to engage stakeholders in developing a CCTV partnership, a national board with responsibility for strategy and the development of public space CCTV is required. This could also be extended further than public space CCTV, to all users of CCTV as a desirable, long term, option.

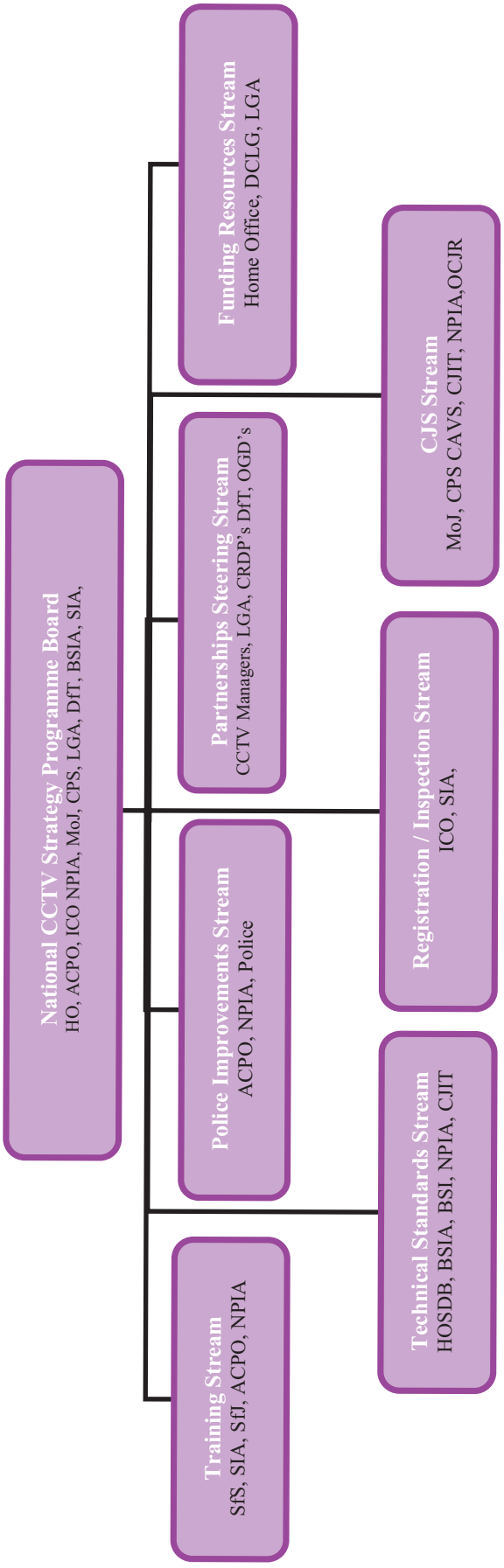
R 10.2. The ability to have police Airwave radio in the control room has been a huge benefit for those control rooms that currently have the facility. The recommendation would be to roll this out to all control rooms as best practice, creating direct communication with the police. Appropriate consultative arrangements would need to be developed in order to inform the National Strategic Board.

R 10.3. The ANPR partnership structure is a good example of a multi-agency approach dedicated to driving forward the ANPR strategy. The ANPR partnership mission statement declares that it will 'work with Partner Agencies at National, Regional and Local level to share assets and data, avoid duplication and enhance operational effectiveness'.

R 10.4. There is a clear inter-agency agreement here, and one that this project should look more closely at for the purposes of a National CCTV Strategy Partnership.

R 10.5. Primacy in relation to CCTV should be determined at a local level by the CDRP, taking into account the strategic guidance provided by the strategy and the National Strategic Board.

PARTNERSHIP MODEL



CHAPTER 11 : MANAGEMENT, FINANCIAL, RESOURCE

11.1. INTRODUCTION

This chapter is primarily concerned with the mechanisms which will drive forward a CCTV scheme, or indeed a CCTV network. Many questions have arisen in relation to who will fund the provision of CCTV.

The question of management has been mentioned in previous chapters particularly in the chapter on partnership working, and has double importance: there is the question of who will be responsible on a national basis for the final strategy and its implementation. Secondly, it concerns the effective management of the systems themselves, and this will encompass all the issues we have seen previously. For example, effective archiving, retention, working in cooperation, inspection and enforcement of the systems.

11.2. KEY ISSUES

- Who or what will fund the provision of CCTV? This is a key issue that is currently preventing CCTV being used more widely and effectively and in limiting cooperation with other partners. CCTV schemes are currently being funded in a number of different ways; a large number were installed as a direct result of government funding under the Crime Reduction Programme. When this dedicated funding ended, town centre schemes looked to such sources of funding for CCTV, including mainstream funding from within general CDRP crime reduction funding streams, re-deployment of cameras for income generation, or outsourcing the systems to private companies to control. A lack of resources has also contributed to the disparity between the effectiveness of systems on a national basis.
- Procurement of new CCTV systems, maintenance, electricity/ transmission provision, are currently undertaken by individual authorities. There may be an opportunity to reduce costs, standardise and improve terms such as electricity / transmission provision, by working with other local authorities or on a national scale.
- There is also a need for management information; it appears that there is a large variation in the amount of management information being kept, published and used as performance indicators. Some CCTV schemes regularly publish key performance indicators (KPIs); others have found it difficult to obtain information from the police and courts.
- Some examples of good indicators include:
- The number of incidents captured on CCTV.
- The number of occasions the CCTV assisted in the arrest of individuals.
- The number of occasions CCTV material is requested by/provided to police.
- How useful the CCTV has been in the investigation.
- The number of occasions the CCTV material has been used in court.
- How useful the CCTV has been at court.

- We have found that the police have been lacking in providing performance figures in the use and effectiveness of CCTV. There are no national indicators like those found for fingerprint and DNA recovery and identifications.
- The CJS have also found difficulty in providing figures on how useful CCTV has been in court, to the contrary some snapshots have shown that CCTV unavailability or playback difficulties has led to cracked and ineffective trials.

11.3. CONCLUSIONS

We can see that the funding issue is a serious threat to the future of CCTV, whether it affects the installation of cameras in areas that currently do not benefit from CCTV, or its expansion and growth into the type of network that has been suggested by the previous chapters, or how it is used by the police or within the CJS. It will be an important factor from beginning to end.

The effectiveness of CCTV schemes cannot be properly assessed by the direct relation to crime statistics alone. CCTV is effective in supporting other activities relating to crime reduction and the potential cost savings down the line in relation to savings in police time, increased detection rates, court time and the increased level of guilty pleas and guilty verdicts obtained when CCTV evidence is available. However, a standard method has to be found to capture this information, and a method of promoting the successes of CCTV locally, (which may then lead to a reduction in crime/deter criminals) and improve public perception of CCTV and at local and national levels to underwrite business cases and provide continuing funding and improvements.

There is no single body that has responsibility and is accountable for CCTV in this country. Equally, there is no single body that can set performance standards and indicators, undertake reviews, improve standards, and determine where public money is best used.

11.4. RECOMMENDATIONS

R 11.1. Establish a body responsible for the governance and use of CCTV in the UK.

R 11.2. Create an effective funding stream, which may include but not be limited to:

- Contributions by stakeholders and interested parties; in the majority of cases this will include a contribution from the police as one of the key players in the use of CCTV
- Further government funding; a dedicated funding stream for CCTV, including funding for maintenance, repair and expansion. This should also include restrictions and conditions on the use of funds to enable standards to be conformed to
- Income generation by the system itself; use of CCTV in a variety of ways from traffic, bus lane, and bylaw enforcement to alarm monitoring, lone worker monitoring and electronic patrolling of retail and business parks, where the system is 'funding itself'. The concern here is that cameras and/or the CCTV operators will be increasingly used for these purposes, detracting from the use of cameras for crime prevention and law enforcement. This last point is an increasing worry from a police perspective
- Partial funding from a CCTV Registration Scheme

R 11.3. Standardised national key performance indicators should be introduced for use by CCTV operators, the police and the courts.

R 11.4. Promote CCTV and its expansion, by forming business cases that evidence the effectiveness of systems, focusing on the best elements of a CCTV system, how useful CCTV can be for pre-emptive/reactive purposes, value for money, and number of arrests per year. This will be the key to gaining funding and resource support.

CHAPTER 12 : SUMMARY OF RECOMMENDATIONS

CHAPTER 2 – STANDARDS		
1	R2.5, R2.10, R2.11, R10.1, R11.1	Establish a body responsible for the governance and use of CCTV in the UK.
2	R2.1	Agree on digital CCTV standards and digital video formats for public space CCTV, police, and CJS use.
3	R2.2, R9.3	Seek to influence national and international CCTV standards.
4	R2.3	Continue the review of the Home Office Scientific Development Branch Operational Requirements Manual.
5	R2.4	Develop a program for CCTV operators to review the location and purpose of their CCTV cameras.
6	R2.6	Establish technical requirements that will allow CCTV cameras to be used for multiple purposes.
7	R2.7	Provide clear advice to CCTV operators on police and CPS requirements from CCTV systems to maximise successful prosecutions.
8	R2.8	Establish the gaps in CCTV coverage taking into account the national intelligence model and national threat assessment model.
9	R2.9	Further develop and share best practice in the use and operation of public space CCTV systems.
10	R2.12	Encourage town centre CCTV schemes to monitor existing CCTV systems in other areas of public space and the transport infrastructure thus creating a hub for public space CCTV.
CHAPTER 3 – REGISTRATION, INSPECTION, ENFORCEMENT		
11	R3.1	Greater powers for the Information Commissioner to enforce CCTV licensing requirements of systems and people.
12	R3.2, R3.3, R3.4	Develop legislation to ensure the appropriate regulation of CCTV systems.
13	R3.6	Develop a system of registration that assists in the regulation of CCTV systems.
14	R3.5	CCTV should be considered as an element of planning and licensing applications.
15	R3.7	Develop a mechanism to allow CCTV standards to be enforced.
CHAPTER 4 – TRAINING		
16	R4.1	Security Industry Association (SIA) to clarify the requirements in relation to operator licensing.
17	R4.2, R4.3, R4.4	Develop minimum training requirements and ultimately an accredited training programme for all those engaged in CCTV.
CHAPTER 5 – POLICE USE OF CCTV		
18	R5.1	Image retention periods should be standardised and relate to the operational purpose of the CCTV system.
19	R5.5	The Police Service needs to review its internal operational processes and management structure. In effect, it needs to determine ownership for CCTV within each force and consider its link to existing forensic disciplines and its future training and development requirements.

20	R5.3	The Police should develop an organisation model for managing the recovery, analysis and investigation of CCTV evidence.
21	R5.4, R5.11, R5.12	The specialist nature of CCTV recovery, analysis and investigation should be recognised and appropriate training developed.
22	R5.6	Performance standards similar to those that support other forms of crime scene evidence should be developed in relation to CCTV recovery and analysis.
23	R5.7	Research should be undertaken to determine the relative benefits of fingerprint and DNA recovery in comparison with CCTV recovery.
24	R5.8, R10.2	Protocols should be developed allowing the use of Airwave radio in town centre CCTV control rooms and the sharing of intelligence between the police and town centre CCTV monitoring staff.
25	R5.9	Protocols should be developed that require the police to provide feedback to town centre CCTV managers as to the operational usefulness of CCTV images.
26	R5.10	The police service needs to consider the development of a CCTV capability to support serious and organised crime, counter terrorism and the protection of key economic sites across the UK.
CHAPTER 6 – STORAGE / VOLUME / RETENTION		
27	R6.1	Develop CCTV image retention and disclosure guidance.
28	R6.2	CCTV operators, police and CJS agencies should determine respective roles and responsibilities in relation to the short and long term retention (including archiving) of CCTV material.
29	R6.3	Evaluate 'camera to archive' network access and data archiving methods.
CHAPTER 7 – CCTV NETWORKS LIVE AND STORED		
30	R7.1, R7.2,	Establish a basic CCTV network infrastructure. Establish security and access rights and permissions.
31	R7.2	Establish the effectiveness of CCTV networks by running pilot projects.
32	R7.3, R9.5	Determine the strategic CCTV network required.
33	R7.4	Facilitate the connection of digital CCTV systems to the network.
CHAPTER 8 – FACILITIES IN THE CJS		
34	R8.1, R8.3, R8.4, R8.5, R8.6, R5.2	The Crown Prosecution Service and Court Service should develop the capacity to view digitally recorded CCTV evidence.
35	R8.2	Crown Prosecution Service and the police to develop a better understanding of disclosure and evidence continuity rules to ensue trials are not lost due to a failure to adopt proper procedures.
36	R8.7	In the event of a guilty plea there should be presumption that CCTV evidence is played in court where this may assist in determining an appropriate sentence.
CHAPTER 9 – CHANGE – EMERGING TECHNOLOGIES / CHANGING THREATS & NEW PRIORITIES		
37	R9.1	Establish a structure/body that promotes a greater relationship/ partnership between the universities, manufacturers and users.
38	R9.2	Establish closer ties with the Information and Surveillance Commissioners in developing surveillance technologies.

39	R9.4	Use National Threat Assessments and develop other tools and initiatives to increase the effectiveness of CCTV in managing and reducing the threat of serious, organised crime and terrorism.
40	R9.6	Promote the use of the National Intelligence Model and establish other tools and practices to improve the responsiveness of CCTV to changes in local crime and local priorities.
CHAPTER 10 – PARTNERSHIP WORKING		
41	R10.5	Primacy in relation to CCTV should be determined at a local level by the CDRP, taking into account the strategic guidance provided by the strategy and the National Strategic Board.
CHAPTER 11 – MANAGEMENT, FINANCIAL, RESOURCE		
42	R11.2	Create an effective funding stream for public space CCTV.
43	R11.3	Develop national key performance indicators relating to the use of public space CCTV across all associated agencies.
44	R11.4	Promote CCTV and its expansion by forming evidence based business cases.

CHAPTER 13 : NEXT STAGE

The 44 recommendations contained in this strategy represent a significant effort for all agencies involved in CCTV. However, progress in these areas is extremely important if we are to realise the full potential of CCTV across a varied range of uses and importantly continue to receive the support of our communities across the UK in its use.

The next stage of this work will be in the form of a 12 month implementation phase which will prioritise and develop the recommendations. In order to do this we have established a multi agency team and an overarching Programme Board, representative of key stakeholders, to ensure that there is full cooperation, agreement and vision on the strategy's implementation.

APPENDIX 1 : GLOSSARY

ACPO	Association of Chief Police Officers
ANPR	Automatic Number Plate Recognition
BCU	Basic Command Unit
BSCF	Building Safer Communities Fund
CAD	Computer Aided Dispatch
CCTV	Closed Circuit Television
CENTREX	The Central Police Training and Development Authority. As of April 2007, Centrex was subsumed by the NPIA.
CJIT	Criminal Justice Information Technology
CJS	Criminal Justice System
CPS	Crown Prosecution Service
Cracked Trial	On the trial date, the defendant offers acceptable pleas or the prosecution offers no evidence. A cracked trial requires no further trial time.
CDRP	Crime and Disorder Reduction Partnership
CRP	Crime Reduction Programme
CSI	Crime Scene Investigators
DCLG	Department for Communities and Local Government
DPA	Data Protection Act
HOSDB	Home Office Scientific Development Branch
ICO	Information Commissioner's Office
Ineffective Trial	On the trial date expected progress is not made due to action or inaction by one or more of the prosecution, the defence or the court and a further listing for trial is required.
NAO	National Audit Office
NIM	National Intelligence Model
NPIA	National Policing Improvement Agency (NPIA) as of April 2007 replaced and took on much of the work of Centrex, PITO, parts of the Home Office which supported the police service in rolling out operational change programmes, and a number of smaller ad-hoc projects
OCJR	Office for Criminal Justice Reform
OR	Operational Requirement
PAL	Phase Alternate Line (UK Television System)
PCMA	Public CCTV Managers Association
PITO	Police Information Technology Organisation. As of April 2007, PITO was subsumed by the NPIA.
PTZ	Pan-tilt-zoom (general term for cameras whose direction and level of zoom can be remotely controlled to allow operators to position, track or zoom in on areas of interest.
RIPA	Regulation of Investigatory Powers Act
SCI	Safer Communities Initiative
SIA	Security Industry Authority
SSCF	Safer Stronger Communities Fund