A National Approach to Closed Circuit Television

National Code of Practice for CCTV Systems for Mass Passenger Transport for Counter-Terrorism

Agreed by the Transport and Infrastructure Senior Officials Committee

March 2012

CCTV Rewrite Working Group (2011-2012)

The original edition of the *National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism* (the Code) was published on 14 July 2006. The Code was reviewed in 2010-2011[1]. The Review recommended that:

- Governments agree to develop a revised version of the Code, under the Standing Committee on Transport (SCOT) leadership and in consultation with the National Counter-Terrorism Committee (NCTC), that includes the proposed changes identified in this Review.

- Governments agree to inform the NCTC CCTV Working Group of the findings from this Review, including the development of a national approach to the use of CCTV for counter-terrorism.

These recommendations and the proposed changes identified in the Review are reflected in this updated version of the Code. The March 2012 version of the Code supersedes the 14 July 2006 version.

All Australian Governments were represented or had input into the review and subsequent rewrite working groups through the lead agencies listed below.

Commonwealth

Department of Infrastructure & Transport

Australian Security Intelligence Organisation

Australian Customs & Border Protection Services

Australian Federal Police

New South Wales

Transport for NSW

New South Wales Police Force

RailCorp

Victoria

Department of Transport

Victoria Police

Queensland

Department of Transport & Main Roads

[1] SCOT Security SSC, March 2011. *CCTV Code of Practice' Review 2010-11: Monitoring and Review of the Code*.

Western Australia
Public Transport Authority

South Australia
Department of Planning, Transport& Infrastructure

South Australia Police

Tasmania
Department of Infrastructure

Northern Territory
Northern Territory Transport Group, Department of Lands & Planning

Australian Capital Territory
Justice & Community Safety Directorate

Local Government
Australian Local Government Association

In addition, the National Counter-Terrorism Committee (NCTC) was consulted regarding law enforcement and evidentiary elements. National ICT Australia Ltd (NICTA) provided advice on technological advances and trends in relation to CCTV.

Important Terms

ALGA	Australian Local Government Association
ASIO	Australian Security Intelligence Organisation
ATC	Australian Transport Council (now redundant – replaced by SCOTI)
CCTV	Closed-circuit television
COAG	Council of Australian Governments
CT	Counter-terrorism
DOT	Department of Transport
IGA	Intergovernmental Agreement on Surface Transport Security
Interoperability	The ability of CCTV system components to operate together on the same network and the ability to share video between networks or jurisdictions.
IPP	Information Privacy Principle
ISR	Intelligence, Surveillance, Reconnaissance
NCTC	National Counter-Terrorism Committee
NICTA	National ICT (Information & Communications Technology) Australia
NIFS	National Institute of Forensic Science
NSTSS	National Surface Transport Security Strategy
OTS	Office of Transport Security
PIA	Privacy Impact Analysis
PIC	Privacy Impact Checklist
SCOT	Standing Committee on Transport (now redundant – replaced by TISOC)
SCOTI	Standing Council on Transport & Infrastructure (replaced ATC)
SISTO	Security-identified surface transport operations

Security SSC	Security Standing Sub-Committee (now redundant – replaced by TSC)
TSC	Transport Security Committee (replaced Security SSC)
TISOC	Transport & Infrastructure Senior Officials Committee (replaced SCOT)

Contents

CCTV Rewrite Working Group (2011-2012)		**2**
Important Terms		**4**
Part A	**Introduction and Context**	**9**
Section 1	**A National Approach**	**10**
1.1	**Introduction**	**10**
1.2	**A Risk-based Approach**	**10**
1.3	**Security Context**	**11**
1.4	**Related Information Technology Issues**	**14**
1.5	**Broad Contextual Considerations**	**14**
Section 2	**Outline of the National Code**	**15**
2.1	**Background**	**15**
2.2	**Objective**	**16**
2.3	**Code Framework**	**17**
2.4	**Planning**	**17**
2.5	**Wider Application of the Code**	**19**
2.6	**Jurisdiction Policy Relevant to the Code**	**19**
Part B	**Performance Guidance**	**20**
Section 3	**Guidelines for CCTV Systems and Technology for Counter-Terrorism Purposes**	**21**
3.1	**Forms and Uses of CCTV Systems**	**21**
3.2	**System Components**	**21**
3.3	**System Monitoring**	**22**
3.4	**CCTV for Counter-Terrorism Purposes**	**22**

Section 4	**Recommended CCTV System Guidelines to meet Operational Objectives**	**24**
4.1	**Applying the Code**	**24**
4.2	**Determining the Transport Security Priority**	**25**
4.3	**Determining Operational Objectives**	**26**
4.4	**CCTV System Performance Criteria**	**26**
Part C	**Legal and Procedural Aspects**	**37**
Section 5	**Legal Issues and Accountability**	**38**
5.1	**Purpose of this Section**	**38**
5.2	**Legal Context**	**38**
5.3	**Onus on Owner/Operators to Report Incidents and Suspicious Activity to Assist Counter-Terrorism**	**39**
5.4	**Privacy**	**40**
5.5	**Compliance with Privacy Principles**	**40**
5.6	**Evidence-Handling Procedures**	**41**
5.7	**Jurisdictional Capabilities for Reviewing Mass CCTV Product**	**43**
5.8	**Registers of CCTV Systems**	**43**
5.9	**Related Legislation and Standards**	**43**
5.10	**Safety in Design**	**44**
5.11	**Legal Advice**	**45**
Section 6	**Monitoring and Review of the Code**	**46**
6.1	**Review**	**46**
Part D	**Appendixes**	**47**
Appendix A	**Technical Acronyms**	**48**
Appendix B	**New Technologies**	**50**
Appendix C	**Bibliography**	**56**

Appendix D **Recommended Security Functions, Operational Objectives and Transport Security Priorities** **59**

Appendix E **Recommended CCTV Performance and Storage Criteria** **66**

Appendix F **Code Background, Objectives, Development and Application** **71**

Part A Introduction and Context

Section 1 A National Approach

1.1 Introduction

The Code has been developed by Australian Governments as a guide to future investments in CCTV. It is not mandatory.

The Code is not designed as a uniform, 'one-size-fits-all' prescription or specification. It supplements other guidance material, the application of which is determined by each jurisdiction's transport security risk assessments and legislation.

For more localised advice, those in the transport sector ('owner/operators') who plan to install or upgrade CCTV systems should engage in the first instance with their respective jurisdiction transport security regulatory authority, then with law-enforcement authorities and other stakeholders. Being key agencies in transport security and counter-terrorism, their input in planning and execution is essential.

1.2 A Risk-based Approach

The Code provides a voluntary, risk-based approach to planning and implementing CCTV and allows each jurisdiction to determine and apply its own CCTV requirements for counter-terrorism purposes, taking into account its own priorities for the application of resources to wider counter-terrorism initiatives. How these elements are balanced will depend on perceived risk within the particular operating environment and be informed by existing counter-terrorism arrangements, plans and capabilities specific to each jurisdiction. This is essential, because transport systems are large and complex—no single, universal standard of CCTV implementation would be rational or affordable.

In doing so, the Code defines core performance criteria for four operational objectives (*'monitor', 'detect', 'recognise', 'identify'*) across three priority-graded 'transport security priority areas' for upgrades and enhancement of CCTV systems. Determining the priority grading ('Priority 1', 'Priority 2', 'Priority 3') is risk-based. Priority would typically be assigned on the basis of the assessed vulnerability of people within the system, more than critical assets. In this way, the application of the Code will not only provide an effective counter-terrorism tool, primarily in response to a terrorist incident, but should also improve the general security of mass passenger transport.

To conform to good risk management practice, owner/operators should conform with the relevant standard, AS/NZS ISO 31000—2009: *Risk Management—Principles and Guidelines* and other handbooks (refer to Appendix C—Bibliography).

One critical element of an effective risk assessment is defining the current internal and external context, which characterises internal circumstances that have a security bearing and the nature of the security environment itself. Context statements may be subject to rapid and unexpected change due to variations in the international and national security environments. Seeking current information is critical to the formulation of a credible risk assessment, which in turn is a critical element of a defensible business case for recommended security risk treatments, including CCTV.

The following is an example of a high-level context statement.

> *Transport systems continue to be attractive targets for terrorists seeking to inflict mass casualties, economic damage, instil fear and create spectacular media imagery. Transport systems are inherently vulnerable to terrorist attack, as they are open systems that gather large numbers of people at predictable times in predictable places.*
>
> *Transport security encompasses aviation, air cargo supply chain, maritime (including offshore oil and gas) and mass passenger transport systems such as road, rail, trams and ferries. Transport security is a common usage term that belies the complexity of roles, responsibilities and relationships in the aviation, air cargo supply chain, maritime and mass transit sectors. Industry is at the core of these sectors. Clustering around industry, in a multi-agency and multi-jurisdictional domain, are border security, regulatory, law enforcement and intelligence agencies from the Commonwealth and States and Territories*[2].

This generic statement would require further localised detail. Of relevance to CCTV, this might include considerations relevant to the attack planning and surveillance *modus operandi* of terrorists, as well as post-attack evidentiary requirements.

Organisations undertaking risk assessments may seek current information on broad terrorist threat from the Office of Transport Security and State and Territory Police counter-terrorism units for more localised threat information. Owner/operators are also advised to seek information and guidance throughout their CCTV implementation planning from their jurisdiction transport security regulatory authority.

1.3 Security Context

The threat of terrorism in Australia is real and enduring. It has become a persistent and permanent feature of Australia's security environment. The terrorist threat from people born or raised in Australia, who have become influenced by the violent jihadist message, has increased in recent times. A number of Australians are known to subscribe to this message, some of whom might be prepared to engage in violence. Many of these individuals were born in Australia and they come from a wide range of ethnic backgrounds. The pool of those committed to violent extremism in Australia is not static —over time some move away from extremism while others become extreme.

These terrorists share ideology and broad strategic objectives with transnational cells, but add a different element of complexity to security considerations as a result of their local knowledge and community connections.

Counter-terrorism operations in Australia have resulted in a number of people being prosecuted and convicted of terrorism offences under the Criminal Code. From 2001 to 2010, four mass casualty attacks within Australia were disrupted only because of the work of intelligence and law enforcement agencies. Australians and Australian interests

---

[2] Commonwealth Department of Infrastructure and Transport. Viewed on 4 November 2011 at http://www.infrastructure.gov.au/transport/security/index.aspx

have been attacked overseas (including the 2002 and 2005 Bali bombings, and the 2004 and 2007 attacks against the Australian Embassy in Jakarta).

In the Australian context, a terrorist attack could be conducted by a transnational terrorist cell, local extremists acting independently, or a collaborative effort between the two. The September 2001 attacks against the World Trade Centre and the Pentagon in the United States were carried out by a transnational terrorist cell, directly linked to al-Qa'ida. In European locations such as London, Frankfurt, Copenhagen and Stockholm, domestically based groups or individuals have planned or undertaken attacks inspired by the ideology and activities of al-Qa'ida.

1.3.1 Terrorist Threat to Mass Passenger Transport Operations

In selecting a target for attack, terrorists may focus on symbolic and iconic locations, and causing mass casualties or economic damage. Other objectives include the desire to make a symbolic statement that resonates with extremists and the target population, and generates public anxiety and spectacular media imagery.

Terrorists are inventive, their tactics and targets evolve, and they take account of vulnerabilities, opportunity and likelihood of success when selecting targets and attack methods.

Mass passenger transport operations fulfil many terrorist targeting criteria. Public transport concentrates people in large numbers, in accessible places, at regular and predictable times. These characteristics apply to bus, rail, ferry and intermodal operations. An attack against transport operations, particularly during peak times, could achieve terrorist objectives by causing mass casualties and economic damage, as well as generating widespread media interest and imagery.

Despite mitigation measures put in place to strengthen the security of the sector, mass transport operations are likely to remain a preferred target for terrorist groups. As well as meeting terrorist strategic objectives, mass passenger transport operations are, by their nature, open to the public, allowing terrorists to access a potential target as a member of the travelling public, to conduct reconnaissance, surveillance and attack planning, and to execute the attack.

1.3.2 Terrorist Intelligence and Attack-planning Activities

Terrorist planners can conduct extensive research as part of their target selection. This can involve obtaining photographs, plans and maps, undertaking physical or video reconnaissance, testing security countermeasures, conducting attack 'dry runs' and planning escape routes.

- The 7 July 2005 London bombers used dry runs to simulate an attack, to expose strengths and weaknesses in their planning, and to tailor their plan to the operating environment.

Terrorist attack planning can be difficult to detect as activities may occur out of sequence, take place over varying timescales and be compartmentalised. However, terrorists require information to conduct their operations—representing to varying degrees, an intelligence capability within each terrorist group or cell, which is designed

to support their attack-planning activities, target-assessment and related missions. The presumption that terrorist organisations undertake surveillance and reconnaissance—supported by research and other activities—to support this intelligence mission is based on reporting of its use in actual attack-planning, alongside its existence in written training material and doctrine devoted to instructing terrorist personnel in how to conduct terrorist intelligence activities.

It is this process involving reconnaissance around and surveillance of or inside their potential targets that, when observed, provide indicators of attack planning and other terrorist activities. The process by which a terrorist collects information on a potential target is matched, ideally, by a counter-process in which the defender (or counter-terrorist) attempts to degrade the terrorist's intelligence picture of their target; at the same time, the counter-terrorist attempts to learn everything that they can about the terrorist—their identity, capability and intentions. Overall, the terrorist's intelligence-collection task can be encapsulated in the term "intelligence, surveillance and reconnaissance" —or ISR; it therefore follows that a key task for the counter-terrorist is undermining terrorist ISR—or counter-ISR.

The ability to counter terrorist ISR is premised upon the detection and resolution of apparently suspicious activities that may indicate terrorist ISR. The detection and interdiction of terrorist ISR may be relatively easy around hardened targets with strong, obstructive protective security regimes. But it is an entirely different challenge around large, complex infrastructures such as public transport, whose open nature contributes to their vulnerability to attack. It is for this reason that the preventive security measures and mechanisms instituted within and around these environments must—by the very nature of the business these infrastructures support—be far less obstructive or intrusive than may be desired solely from a protective security perspective. Therefore, preventive security in such open environments must be intelligence-led, and rely heavily on human factors to support the detection and resolution of suspicious activities, in combination with other security measures such as CCTV.

1.3.3 The Role of CCTV

In the context of preventative security, CCTV's utility extends beyond the traditional post-evidentiary purposes. CCTV plays a central role in countering terrorist ISR, both actively and passively. In terms of the former, it provides the best live portal into the transport environment from a single terminal, and can be used most effectively in identifying suspicious activities as a trigger for follow-up investigation and resolution; in its most advanced form, it is not only used proactively – to identify suspicious activities as they occur (as opposed to forensically or reactively once an incident or activity has already occurred and is being investigated)—but also serves as a potent tool to deter or shape the terrorist's activities. In terms of the latter, its placement and presence serves as a passive dissuader to terrorists conducting ISR and attack planning—in case after case, terrorists have identified CCTV as something that they both do not like and wish to avoid, highlighting its positioning (and even capabilities where known) in their intelligence reports and target-folders. For these reasons, CCTV —and its sophisticated use—is central to any preventive security regime, especially one predicated on the human factors necessary to detect and resolve suspicious activities.

In the Australian transport sector, overall, CCTV is heavily observed but largely trigger-driven—in other words, being used to respond to on-going or completed incidents, rather than used proactively to identify suspicious activities and behaviours, essential for counter-ISR. This would appear to be down to a combination of limited staff resources to monitor CCTV cameras—especially in the larger control rooms—limitations in the training of CCTV operators, very limited take-up of `smart' software to increase the efficacy of CCTV, and, in some cases, the failure of organisations to appreciate the possibilities that CCTV presents for preventive security that goes beyond a reactive or forensic use.

As with other security measures, the extent to which CCTV is applied needs to be proportionate to the risk. Security elements such as active monitoring and use of `smart' software can be scaled up or down as the risk changes.

1.4 Related Information Technology Issues

In addition to the above context, agencies and owner/operators should be aware of the degree to which information systems (including in the transport sector) are open to abuse. This has implications in counter-terrorism. Supervisory Control and Data Acquisition (SCADA), as well as CCTV data communications, are more frequently occurring over non-dedicated IP networks, which may be more vulnerable to attack than dedicated or 'air-gapped' networks.

1.5 Broad Contextual Considerations

1.5.1 Pace of Change

Although in very broad terms the *modus operandi* of terrorists is not changing rapidly, it is important for jurisdictions and owner/operators to be aware of the rate of technological change in CCTV and related applications, including resolution, communications, software and storage. Owner/operators and jurisdictions need to ensure that strategic purpose drives CCTV implementation, not, as can be the case, the attractiveness of an emerging technology.

Furthermore, as elements of security design are being impacted by rapid technological change, the place of CCTV in the mix of counter-terrorism and broad security measures will change. The role and capability of the best-planned CCTV system will be superseded in time.

For these reasons, owner/operators and jurisdictions need to keep their CCTV measures under review, to ensure that the impact of changes in the security and technological contexts are properly informing their understanding of risk and, in turn, are being reflected in the purpose and the nature of their systems.

Section 2 Outline of the National Code

2.1 Background

Australia's national mass passenger transport security arrangements are primarily framed by the *Intergovernmental Agreement on Surface Transport Security* (the IGA), signed by the Commonwealth and State and Territory Governments in 2005, which aims to implement nationally-consistent protective security planning and preventive measures in the surface transport system. Under the agreement, the States and Territories aim to ensure that appropriate action is taken by *security identified surface transport operators* within their jurisdictions with respect to surface transport security.

The Commonwealth Government regulates security for aviation, ports and shipping consistent with international agreements. State and Territory Governments regulate security in other transport sectors, in particular mass transport, including road, rail and ferry.

Consistent with the IGA, the *National Surface Transport Security Strategy* (the NSTSS) provides a framework for Australian Governments to work collaboratively to improve security capabilities and resilience across surface transport sectors, including mass passenger transport. In recent years, all Australian Governments have invested heavily in additional security measures and capabilities for the mass passenger transport sectors, including in CCTV. It is accepted that collaboration between jurisdictions (and between agencies and operators) can play a critical part in better security outcomes in general. This extends to the planning, design and operation of CCTV systems.

The significant role of CCTV in investigations of past major terrorist attacks has highlighted CCTV as an important element of counter-terrorism strategies and arrangements. Although the transport sector has made significant investment in CCTV, such systems have generally been designed and used to assist transport operational outcomes and passenger safety. Accordingly, such systems have widely varying levels of coverage, resolution, capability, technical quality and accessibility, which may not be suitable for counter-terrorism purposes.

In September 2005, the Council of Australian Governments (COAG) Special Meeting on Counter-Terrorism agreed to the development of 'a national, risk-based approach to enhancing the use of closed-circuit television for counter-terrorism purposes', including the development of this Code for the mass passenger transport sector. The Code was designed to allow each jurisdiction to determine its own CCTV requirements 'having regard to the use of CCTV for local counter-terrorism purposes' Drafting of the Code was informed by expertise regarding technological aspects of CCTV systems and other critical elements such as law enforcement, counter-terrorism, mass passenger transport, and legal and legislative considerations.

Ongoing management of the Code is the responsibility of the then-Australian Transport Council (ATC)[3] in consultation with the National Counter-Terrorism Committee (NCTC).

In accordance with the 'Review' provisions of the Code, in February 2011, the then-Standing Committee on Transport (SCOT) Security Standing Sub-Committee (SSC)[4] completed a Review of the Code, which was led by Victoria (Department of Transport) with membership from jurisdictions and appropriate agencies. As with the Code itself, the Review was directed to jurisdictions with the responsibility for developing and implementing CCTV system projects for the mass passenger transport sector.

The Review concluded that the Code was functional and that it should be revised to reflect a range of recommended amendments. In March 2011, SCOT endorsed the Review Group's recommendation that Governments agree to develop a revised version of the Code, under SCOT leadership and in consultation with the NCTC, which includes the proposed changes identified in the Review, in particular regarding:

- The impact of new technologies and applications of CCTV systems for security purposes
- Changing terrorism risks [as they relate to CCTV]
- The effectiveness of application and utility of the Code in guiding CCTV systems implementation and
- Legal and privacy aspects.

2.2 Objective

The objective of the Code is to define a nationally-consistent framework to enhance the capacity of CCTV in Australian mass passenger transport systems to contribute to counter-terrorism outcomes. In doing so, the Code provides owner/operators (which may include security-identified transport operators and security-regulated transport areas and government agencies) with a non-mandatory functional standard and set of performance criteria regarding risk-based implementation of CCTV in the counter-terrorism context.

The Code provides a framework by which CCTV product of an appropriate functional standard and value is readily available to, and usable by, law enforcement, national security and other relevant agencies, specifically for counter-terrorism purposes. Although video analytics that enable automated surveillance and pre-event response continue to evolve, CCTV in the counter-terrorism context largely continues to be a post-event analysis and response tool. Law enforcement and national security requirements in relation to CCTV coverage following an event will necessarily be rigorous. For this reason, forensic and evidentiary requirements should always be key considerations for owner/operators in planning for new or upgrading CCTV systems.

[3] SCOT is now known as TISOC (Transport & Infrastructure Senior Officials Committee) and the ATC as SCOTI (Standing Council on Transport & Infrastructure). The Security Standing Sub-Committee is now known as the TSC (Transport Security Committee).

The Code reflects current and anticipated counter-terrorism priorities regarding preparedness, prevention, response, investigation and recovery, in line with the National Counter-Terrorism Plan. It also reflects NCTC priorities regarding the use of CCTV data for evidentiary purposes.

2.3 Code Framework

The Code outlines levels of CCTV system performance that correlate with the security and operational profile of particular transport services. The methodology retains flexibility and avoids arbitrarily defining innumerable combinations of individual standards to meet all possible circumstances or technologies. Appendix A defines technical acronyms used in this document. Appendix B includes information on emerging CCTV technologies. Appendix C lists relevant technical standards that should generally be applied to CCTV systems, where appropriate.

The Code recommends some broad standards for security-identified transport operators and security-regulated transport areas where their risk assessments determine them to be appropriate. Section 4 and Appendixes D and E provide further details.

Also, where appropriate, the Code offers performance criteria for CCTV for the routine monitoring of identified 'at-risk' environments, for the resolution of suspicious activity and actual incidents, and for investigation purposes, while ensuring the fulfilment of privacy obligations.

Key to the effectiveness of the framework defined in the Code, owner/operators of CCTV systems need to be familiar with their environments and fully cognisant of the system specifications and operating procedures applicable in their particular situations. They need also to be aware of the range of legal obligations that relate to CCTV and surveillance in general. The Code provides guidance on these elements.

The use of CCTV technology for counter-terrorism purposes must balance the security benefits against the Australian community's expectations of privacy and civil liberties. Appropriate legal and legislative arrangements are necessary to ensure that CCTV can be used to help protect the community, while maintaining appropriate safeguards against abuse and unnecessary erosion of privacy. Section 5 addresses legal issues and accountability. Section 6 outlines ongoing management of the Code.

2.4 Planning

Effective planning is the obligation of the owner/operator and is essential in design and implementation.

CCTV and the associated analytics are evolving rapidly in sophistication and application. A properly informed (evidence-based) definition of purpose is critical in planning an effective, 'fit-for-purpose' CCTV system or upgrade. Purpose in turn needs to be informed by detailed familiarity with the relevant elements of the internal and external operational and security contexts.

Early in planning, owner/operators need to engage with the relevant transport security regulatory authority and inform themselves of all security policy and other considerations (legal) to their CCTV requirements. These authorities are typically, though not always, located within a jurisdiction's Transport or Infrastructure portfolio.

Defining a purpose and effectively planning a CCTV implementation will be informed by, but will not necessarily be limited to:

- security and operational risk
- other planned or existing security measures
- available technology
- interoperability
- maintenance
- cost
- evidentiary, privacy and other legal considerations.

Effective planning is inclusive of the operational and security context of the owner/operator. This means that planning needs not only to be informed by a well-founded awareness of terrorist risk. It also needs to include all related stakeholders, or those organisations that bear some relationship to the owner/operator and who might impact or benefit (or be impacted or benefited by) the owner/operator's planned CCTV implementation. They may include other transport operators, or local government, retail outlets, host building management, or law enforcement and national security organisations. Consultations within the stakeholder community also need to occur early in planning. The transport security regulatory authority may be able to help identify related stakeholders.

2.4.1 Interoperability

It is likely that the planning or execution of a terrorist or other security attack will leave traces within more than one owner/operator's system and that relevant data will exist on more than one CCTV system. For example, piecing together events leading up to and following an attack in an airport or surface transport hub will likely require analysis of the data outputs of many distinct systems within the target facility and possibly neighbouring facilities or the adjacent public domain. These systems may deliver differing resolution outputs and require system-specific proprietary software to read. This can hamper data sharing, potentially impacting the effectiveness of response operations or, more likely, post-response evidence collection.

Interoperability needs to be addressed early in planning and included in consultations with transport security regulatory authorities and other stakeholders, in particular law enforcement authorities and neighbouring owner/operators or operations. This will assist in defining CCTV technical and system design criteria that will optimise data sharing with relevant stakeholders.

Legal provisions relating to lawfully sharing private data also need to be complied with and allowed for in planning. As indicated in Section 2.4.3, owner/operators are obliged to inform themselves of the legal implications of their CCTV measures.

Dealing with these issues is an ongoing focus of many owner/operators and jurisdictions. The work done by some jurisdictions in developing 'Precinct Committees' and 'Precinct Action Plans' represents good practice that may be relevant to owner/operators in planning.

For an effective response to terrorism, data sharing and exchange of images need to be routine activity, not limited to times of emergency. This is an ongoing responsibility of government (please refer to Section 4.4.7).

2.4.2 Maintenance

Owner/operators need to budget for whole-of-system maintenance in their initial planning and subsequent implementation. CCTV can be seen as a system involving the collection, communication and management of video data. Any system is only as functional as its least-functional element. The most advanced high-resolution camera may be compromised by a dirty lens; an ill-maintained power supply has the potential to cause system failure. Provision needs to be made for planned maintenance of all system elements.

2.4.3 Legal Framework

Planning also needs to be informed by legal frameworks that are relevant to CCTV. These will typically include, but not necessarily be limited to, provisions regarding admissibility of evidence, the exercise of emergency powers, the right to privacy, workplace relations, freedom of information and constraints and powers in relation to surveillance in general.

Some of these elements are the same or similar across the jurisdictions, others are not the same. All may change through time. Owner/operators need to be cognisant of their legal obligations. Good practice is to seek advice from the relevant jurisdiction transport security regulatory authority and legal policy portfolio; and to do so early in planning.

2.5 Wider Application of the Code

While the Code is specific to counter-terrorism in the mass passenger sector, CCTV systems are used in many other places and circumstances. In applying the Code, it is advisable to consider including in design other beneficial outcomes such as public safety, law enforcement, operational and broad security. In addition, the Code could be applied to improve the capacity of CCTV systems to contribute to counter-terrorism outcomes in other places (outside of the transport sector) where large numbers of people gather. Adaptations for such application will need to take into account context, specific risk assessments and physical circumstances.

2.6 Jurisdiction Policy Relevant to the Code

Each jurisdiction has legislation and policy relevant to the use of CCTV. These change through time. Owner/operators need to inform themselves of these critical elements early in planning. In the first instance, advice on relevant regulatory arrangements and policy should be sought from their jurisdiction transport security regulatory authority.

Part B Performance Guidance

Section 3 Guidelines for CCTV Systems and Technology for Counter-Terrorism Purposes

3.1 Forms and Uses of CCTV Systems

CCTV is by definition a television system that transmits images within a closed system. Images are available only to people directly connected to the transmission system or given access rights to a closed user group within an information and communications technology network.

CCTV systems are installed in open public areas, such as streets; in privately-owned or government-owned spaces that are generally accessible by members of the public; in commercial premises (such as retail premises, cash-handling facilities and bars); in security-sensitive workplaces (such as critical infrastructure); and in private spaces (including staff or accommodation areas).

Mass transit CCTV networks should use high-quality CCTV cameras. These are installed in and around public transport (such as hubs, terminals, stations, stopping points, trains, trams, buses, monorails, ferries and car parks), and critical areas (power or fuel sources, control rooms etc.) according to the environment and the transport operator's needs. Major airports or other large transport precincts also have CCTV systems, with coverage appropriate to the operational, safety or enforcement purposes of the precinct owners, tenants or government.

The intended uses of the CCTV system influence the installation locations and the type of technology used. For example, CCTV equipment installed for law enforcement or evidentiary or safety purposes is likely to be installed in locations different from those used by a public transport operator for traffic flow monitoring, and it will generally be designed to meet higher performance and technical specifications.

3.2 System Components

CCTV systems consist of cameras, monitors, recorders, interconnecting hardware and support infrastructure. Images may be transmitted via wired or wireless technologies in digital or analogue form. New installations are usually digital, but may incorporate analogue cameras or legacy analogue equipment interfaces. With the exception of legacy equipment and specialist CCTV keyboards, most system components draw on technology used by the information and communication technology (ICT) industry, including image storage and processing, and interconnecting IP network hardware. Images are usually recorded on hard disk or solid-state disk technology. Some CCTV operators do not record imagery, because it would not be cost-effective or practical, or because real-time monitoring meets their operational needs.

3.3 System Monitoring

CCTV can be monitored in three ways:

- *Active*. In some crime-prevention tasks, trained personnel use cameras actively to conduct surveillance of areas in support of law enforcement or security officers on the ground. Similarly, transport control personnel use CCTV systems to manage signals or controls to balance passenger and vehicle flows and automated responses to highlight exception-event triggers. Historically, the active use of CCTV has mostly been in operational functions; more recently, active use for crime prevention has increased.

- *Passive*. More traditionally, CCTV camera systems are used passively. An employee merely monitors a small number of television screens showing a selection of available CCTV footage (often in conjunction with, or incidental to, other duties).

- *Recording*. CCTV systems may record images whether they are monitored or not. Such records may be accessed and used for intelligence, investigative or evidentiary purposes. How much is retained, and for how long, are determined by needs, cost-effectiveness and practical limitations. Traditionally, transport operators retain records for only a limited time.

In some environments, all cameras in a CCTV system are monitored; more commonly, in large systems, no more than a small proportion of cameras, if any, are monitored live. In the latter cases, imagery is only examined when required—either live or from recordings.

Some CCTV systems can be supervised by personnel in monitoring centres, which can be designed for transport operational, security or policing functions, or a combination of these. Monitoring in centres may be general or selective. Selective monitoring may be to detect events of interest, in response to reports of incidents, or in response to security or operational alarms. Alarms may be triggered by switches or detectors, or by the automated processing of CCTV imagery.

In simpler or dispersed CCTV systems that do not use monitoring centres, the same functions are performed by people watching monitors in their work locations, as an incidental part of their duties.

3.4 CCTV for Counter-Terrorism Purposes

The Code addresses the four main uses of CCTV in counter-terrorism:

- monitoring, surveillance, deterrence and intelligence gathering
- assessment and response to a possible incident
- assessment and response following an actual incident
- forensic and evidentiary analysis after an incident.

The extensive use of CCTV in the transport sector is generally designed to aid operational management, to deter or detect wilful damage, theft or minor assault, and for border control purposes. Most original systems were not designed for counter-terrorism. CCTV systems in the sector vary widely in their coverage, resolution, capabilities and technical quality.

Current and potential owner/operators of CCTV imagery obtained in or around transport infrastructure include: law enforcement agencies; emergency services; national security and intelligence services; government infrastructure agencies; mass transit operators; other critical infrastructure operators; municipal councils; courts and parties to litigation; private venue operators; and security monitoring companies. The processes for managing these owner/operators' access to CCTV imagery and associated data are subject to information privacy legislation and, in some areas, codes of practice. This is particularly relevant where law enforcement requires CCTV data to be shared between jurisdictions.

Section 4 Recommended CCTV System Guidelines to meet Operational Objectives

4.1 Applying the Code

Application of the Code begins with a risk assessment and site evaluation of the transport service. Tables are then used to link security operational objectives to determine the recommended recorded imagery output, leading to selection from within a range of recommended CCTV performance criteria.

Existing CCTV systems can then be assessed against the performance criteria, or new systems can be designed to comply with the criteria.

In more detail, the process involves:

1. Determining a **transport security priority** (*Priority 1—the highest priority, Priority 2, Priority 3, Not Applicable*) for the transport service through a risk assessment for the purpose of this Code.

2. For each transport security priority, recommending **operational objectives** (*Monitor*, *Detect*, *Recognise* or *Identify*[4]) in relation to people, objects or vehicles for typical areas within the infrastructure:

   - *Monitor* Monitor/observe the flow of traffic or movement of people generally—not individual figures.
   - *Detect* Detect the presence of a person without needing to recognise or identify them.
   - *Recognise* Recognise somebody who is known to the user, or determine that somebody is not known; monitor or track an individual person, object or vehicle.
   - *Identify* Capture enough detail to identify a person, object or vehicle beyond reasonable doubt.

3. For each operational objective, setting recommended **performance criteria** for CCTV systems[5].

---

[4] These definitions are informed by the UK Home Office document, *CCTV Operational Requirements Manual, 2009*, which is generally considered to represent international good practice. In particular the descriptors *"monitor", "detect", "recognise", "identify"* are consistent with the UK Home Office approach, as are the intent and meaning of their respective definitions.

It should be noted that the UK Home Office document was preceded by several years by the relevant Australian Standard (AS 4806.2–2006: *Closed-Circuit Television (CCTV)—Part 2: Application Guidelines*), which provided guidance along similar lines and is still in force.

[5] The relationship between sector-specific security functions and operational objectives is detailed at Appendix D, Tables D1, D2, D3 and D4.

Using this methodology avoids the need to define arbitrary, technology-specific standards for all the possible combinations of cameras, recording and transmission systems, image resolution, lighting, and IT networks.

4.2 Determining the Transport Security Priority

The Code recommends the grading of types of transport through transport security risk assessments for each transport service and/or for critical parts of the service. This will determine the **transport security priority** (*Priority 1—the highest priority, Priority 2, Priority 3*, *Not Applicable*).

The transport security priority should be informed by:

- available current threat information
- jurisdictional and national priorities
- local security issues and circumstances
- a security risk assessment conducted by the owner/operator.

Transport security priority ratings should not be confused with national alert levels or threat assessment levels, which are inputs to the security risk assessment process.

The transport security priority provides guidance on where and how extensively investment in CCTV should be prioritised for particular transport modes or parts of transport systems.

For example, the Code may be applied (at any of the three transport security priority levels) to one or more of:

- security-identified surface transport operations (SISTOs) determined by jurisdictions under the *Intergovernmental Agreement on Surface Transport Security*
- transport areas identified as being 'critical infrastructure', as defined in the *National Counter-Terrorism Committee National Guidelines for Protecting Critical Infrastructure from Terrorism*
- mass passenger transport systems that have been assessed by the Australian Security Intelligence Organisation (ASIO) as being at a given threat assessment level (of, for example, 'medium' or higher)
- transport facilities subject to security regulation within the jurisdiction (for example, under the Commonwealth *Aviation Transport Security Act 2004* or the Victorian *Terrorism (Community Protection) Act 2003*).

Specific warnings of terrorist attacks are unlikely, so vulnerability-based assessments should be used in risk assessments in addition to intelligence-based threat assessments provided by government. This will allow prioritisation to include broad consideration of such factors as terrorist capacity and typical actions, asset significance, and the possible consequences and impact of potential attacks. The vulnerability of the whole transport system should be taken into account in determining the relative transport security priority for each area.

Where the transport security priority is assessed to be 'Not Applicable', elements of the Code may provide an appropriate benchmark for the selective application of some aspects of CCTV systems, such as coverage of key areas, evidentiary requirements or operational procedures.

4.3 Determining Operational Objectives

The applicable security functions to be fulfilled should be identified for each security-assessed site. These are explained in Table D.1 in Appendix D and relate to operational objectives, which are in Tables D.2 to D.4. The CCTV performance criteria recommended for each operational objective are shown in the tables in Appendix E, in particular Tables E1, E2 and E3. Operational objectives should be determined for each camera within a CCTV system.

4.4 CCTV System Performance Criteria

4.4.1 General Principles

Mass passenger transport systems are vulnerable to terrorist attack. CCTV contributes to the application of 'security-in-depth' principles to such systems and should be combined with other appropriate security measures.

The value of CCTV lies in its ability to record what happens and to provide live images for prevention, response, investigation and evidentiary purposes. The underlying requirement of authorities responding to a terrorist incident is to know what has happened and who did it. Secondary benefits include the identification of suspicious behaviour or objects before an incident takes place. The performance criteria in this Code relate to the recorded image product rather than camera or transmission performance.

Ideally, CCTV systems across a mass passenger transport system would capture images that could be used to *identify* people within the system and to record images of all activity taking place across the system. After assessing identified risks, it is not usually appropriate to implement CCTV systems of such magnitude. However, for counter-terrorism purposes, the aim should still be to capture images to identify *all* people within the system, and to record activity at *key* locations identified by an appropriate risk assessment. Operational objectives can be identified that will aid the appropriate placement of cameras and selection of appropriate image quality and capture rates.

Once a high-quality image with enough detail to *identify* a person has been captured, other images can be captured that will allow for *recognition* of that person in other areas of the system. This will support the principal aim of providing investigators with information that helps determine what has happened and who was involved.

The combination of three levels of *transport security priority* with four *operational objectives* allows for up to 12 levels of CCTV *performance criteria*, to cater for the wide range of security circumstances across transport systems.

The performance criteria for image size are included in Table E.1 in Appendix E. The criteria for image resolution and image capture rates are described in Section 4.4.2, and a reference example for image resolution is given in Table E.2 in Appendix E.

4.4.2 Image Capture Rates

The rate at which images are captured and stored is one determinant of the amount of storage media required in a CCTV system. As such, intelligent design processes that focus on issues such as camera numbers and location, environmental lighting, target speed across fields-of-view and camera shutter speeds should be applied using appropriate frame capture rates to ensure the operational objective of each camera is achieved.

Image capture rates should also be determined, consistent with the operational objective, to ensure that:

- a monitoring officer can make an informed decision about what is happening within view of the camera
- recorded images are suitable for analysis by investigators and the courts and show what actually happened consistent with the nature of the threat.

Issues to consider include:

- recording mode (continuous recording, recording in response to activity detection, recording triggered by an alarm device or by software, time-based recording schedules) to ensure a record of any relevant activity within the field-of-view
- allocation of limited recording resources to areas of higher risk or priority
- network and storage capacity for future frame rate increases
- retention of recordings.

Image quality is of paramount importance. While required image capture rates can vary significantly depending on the operational objective for a particular camera, high capture rates should not be sought at the expense of image quality. Users must be careful to ensure that the chosen frame rate captures the required information and permits video analytics processing to operate correctly, if implemented.

4.4.3 Image Resolution

Resolution is the measure of detail and clarity of a still or video image. It is not a measure of the size of the image. In an end-to-end CCTV system, video image resolution is determined by the:

Image Capture:

- dome/window optical quality and cleanliness
- the quality of the camera lens
- lens focus
- type, intensity and arrangement of lighting
- the type and quality of the camera
- camera electronic shutter speed
- target velocity

- type and profile of digital video compression
- transmission system capabilities
- recording and display system capabilities.

Image Display/Replay:

- the resolution of the display device
- the scaling of the image for display
- transcoding of images for export to removable media or remote access
- transmission system capabilities
- recording and display system capabilities.

Digital video compression occurs at the camera, recorder or intermediate box and is called 'encoding'. Decompression for display usually occurs at a PC attached to the display monitor and is called 'decoding'. Together, the compression-decompression software is known as the 'codec', which generally uses standards-based algorithms (e.g. MPEG4, H.264, JPEG 2000) with a range of settings that govern the video image's size, rate and resolution. These settings are limited by the processing requirements of the codec and the capacity of the network available to transmit and store the video data.

Objectives of the codec settings are to: minimise the required processing power, maximise the image quality and minimise the resulting data volume. Standard 'profiles' have been established that attempt to optimise aspects of all three objectives. Manufacturers may make further adjustments, allow users to adjust the settings, or provide automatic functions to optimise the configuration depending on dynamic conditions such as time of day, external alarm or movement in the camera field-of-view and network and system load.

Codecs providing high compression ratios and low data rates may require more powerful processors or produce low-quality images. As processor power, data bandwidth, storage capacity and camera quality all influence the cost of the design, the resulting digital video quality is also directly linked to cost.

In a post-incident review, the resolution of the recorded video will be considered most important. At that point, the resolution will have been affected by all the components forming the CCTV system. Video exported for review by external organisations may include a software copy of the native system codec to help ensure image replay is at optimum quality.

Various objective test charts available from industry (for example, the RETMA, IEEE-208, ViDi Labs and the draft National Institute of Forensic Science (NIFS), Electronic Evidence Specialist Advisory Group draft chart) use patterns of converging lines to enable the visual measurement or rating, in horizontal TV lines, of the resolution of a complete CCTV system. Test-pattern generators can also be used to measure visually the resolution performance of a digital video recorder separately in systems with analogue camera inputs. The Australian Standard *AS 4806.2—2006: Closed-Circuit Television (CCTV)—Part 2: Application Guidelines* gives further details of objective testing techniques for resolution using test charts and test-pattern generators for analogue and Standard Definition digital systems.

To establish a rating scale of resolution performance that could be used to set standards for the Code against the operational objectives of *monitor*, *detect*, *recognise* and *identify*, user instructions for the particular test chart or test pattern generator selected should be reviewed. Table E.2 in Appendix E gives parameters, using the ViDi Labs and draft NIFS test charts, for the video resolution required for *monitoring* behaviour, *detecting* an incident, *recognising* people or vehicles, and capturing facial detail or reading number plates for the purpose of *identification*. To aid interpretation of Table E.2, an example of the layout of the ViDi Labs and draft NIFS test charts are in Figures E.4 and E.5.

CCTV systems to which this Code applies should achieve resolution results equal to or better than those indicated in Table E.2. By configuring various alternative test charts and pattern generators in accordance with their manufacturers' recommendations, objective testing can be carried out using manufacturer-designed parameters to identify levels of resolution acceptable for all operational objectives.

Regardless of the objective testing technique applied, evaluation through observation should be carried out at commissioning, and regularly audited, to confirm that the relevant operational objectives are being met. Evaluation should also consider performance under night-time lighting conditions.

4.4.4 Intelligent Software

A range of products are available to automate CCTV systems by analysing images using computer programs. The benefits of these products include a reduced reliance on live monitoring of systems by personnel. There can also be significant savings in recorded vision storage, as systems can be configured to record only specific incidents or events in areas with infrequent activity. Software designed to record or alert when movement or specific types of events are detected can assist in detecting suspect incidents, provided they are configured appropriately.

Intelligent software or 'video analytics' can also be used to avoid recording any irrelevant activity needlessly (for example, by interpreting the entry of pedestrians into train tunnels as an abnormal event and recording it, but not recording the routine entry of trains).

Using intelligent software in conjunction with CCTV for counter-terrorism purposes requires caution. Software designed to record specific actions (such as 'left objects', 'removed objects', or movement direction counter to pedestrian flow) will not record all activity within the view of the camera and therefore might not record an actual terrorist incident or preparations for it. While intelligent software has a role in CCTV networks, it should generally be used to complement or reduce the requirement for live monitoring and unnecessary recording at key locations, but not to replace them.

Appendix B summarises possible technological solutions, in particular Tables B.1 and B.2.

4.4.5 System Guidelines to Meet Operational Objectives

The design of the CCTV system should be guided by the performance criteria for each operational objective, and for each of the nominated areas indicated in Tables D.2 to

D.4 in Appendix D for the respective mode of mass passenger transport. Where the tables do not define an operational objective, the operator should be informed by the risk assessment and a comparison with similar contexts, or by the requirements or guidance of the security regulator.

For each *transport security priority rating* (*Priority 1—the highest priority, Priority 2, Priority 3*), the Code recommends typical areas within transport services for setting *operational objectives* that lead to *performance criteria* for CCTV systems commensurate with the risk.

4.4.6 Data Networks for Digital Video Systems

Most data distribution networks use cabled Ethernet with RJ45-connected unshielded twisted pair cables, optical fibre cables, or local wireless transmission, with a series of network protocols complying with the 'TCP/IP model'. This is often referred to generically as an 'IP network'.

IP networks are divided into Local Area Networks (LANs) and the Wide Area Network (WAN)[6]. Design of a network to transmit video data requires an understanding of how much data is involved, its source, destination, sensitivity, required availability and the consequence of delays or losses. This will dictate the design of the LANs, the WAN and the interface between them. Some considerations that need to be made in planning Data Networks for digital CCTV systems are included in Appendix B.

While in simpler IP networks the components can be 'plug-and-play', more complex video systems require networks that adequately consider the CCTV data demands. Input from IT professionals should be sought early in the planning process.

4.4.7 Performance and Interoperability

Interoperability refers to both the ability of CCTV system components to operate together on the same network and on the ability to share video between networks or jurisdictions. This is outlined previously at Section 2.4.1.

At the procedural level, it is important to identify other parties with which interoperability may be desirable or beneficial. Establishing these arrangements is a critically important element of planning for a CCTV implementation and should include agreed procedures for interoperability and the technical means by which it will occur.

At the technical level, interoperability relies on the manufacturer's interpretation and implementation of relevant standards. Analogue video interoperability needed few standards and variables. Digital CCTV systems rely on far more, many of which are optional or whose detailed implementation varies from one manufacturer to the next. Standards for digitising and encoding video streams are well-established though video conferencing, broadcast and entertainment markets, with most CCTV systems able to accept video images from equipment produced by multiple manufacturers. While this provides digital CCTV interoperability at the same level as an analogue system, digital systems have far greater interconnectivity, far more capabilities and, therefore, far more functions and variables requiring a common interface.

The Open Network Video Interface Forum (ONVIF) has emerged as the primary industry body driving CCTV interoperability standards, offering highly detailed

[6] Metropolitan Area Network (MAN) arrangements offered by some carriers provide cost and bandwidth advantages over a WAN, but without the same geographic coverage.

specifications for functions supported by, and communications between, video transmitters, displays, recorders and video analytics devices. The specifications include provision for metadata streams with elements for analytics, control and events.

While uptake of standards is increasing, ONVIF compliance does not mandate implementation of all provisions of the specifications and therefore does not guarantee that devices will be interoperable across their full functional range. Transport operators must ensure that specific requirements for interoperability are well-understood, justifiable and clearly specified when procuring CCTV equipment. Over-specification will limit the availability of compliant equipment, while under-specification may result in equipment that does not meet interoperability requirements. It is recommended that interoperability capabilities are fully demonstrated prior to committing to a specific product.

4.4.8 Storage Periods for Images and Other Data

It is recommended that video images are stored for 31 days in accordance with Australian Standard 4806.1–2006: *Closed-Circuit Television (CCTV)—Management and Operation.*

4.4.9 System Protection and Redundancy

In applying this Code, CCTV systems should be configured, installed and operated to provide reasonable protection from natural hazards and human interference in the relevant environment, and to provide redundancy and reliability of operation consistent with the assessed risks. This includes consideration of:

- system architecture to achieve prudent redundancy of networks and recorded imagery
- selection of components for resilience and suitability for the environment
- redundancy of electricity supply to key components, with preference for backup power and surge protection
- redundancy of communications and transmission paths
- adequate operational management and maintenance arrangements to support system availability and reliability relevant to CCTV networks
- lighting.

All recorders, database servers and workstations should be time-synchronised, preferably to a Stratum 1 time source. Clear understanding is required as to how the system deals with daylight-saving changes and the potentially duplicate or missing video timestamps.

All field equipment should be rated for the industrial environment and require minimal maintenance. Restart following restoration of power after a failure should be automatic, with all devices returning to a known defined state or to the state prior to the power failure.

WAN connections should have suitable resilience to ensure post-incident access to imagery. This might be in the form of path diversity and self-recovery.

System configurations need to provide adequate security and privacy safeguards. Remote connections through the CCTV network to workstations *outside* controlled areas should be secured by firewall or similar at both ends (the CCTV network and the remote site). Wireless links should include security mechanisms to limit the risk of unauthorised access to or interruption of the network.

4.4.10 Camera Positioning and Features

Operational needs will dictate the choice, number and positioning of cameras. A basic network of fixed cameras ensures that all activity is captured at some level. Additional pan–tilt–zoom cameras allow close-up monitoring in real time.

In selecting and installing cameras, consideration should be given to the physical environment and the features that may be required in cameras or supporting infrastructure. Such considerations should include, but not be limited to:

- placement of cameras at strategic 'choke' points to provide continuous coverage at transport hubs, such as all entry/exit points and escalators or stairways
- the placement, density and types of cameras to meet the operational objectives
- cameras used to monitor traffic flows in and around mass passenger transport sites
- the combination of numbers of fixed-aim cameras and the image capture rates of cameras for all monitoring purposes (which should enable the movements of a person or vehicle to be clearly evident, and should be of a standard accepted by the courts)
- the preventive functions of the CCTV system (which aid specific identification, in areas of interest, of all individuals and the detection of abandoned packages, bags, vehicles etc.)
- where possible, camera placement should ensure at least one *identify*-grade view of each person
- locating cameras in respect to privacy issues
- locating cameras in respect to their susceptibility to theft, tampering and vandalism
- siting cameras so that people normally approach them through that camera's field-of-view
- installing cameras so that each is covered by another camera's field-of-view
- the use of cameras with greater low-light sensitivity in areas where artificial lighting is limited
- the use of housings incorporating measures to mitigate against the easy determination of the camera's field-of-view
- the use of housings incorporating measures to mitigate against the effects of extreme weather or grime
- back-up power supplies for cameras and CCTV systems

- incorporation of pan-tilt-zoom cameras that will allow staff to control cameras to follow and 'close in' on persons, objects or vehicles
- positioning cameras to enable any selected video analytics detection technologies to operate correctly
- positioning cameras to enable economical periodic maintenance
- siting cameras and selection of suitable camera technology for the lighting conditions.

Thermal imaging cameras, which can sense body heat and operate without any lighting, should be considered for emergency coverage of locations that rely permanently on artificial lighting, such as tunnels and underground facilities, where the additional cost may be warranted.

Megapixel cameras have higher resolutions and may permit area coverage with fewer cameras. Megapixel camera lenses must provide increased optical quality to enable the full resolution of the camera to be achieved. Unlike good quality optical zoom lenses, the use of digital zoom reduces image resolution and its use must always be considered in line with resolution requirements required to meet the o*perational objectives*.

4.4.11 Imagery Recording Equipment

Imagery recording systems (recorders and storage devices) should be in lockable enclosures to protect against unauthorised access or vandalism, suitably mounted, and protected from vibration, shock, dust, water, electromagnetic interference, and disconnection or loss of power.

Imagery should be stored securely to protect it from blast, fire, smoke, chemical or other damage during a terrorist attack on the area covered by the CCTV system. Storage devices for mobile systems (on vehicles) should be reasonably well-protected from wilful damage and unauthorised access. In fixed systems, consideration should be given to offsite video data backup.

Section 4.4.8 recommends 31 days storage. When the recording system reaches capacity, it should automatically overwrite from the beginning of the pre-recorded material. Overwrite protection of security identified material should cause that material to be retained during this process.

Hard disk drives and other storage media should not need regular routine maintenance, such as defragmentation, to remain functional. Multi-disk arrays are preferred for video storage to improve system reliability through redundancy. In the event of failure, the array should provide clear indication of which disk has failed and permit 'hot swap' of the failed unit without power down or loss of data. Consideration should be given to the use of RAID-6 configuration in larger systems to provide fault tolerance for multiple drive failures.

Removable media, including hard disk drives, should be indelibly marked with a unique identification number to enable recognition in legal proceedings. Mechanisms for export of video data from the CCTV system in industry-standard format should be available and clearly understood, including options that may affect the resolution, integrity and accessibility for third-party replay. System design should consider

bandwidth, storage and processing requirements associated with video image export and must ensure all other system functions proceed uninterrupted during the export process. Removable media should be housed in suitable protective enclosures for transportation, to protect them from rough handling, dropping, or unauthorised access.

4.4.12 Monitoring, Reviewing and Archiving

CCTV monitoring centres should be in secure locations where they are unlikely to suffer from criminal attack or from damage during a terrorist attack on the transport service being covered by the CCTV system. Australian Standard *AS 2201.2–2004: Intruder Alarm Systems—Monitoring Centres* specifies requirements and a grading convention for monitoring centres and the operations, equipment and staff necessary to monitor intruder alarm systems. The standard is a useful guide to security and design features that should be considered for high-security monitoring facilities.

Recommended options for retrieval and viewing of stored images are via:

- a high-bandwidth communications link from the location, either continuously or as required and/or
- export to removable media (CD, DVD, BD or USB HDD).

A user-friendly interface should allow reviewing (at user-selectable playback speeds) and archiving of images to high-capacity medium, such as DVD/BD. Recorded images should be exportable in file formats that allow viewing in a range of common desktop applications. Off-line reviewing equipment should be able to view imagery from other CCTV systems without requiring proprietary formats. The equipment should be able to display onto common display(s), in synchrony, those selected from all of the video streams recorded at a particular location, whether or not an alarm mode has been activated.

Reviewing software should have a user-friendly graphical interface that allows searching by time, date, camera identifier, location or vehicle identifier, normal/alarm condition etc.

4.4.13 Operating Procedures

Controlled system management and operating procedure documents should be developed and implemented to meet the principles identified in this Code, including:

- operational objectives
- technical operating requirements
- training requirements and proficiency accreditation
- fault rectification and preventive maintenance
- security of hardware, software, communications and imagery
- system integrity
- redundancy
- adequate documentation of the system (location, coverage), available to operators and law enforcement agencies

- change management
- disaster recovery.

4.4.14 Maintenance Procedures

It is recommended that planning for CCTV systems includes maintenance contracts with service-level agreements and/or defined periodic maintenance tasks. Maintenance must include cleaning of camera housings or domes at intervals matched with the environmental conditions.

Formal procedures for fault reporting should enable operators to describe the nature of a problem and maintenance staff to report the cause and remedial action required. Maintenance documentation should include task intervals and details. Records should include confirmation of all tasks carried out, with provision for comment by maintenance staff regarding deterioration or other issues requiring attention.

Most digital CCTV systems and data networks provide facilities for remote electronic access to equipment to enable status, condition and fault analysis to be conducted from a central location. System design should consider what information is available remotely that may be usefully presented to assist in system management, cost-effective maintenance and reduced down-time.

Maintenance procedures should ensure periodic verification of CCTV system performance in accordance with the design objectives.

4.4.15 Relevant Standards

The Code is not designed as a uniform, 'one-size-fits-all' prescription or specification. It supplements other guidance material, the application of which is determined by each jurisdiction's transport security risk assessments and legislation.

The Code is to be read in conjunction with the provisions of relevant industry technical, safety and procedural guidelines, including but not confined to those listed in Appendix C.

The standards are not prescriptive beyond a certain level of detail and can be applied to suit individual circumstances. They require some expertise to be implemented properly, and are not a substitute for employing suitably experienced and qualified personnel. Rather, the standards help qualified personnel ensure that their work complies with national or international norms. A given situation may warrant measures substantially beyond the baselines prescribed in a standard.

Part C Legal and Procedural Aspects

Section 5 Legal Issues and Accountability

5.1 Purpose of this Section

The purpose of this section is to provide information and guidance on the legal aspects of CCTV, in particular the coordination of owner/operator activities, information sharing between jurisdictions, seizure and use of data under emergency powers, management of CCTV data for evidentiary purposes, and privacy.

5.2 Legal Context

5.2.1 Responsibilities

Australian Governments are responsible for determining the legal implications of using CCTV for counter-terrorism purposes and in applying the Code. This includes the assessment of legal frameworks (including privacy, workplace relations and surveillance legislation associated with the collection of personal information). At COAG's Special Meeting in September 2005, all governments agreed to identify necessary legislative schemes to ensure consistent implementation of the Code.

Compliance with privacy-related legal safeguards on the use of CCTV is needed to ensure that the impact of any proposed legislative amendments on existing privacy provisions is minimised.

Other legal considerations may arise from time to time and may be specific to particular jurisdictions. Care is necessary to ensure that the legal implications of CCTV implementation are understood and have been considered in planning. Owner/operators are obliged to inform themselves of all legal implications and, in the first instance, are well-advised to consult with their jurisdiction's transport security regulatory authority.

It is the responsibility of the owner/operator to ensure that its CCTV installation is compliant with relevant Commonwealth, State and Territory law and Local Government bylaws. Owner/operators are also obliged to inform themselves of the penalties for non-compliance.

This will assist in deterring unauthorised use of the system and supporting compliance with legislation. Policy and procedures should then be tailored to outline use of the system in accordance with relevant legislation[7].

This should also include simple and easily implemented principles, such as:

- People are entitled to a reasonable expectation of privacy when in public places.
- Owners and designers of CCTV systems in public places should act responsibly and consider the reasonable expectations of privacy of individuals.
- Owners and designers of CCTV systems in public places should take reasonable steps to inform people of the use of those devices.

[7] Western Australia, 2009. *Closed-Circuit Television (CCTV) Guidelines.*

- Public place surveillance should be for a legitimate purpose related to the activities of the organisation conducting it.
- Public place surveillance should be proportional to its legitimate purpose.
- Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure.[8]

5.2.2 Legal and Procedural Issues for Ongoing Consideration

In applying the Code, owner/operators may need to consider several legal and procedural issues. These include:

- privacy, including personal information and images
- access to CCTV imagery through freedom of information and other legal mechanisms
- lawful disclosure
- signage, telling the public where CCTV is in use
- protection of information
- permitted uses of images
- automated image recognition or data matching
- ensuring that timely and complete investigations are made of significant incidents, and there is a process for police to obtain data recorded by CCTV systems in public areas by using formal requests without warrant
- retention and disposal of information (which is connected with operational requirements and storage capacity)
- complaints resolution
- registers or databases of CCTV systems
- strategic land-use planning and development controls
- workplace safety.

Owner/operators will also need to address aspects related to incident response, such as how CCTV images from a variety of sources may be collected and stored promptly for future access, and mechanisms to best allow the exchange of data during and after incidents.

5.3 Onus on Owner/Operators to Report Incidents and Suspicious Activity to Assist Counter-Terrorism

To assist with the effectiveness of counter-terrorism measures, owner/operators of CCTV systems should put in place procedures and training for system monitoring that provides that any suspicious activity detected by their personnel is recorded and promptly reported to police (or other appropriate agency).

---

[8] The Victorian Law Reform Commission, 2010. *Surveillance in Public Places Final Report 18.*

5.4 Privacy

When installing CCTV systems, owner/operators must comply with the law pertaining to the management of personal information, which is generally defined as:

> *information or an opinion… , whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*[9]

The objective of information privacy law is to provide a legally binding framework for the responsible, open and accountable collection, storage, use and disclosure of personal information.

As most CCTV systems will capture personal information, this has clear implications for CCTV data, as well as for the use of databases against which recognition technology can compare CCTV footage. As with all elements of the law, owner/operators are obliged to inform themselves of, and to comply with, privacy provisions.

5.5 Compliance with Privacy Principles

Owner/operators are encouraged to follow the established good practice of undertaking a Privacy Impact Assessment (PIA) in relation to their existing and planned CCTV implementations. It is particularly important that this be done at an early stage in planning for new implementations. To determine whether a PIA should be undertaken, a Privacy Impact Checklist (PIC) should be completed. This covers a range of questions in relation to the 11 Information Privacy Principles (IPPs).

Further information is available through the Office of the Australian Information Commissioner at http://www.privacy.gov.au, or its successor[10].

In addition, the privacy law provisions are very similar across all jurisdictions and owner/operators may contact their jurisdiction transport security regulatory authority for additional local advice.

To aid compliance with privacy principles in operating a CCTV system, owner/operators should implement an 'operations manual'. This needs to reflect privacy provisions and might include, but not necessarily be limited to:

- setting system objectives and permitted uses of imagery

---

[9] Office of the Australian Information Commissioner. *Privacy Impact Assessment Guide*. Viewed on November 2011 at http://www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=guidelines&fullsummary=6590&Itemid=1021

[10] Guidance on Completing a PIA. Viewed on 4 November 2011 at http://www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=guidelines&fullsummary=6590&Itemid=1021

- setting minimum technical specifications
- community consultation approaches
- defining key agency/organisation roles
- installation and trials
- camera locations and system configuration
- management of liability
- staffing and control mechanisms
- means and circumstances of police access to, and control of, CCTV equipment or imagery
- permissible uses of CCTV imagery (e.g. planning consideration may need to include the needs of third-party providers in upgrading systems where access to footage may be required)
- permissible means/procedures for releasing CCTV imagery
- archival and document retention methods, including destruction
- permissible uses of any related surveillance technologies (such as number plate recognition, facial recognition or behavioural monitoring)
- complaints handling and resolution
- monitoring and assessment
- audit and compliance monitoring.

5.6 Evidence-Handling Procedures

5.6.1 Emergency Access to Data

Access to CCTV data may lawfully be required by relevant State or Territory or Commonwealth law enforcement authorities under warrant for counter-terrorism or other law enforcement purposes. It is good practice for owner/operators to maintain up-to-date awareness of requirements under emergency powers and their jurisdictions' evidentiary requirements through awareness training of relevant staff. Advice on emergency provisions regarding CCTV data and related evidentiary requirements should be sought from the jurisdiction police service.

Law enforcement authorities prefer real-time or near real-time access to CCTV systems in areas of high transport security risk for counter-terrorism purposes. Some transport facilities, such as major airports, have a standing law enforcement presence for which monitoring facilities are, or could be, provided.

The provision of such data should be subject to a formal agreement between the CCTV owner/operator and the agencies, addressing the intended and permissible use of imagery, and information security and privacy controls and accountabilities.

5.6.2 Evidentiary Responsibilities

CCTV systems should be designed and implemented to ensure that the imagery recovered from recording media could not reasonably be alleged to have been altered from the original view of a particular camera at a known point in time. The admissibility of evidence can be improved by using appropriate technologies (such as system access controls, electronic watermarks, image labelling, encryption and logging), and by strict procedures (such as for physical access, storage, media labelling, training and custody/possession). Strict adherence to data management that is consistent with provision of a clear chain of evidence is critical. Courts may also require information on system configuration, camera location and operation, video extraction, labelling, storage, handling and transportation.

In addition, owner/operators need to maintain adequate processes, mechanisms and capabilities regarding system and data integrity and not be entirely reliant on third-party suppliers or installers. This includes capabilities regarding proper recording and registering consistent with the jurisdiction evidentiary requirements.

Forensic handling of imagery by law enforcement authorities and other agencies should be consistent with authoritative guidance at least equivalent to the 2004 *Australasian Guidelines for Digital Imaging Processes*—prepared by the Electronic Evidence Specialist Advisory Group under the auspices of the Senior Managers Australian and New Zealand Forensic Laboratories.

Those guidelines advise:

> *The development and adoption of methods of best practice with respect to the gathering and presentation of any evidence is essential to ensuring that such evidence is accepted by the courts. It is also essential that the methods employed are constantly reviewed and improved to keep pace with the ongoing advances in technology.*
>
> *This is particularly so with respect to digital imaging, given that its associated technologies permit digital images to be easily duplicated, manipulated, contaminated, or altered. It is self-evident that digital imaging is assuming an ever-increasing importance within the judicial process today and this situation will no doubt continue well into the future. In light of this, it is imperative for forensic science practitioners and agencies to be able to validate the origin and integrity of not only the digital images themselves, but also the image capture and handling procedures employed in the gathering, processing and analysing of this type of evidence, especially when digital visual images are to be used for evidentiary purposes.*

In turn, management and handling of CCTV data by owner/operators needs to be consistent with jurisdictional evidence-handling procedures.

5.6.3 Advice on Jurisdictional Practices

Additional advice should be sought from the jurisdiction police service and the transport security regulator on these matters early in planning for a new or upgraded CCTV

system. This advice should include, but not necessarily be limited to, the proper procedures for the capture, transmission, storage, retention, disclosure, protection and disposal of imagery and to enhance admissibility in court proceedings.

5.7 Jurisdictional Capabilities for Reviewing Mass CCTV Product

Owner/operators should prepare a plan for ensuring a timely response to the need to review large quantities of CCTV product after a major incident.

During a major counter-terrorism investigation involving mass passenger transport CCTV systems, police and other agencies may need to access, review, analyse, store and present evidence from substantial volumes (potentially petabytes (10^{15})) of digital imagery, numerous analogue tapes, or both. As a priority, police and relevant agencies should ensure that they have assessed the potential requirements and resource implications of such an investigation, including the identification of suitable accommodation, equipment, personnel and funding.

This might be in the form of a non-linear video editing suite with the ability to import and synchronise video from multiple sources to frame accuracy, with tools for real-time synchronised replay, image enhancement and automated post-event analysis and enhancement. Not all owner/operators will possess such equipment, but it should be available within a short timeframe for video upload and analysis.

5.8 Registers of CCTV Systems

It is good practice for jurisdiction authorities to compile and maintain a register of CCTV systems in mass passenger transport systems, identifying their capability and scope for counter-terrorism purposes. A cooperative, voluntary 'partnership' approach between police and CCTV operators without legislative formalities is the preferred approach.

This would require owner/operators of CCTV systems to provide government with adequate information on their systems to maintain the register. Where maintaining jurisdiction-wide registers is not possible, up-to-date registers of points-of-contact in other jurisdictions should be maintained.

5.9 Related Legislation and Standards

This Code is to be read in conjunction with the provisions of:

- Relevant legislation involving:
  - CCTV and other security systems, practices and licensing
  - CCTV devices
  - information privacy
  - admissibility of evidence
  - transport safety and security
  - police and emergency services.

- Relevant industry technical, safety and procedural guidelines, including the Australian Standards 4806 series relating to CCTV, and Standards Australia's *Handbook 171 Guidelines on the Management of IT Evidence* (see Appendix C for further information about standards).

As noted, the Code is not designed as a uniform, 'one-size-fits-all' prescription or specification, but supplements other guidance material determined by each jurisdiction.

Owners and operators of CCTV systems need to take into account local legal requirements and prepare specifications and operating procedures appropriate to their specific situations.

5.10 Safety in Design

CCTV design should be informed by safety-in-design principles, in particular public safety and the safety of those who will have to install, maintain, upgrade and decommission the system. Important information on safety-in-design principles may be accessed via the Safe Work Australia website[11].

The Australian Safety and Compensation Council has provided guidance on principles of safety in design, as follows:

> *Principle 1: Persons with Control—persons who make decisions affecting the design of products, facilities or processes are able to promote health and safety at the source.*
>
> *Principle 2: Product Lifecycle—safe design applies to every stage in the lifecycle from conception through to disposal. It involves eliminating hazards or minimising risks as early in the lifecycle as possible.*
>
> *Principle 3: Systematic Risk Management—the application of hazard identification, risk assessment and risk control processes to achieve safe design.*
>
> *Principle 4: Safe Design Knowledge and Capability—should be either demonstrated or acquired by persons with control over design.*
>
> *Principle 5: Information Transfer—effective communication and documentation of design and risk control information between all persons involved in the phases of the lifecycle is essential for the safe design approach.*[12]

[11] http://safeworkaustralia.gov.auor its successor.

[12] Australian Safety and Compensation Council, 2006. *Guidance on the Principles of Safe Design for Work.*

5.11 Legal Advice

Owner/operators considering CCTV implementation are well-advised to seek professional legal advice regarding compliance with relevant Commonwealth, State and Territory legal frameworks and Local Government bylaws.

Section 6 Monitoring and Review of the Code

The ongoing management of the Code, including its review in no less than three years, will be the responsibility of the Transport & Infrastructure Senior Officials Committee (TISOC), in consultation with the National Counter-Terrorism Committee (NCTC), reporting to the Standing Council on Transport & Infrastructure (SCOTI).

This edition of the Code was published in March 2012, following the first review, and reflects the review findings and recommendations. The ongoing monitoring and review mechanisms to gauge the Code's effectiveness and to modify it over time will include:

- Evaluating the impact of new technologies and applications of CCTV systems for security purposes
- Evaluating changing terrorism risks [as they relate to CCTV]
- Monitoring the effectiveness of application and utility of the Code in guiding CCTV systems implementation and
- Monitoring legal and privacy aspects.

6.1 Review

This Code provides non-binding guidance regarding the use of rapidly advancing technologies to deal with a dynamic range of threats and risks in complex environments. It aims to develop a national operational model to guide risk-based prioritisation of CCTV performance objectives for counter-terrorism.

The changing environment in terms of technology and security threat and risk necessitates regular review of the Code. Further review in no less than three years, will be the responsibility of the SCOTI in consultation with Australian Governments and the NCTC.

Part D Appendixes

Appendix A Technical Acronyms

ANPR	Automatic number plate recognition
BD	Blu-ray Disk
CCTV	closed-circuit television
CD	Compact Disk
2D	2-dimensional
3D	3-dimensional
DVD	Digital Versatile (or video) Disk
DVR	Digital Video Recorder
FoV	field-of-view
3G	3rd-generation mobile telecommunications
4G	4th-generation mobile telecommunications
H.264	a common standard for video compression
ICT	Information & Communication Technology
IEEE	Institute of Electrical and Electronics Engineers Inc.
IEEE-208	IEEE Std 208—1995 is a target measured in horizontal and vertical TV lines
i-LIDS	Image Library for Intelligent Detection Systems
IP	Internet Protocol
ISR	Intelligence, Surveillance and Reconnaissance systems
IT	Information Technology
HDD	Hard Disk Drive
JPEG	Joint Photographic Experts Group; and a commonly used reference in relation to 'lossy' compression for digital photography
JPEG 2000	Compression using wavelet in lieu of discrete cosine transformation
LAN	Local Area Network

MAN	Metropolitan Area Network
M-JPEG	Motion JPEG—video formats where each video frame or interlaced field of a digital video sequence is separately compressed as a JPEG image
MP	Megapixels
MPEG	Moving Picture Experts Group; and a commonly used reference in relation to audio and video (AV) compression
MPEG-4	Compression of AV digital data to enable network distribution of data
ONVIF	Open Network Video Interface Forum
PC	personal computer
PTZ	pan-tilt-zoom camera
RAID	Redundant Array of Independent Disks
R&D	Research & Development
RETMA	Radio Electronics Television Manufacturers Association
SCADA	Supervisory Control and Data Acquisition
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair cable (Cat-5, 6 & 7)
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

Appendix B New Technologies

General Comment

Introduction of new technology introduces features that distinguish the new product from the competitors. Commercialising new technology may involve developing new methods to house, mount, power, communicate, integrate, display, control and store information associated with the device. As new technology often precedes associated standards, this can lead to manufacturers taking differing implementation approaches. Early adopters of new technology therefore face the possibility of unproven site-specific performance, implementation-specific faults or errors, incompatibility with other equipment, rapid obsolescence, small installed knowledge base and ties to a manufacturer-unique product.

In determining the requirement for CCTV capability based on new technology, it is essential to consider the availability and breadth of relevant local support, the suitability of the technology for implementation in the method intended, operability by existing staff under existing procedures, and interoperability with existing equipment.

Intelligent Surveillance

Intelligent Surveillance software or 'video analytics' allows the interpretation of imagery to:

- identify particular events, such as leaving an unattended bag or suspicious behaviour
- recognise inappropriate motion, or movement in an inappropriate location
- recognise car registration numbers and match them to a database
- recognise that an image of a person is very similar to a reference image.

This technology may assist in meeting operational objectives in support of counter-terrorism in mass passenger transport environments.

These systems may assist in providing automated real-time and post-event system capabilities, such as:

- better capability to recognise suspicious behaviour, activity or objects and alert those monitoring
- better ability to identify individuals in a crowd, in poor lighting and when individuals are partly obscured
- better ability to track individuals in crowds and on 'handover' between systems or cameras
- better CCTV data retrieval and analysis.

Real-time image processing technology in the CCTV industry has been available for over 20 years. The ability of a machine to automatically identify, classify and highlight video content potentially of interest to the user offers significant advantages in the effectiveness of video surveillance in mass passenger transport environments. The

performance of this technology is critically dependent upon its ability to be configured for site-specific conditions, including:

- environmental influences (wind, rain, fog)
- lighting conditions (including target illumination, glare, contrast, shadows, backlighting etc.)
- target distance and direction
- camera position and performance
- non-target related movement in the field-of-view
- movement of the camera.

Without appropriate configuration for site-specific conditions, incorrect targeting will occur, resulting in: nuisance alarms, missed targets or false identification.

Manufacturer's claims with regards to the reliability and capability of CCTV image processing technology will assume limits in site-specific conditions that may or may not apply to every site and camera. Large-scale deployment of the technology should always be preceded by extended duration site-specific evaluation under the conditions expected in the final installation.

Systems may be designed to permit progressive rollout, with simpler proven or less critical functions, such as movement-activated recording or people-counting implemented initially, and more complex functions trialled selectively in important or controlled areas. Note that camera position with respect to the target may vary for each analysis function and requires advance consideration where progressive rollout is planned.

The UK Home Office provides a library of video images that can be used to test intelligent surveillance systems and also offers an independent testing service for these systems (limited detection scenarios only). Products that have been passed by this organisation are granted 'i-LIDS' certification and may be more reliable in conditions similar to the test environment.

High-Resolution Cameras

Following the consumer digital camera technology trend, CCTV cameras are increasingly available with large format image sensors allowing capture of video images with extremely high resolutions. Analogue equivalent images are about 0.3 megapixels (MP), high definition home movie images are up to about 2MP, and single sensor CCTV cameras are available with resolutions over 16MP and multi-sensor cameras with over 50MP.

Large image sizes require higher capacity processors for image compression/decompression, bandwidth for image transmission and hard disk storage. Very high resolution cameras require special handling of the large video data streams, are less likely to provide 25 images per second and may not facilitate interoperability with equipment from other vendors.

Operators considering implementation of high resolution cameras should balance the potential for reduced camera numbers against cost, functionality and interoperability requirements.

Data Networks

Digital data network technology is well-established but continually evolving. Network design should take into account CCTV-specific requirements including:

- the size of the video data stream for each camera/encoder
- the variability of the stream size
- how many different versions of the stream are sent and under what conditions
- if separate streams are sent for each recorder and monitor, or if one stream is shared among all
- if all streams go through a central point such as a recorder or server, or if streams are sent directly from the camera/encoder
- the maximum number of simultaneous streams (in and out) that can be accommodated by the recorder or video analytics processor
- the maximum number of streams that can be processed simultaneously for display on one display device
- how the system deals with requirements for different video rate/resolution on various monitors, recorders or remote access devices
- what happens when video data is delayed, lost or contains errors.

An organisation's operational requirements, commercial arrangements, site conditions, existing infrastructure and risk management strategies may also dictate aspects of network design, including:

- compatibility with corporate networks
- network path or device redundancy
- power distribution and backup
- environmental ratings
- existing cables, cable pathways, local or wide-area data network availability
- network physical and data security.

Numerous technical standards address these issues, identifying requirements and mechanisms for network design, including:

- maximum cable lengths
- cable data bandwidths (10/100/1,000/10,000 Mbps)
- logical separation of data on a physical network (VLANs)
- prioritising which data gets sent or discarded first (Quality of Service)
- power to devices over the copper data cable (Power over Ethernet)

- broadband Wireless Access (WiMAX)
- mobile Broadband (3G, 4G)
- one-to-one or one-to-many destinations (uni/multicasting)
- wireless connectivity (WLANs)
- security (protection, authentication, authorisation, encryption)
- management (status monitoring, fault investigation, remote configuration etc.).

Table B.1 Technologies for Real-time Situational Awareness

Application / requirement	Features/problems
Facial recognition	• Requires high resolution and extensive database capability • Current face-in-a-crowd technology has low reliability • Requires significant R&D and testing in real environment
Unattended item recognition	• Current technology requires extensive configuration for individual environments, and can have high false-alarm rate • Further R&D required to reduce false-alarm rate and improve analysis of video motion and events
Tripwire	• Current technology with multiple established vendors • Requires appropriate camera position and lighting
External stimulus event triggering	• Devices that detect environmental variations such as infra-red, pressure, light/heat, smoke and/or respond to intruder alarm interfaces (intelligent and dumb) • Integrated in logic-based video analysis and subsequent event management • Further R&D would see ultimate solution based on video analysis, not external components
Number plate recognition	• Read vehicle number plates and highlight targets of interest • Requires specific camera position and target illumination • Established and proven technology
Loitering	• Detects the extended presence of an individual in one place • Affected by proximity to the camera, lighting and crowd conditions • Requires site-specific evaluation
'Man down'	• Detects when someone has fallen over • Affected by proximity to the camera, lighting and crowd conditions • Requires site-specific evaluation
Directional motion	• Detects contra-directional traffic flow • Affected by proximity to the camera, lighting and crowd conditions • Requires site-specific evaluation
Gait analysis	• Differences in walking style used to biometrically identify individuals
Camera status monitoring	• Automatic detection of camera basic image function • Image is in focus, image is adequately lit, camera has not been obscured or blinded by torchlight
Thermal imagery	• Provides high-contrast images at long distances in no-light conditions • Cannot identify a person or vehicle • Specialist camera, fixed lens and lower resolution
Terahertz cameras	• Detection relies on obstruction of natural passive terahertz radiation • Low resolution and frame rate requires closely defined camera and target positions to be effective. Few commercial products. • Alternative to backscatter x-ray. Should be supplemented with visual images.

Table B.2 Technologies for Post-event Forensic Analysis

Application / requirement	Features/problems
Automated person identification	• Currently requires significant human effort to search • Significant R&D is required to efficiently and accurately search archived footage with low false-alarm rate
Automated event search	• Needs to be tailored to specific application/event • Possibly high false-alarm rate • Can be applied to face matching or to pattern/movement matching • Significant R&D needed for full reliability
Video parameter enhancement	• Manipulation of various image components and temporal or spatial processing to enhance an existing photograph/video segment • Significant R&D for full reliability (limited by quality of original information—requires high frame rate)
3D image analysis	• Development of 3D scenarios from multiple 2D images • Applications need to be enhanced for counter-terrorism work • Significant R&D required
Automatic event reconstruction	• Collection, analysis and meaningful combination of CCTV (and other) imagery from disparate systems (e.g. shops, supermarkets, chemists, liquor stores etc.) to form a 'combined' view of an event from imagery originally recorded for other purposes • Disclosure and privacy regulations need to be considered • Significant R&D for full reliability (problems include different formats, quality etc.)
Non-visible spectrum analysis	• Use of thermal imaging and fluorescent analysis tools (and surveillance systems) integrated with or separate from 'normal' CCTV applications for extra security and/or coverage • Currently very expensive. Needs to be developed, especially for counter-terrorism applications

Appendix C Bibliography

Relevant Standards

The Code is not designed as a uniform, 'one-size-fits-all' prescription or specification. It supplements other guidance material that is applicable according to a jurisdiction's transport security risk assessments and legislation.

The Code is to be read in conjunction with the provisions of relevant industry technical, safety and procedural guidelines, including, but not confined to:

- AS 2201.2–2004: *Intruder Alarm Systems—Monitoring Centres*.
- AS 2834–1995: *Computer Accommodation*.
- AS 4806.1–2006: *Closed-Circuit Television (CCTV)—Part 1: Management and Operation Code of Practice.*
- AS 4806.2–2006: *Closed-Circuit Television (CCTV)—Part 2: Application Guidelines.*
- AS/NZS ISO/IEC 17799—2006: *Information Technology—Security Techniques—Code of Practice for Information Security Management.*
- AS/NZS ISO/IEC 27001–2006: *Information Technology—Security Techniques—Information Security Management Systems—Requirements.*
- AS/NZS ISO 31000–2009: *Risk Management—Principles and Guidelines*.
- HB 171–2003: *Guidelines for the Management of IT Evidence.*
- HB 231—2004: *Information Security Risk Management Guidelines.*
- HB 221–2004: *Business Continuity Management*.

Standards are usually guidelines; they require some expertise to be implemented properly. They are not a substitute for employing suitably experienced and qualified personnel, but help those personnel to ensure that their work complies with national or international norms. A given situation may warrant measures substantially beyond the baselines prescribed in a standard.

Other Potentially Useful Reference Documents

- Attorney General's Department (NSW), 2000. *NSW Government Policy Statement and Guidelines for the Establishment and Implementation of Closed-Circuit Television (CCTV) in Public Places*.
- British Standard BS8495–2007: *Image Export for Evidence.*
- Crime Prevention & Community Safety Council (TAS), 2008 *Policing Requirements for Closed-Circuit Television*.

- Department of Justice (VIC), 2011. *Guide to Developing CCTV for Public Safety in Victoria*.

- Department of Transport & Main Roads (QLD), March 2008. *Recommended Guidelines for the Installation and Use of Closed-Circuit Television (CCTV) in Queensland Buses*—PT 406/03.08.

- Home Office Scientific Development Branch, 2009. *CCTV Operational Requirements Manual*. Downloaded on 14 December 2011 from http://www.nactso.gov.uk/SiteCollectionDocuments/ManagingTheRisk/28_09_CCTV_OR_Manual2835.pdf.

- National Institute of Forensic Science, Electronic Evidence Specialist Advisory Group, 2011. *CCTV Test Chart* (draft).

- Office of Crime Prevention (WA), 2009. *Western Australia Closed-Circuit Television (CCTV) Guidelines.*

- QLD State Archives, October 2010. *Managing Closed-Circuit Television (CCTV) Records—Guideline for Queensland Public Authorities*.

- ViDi Labs, 2011. *CCTV Test Chart*. Downloaded on 4 November 2011 from http://www.vidilabs.com/

Policy Guidelines

- Australian Safety & Compensation Council, 2011. *Guidance on the Principles of Safe Design for Work.* Downloaded on 15 December 2011 from http://safeworkaustralia.gov.au/AboutSafeWorkAustralia/WhatWeDo/Publications/Documents/154/GuidanceOnThePrinciplesOfSafeDesign_2006_PDF.pdf

- Council of Australian Governments, 3 June 2005. *Intergovernmental Agreement on Surface Transport Security*. Downloaded on 4 November 2011 from http://www.coag.gov.au/intergov_agreements/docs/transport_security.pdf

- Council of Australian Governments, 14 July 2006. *A National Approach to Closed-Circuit Television*. Downloaded on 4 November 2011 from http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.pdf

- National Institute of Forensic Science, 2004. *Australasian Guidelines for Digital Imaging Processes*. Downloaded on 4 November 2011 from http://www.nifs.com.au/2004%20Digital%20Imaging%20Guidelines.pdf .

- Office of the Australian Information Commissioner, 2011. *Privacy Impact Assessment Guide*. Downloaded on 4 November 2011 from http://www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=guidelines&fullsummary=6590&Itemid=1021

- Safe Work Australia, 2011. *Safe Design Resources.* Downloaded on 15 December 2011 from

http://safeworkaustralia.gov.au/safetyinyourworkplace/safedesign/Resources/Pages/SafeDesignresources.aspx

- Standing Committee on Transport Security Standing Sub-Committee, March 2011. *CCTV Code of Practice Review 2010-11: Monitoring and Review of the Code*.

- The Victorian Law Reform Commission, 2011. *Surveillance in Public Places Final Report*. Downloaded on 4 November 2011 from http://www.lawreform.vic.gov.au/wps/wcm/connect/justlib/law+reform/home/completed+projects/surveillance+in+public+places/lawreform+-+surveillance+in+public+places+-+final+report

Legal Framework

The legislative framework relevant to a great many elements of society, including the implementation of CCTV systems, changes through time. It consists of a range of primary and delegated legislation in all jurisdictions. It is not possible to detail an exhaustive list of 'current' legislation.

It is the obligation of agencies and owner/operators to inform themselves of their respective legal obligations in relation to CCTV. In the first instance, advice should be sought from the jurisdiction transport security regulatory authority. Professional legal advice may also be sought.

Breaches of the law, for example in respect of privacy, can result in substantial penalties. Agencies and owner/operators are strongly advised to inform themselves.

Appendix D Recommended Security Functions, Operational Objectives and Transport Security Priorities

Table D.1 summarises the relationships between the various security functions that can be performed by CCTV systems and the four operational objectives (*Monitor*, *Detect*, *Recognise* and *Identify*).

Tables D.2, D.3 and D.4 recommend operational objectives for typical areas within transport modes for each transport security priority. Supplementary capability may include portable CCTV when circumstances require increased intensity of coverage, or to meet police operational objectives.

Table D.1 Relationship of Security Functions to Operational Objectives

Security function	Description: Operational Objectives
Deter	Providing a visible *deterrent* to potential offenders by the presence of a monitored CCTV system with appropriate signage and advertising
Detect	*Detecting* suspicious activity through live monitoring of a CCTV system by: • conducting an 'electronic security patrol', discreetly *monitoring* many locations in a short time • verifying that an incident is occurring, after a report or alarm

Respond	Through live monitoring of the system, aiding the response to an incident by:
	• *monitoring* the incident from a safe location (e.g. a secure monitoring centre) and providing information about the incident, including:
	  • the location, nature and extent of the incident
	  • the immediate response required (fire, police, ambulance)
	  • safe entrance locations
	  • safe evacuation paths
	• *recognising* a suspect moving in or through an area and tracking their movement
	• operating cameras to *identify* a suspect (e.g. in a hostage incident) as is 'known' or 'not known' Responding authorities with direct access to live CCTV will manage the response to the incident. This may include *monitoring* the incident/response, *recognising* and *identifying* people present, and helping to manage the incident.

Investigate	Investigators reviewing recorded CCTV product after an incident to find out what happened and who was involved. This will include: • views before, during and after the incident with enough detail to *recognise* those present, and what happened, to a required evidentiary standard • images to *identify* all people present (e.g. victims, witnesses and suspects)
Reassure community	Providing reassurance to the members of the community who will recognise that CCTV is a valuable security risk treatment

Table D.2 Operational Objectives for Buses, Ferries, Interchanges and Terminals

Location	Area	Operational Objectives		
		Priority 1 transport security priority areas	**Priority 2 transport security priority areas**	**Priority 3 transport security priority areas**
Interchanges and terminals				
Public access areas	• Public entry/exit at strategic choke points	Identify	Recognise	Monitor
	• Passenger waiting areas	Detect	Detect	Not defined
	• Platforms, wharves	Recognise	Monitor	Not defined
	• Public access areas (general)	Monitor	Monitor	Not defined
	• Baggage handling areas	Monitor	Monitor	Not defined
Car parks	• Entry/exit points (vehicles)	Identify	Recognise	Not defined
	• Open-air car parks	Detect	Monitor	Not defined
	• Enclosed car parks (vehicles)	Recognise	Monitor	Not defined
Non-public access areas	• Entry/exit to critical areas (restricted access/security areas)	Identify	Recognise	Monitor
	• Entry/exit to non-critical areas (restricted access/security areas)	Recognise	Monitor	Not defined
	• Baggage handling areas	Monitor	Monitor	Not defined
Stabling yards Depots Maintenance areas Maintenance dockyards	• Major plant rooms, fuel storage, power facilities	Detect	Monitor	Not defined
	• Entry/exit points to site	Recognise	Monitor	Not defined
	• Location of rolling stock/fleet	Detect	Monitor	Not defined
On-board (mobile) CCTV—buses/ ferries				
Mass transit buses/ferries	• Passenger areas	Recognise	Detect	Not defined
	• Entry/exit points	Identify	Recognise	Not defined
Other buses/ferries		Not defined	Not defined	Not defined

Table D.3 Operational Objectives for Trains, Trams, Stations, Stops, Interchanges and Terminals

Location[a]	Area	Operational Objectives		
		Priority 1 transport security priority areas	**Priority 2 transport security priority areas**	**Priority 3 transport security priority areas**
Areas				
Public access areas	• Public entry/exit at strategic 'choke' points	Identify	Recognise	Monitor
	• Passenger waiting areas	Detect	Detect	Not defined
	• Platforms, lounges	Recognise	Monitor	Monitor
	• Public access areas (general)	Monitor	Monitor	Not defined
Car parks[b]	• Entry/exit points (vehicles)	Identify	Recognise	Not defined
	• Open-air car parks	Detect	Monitor	Not defined
	• Enclosed car parks (vehicles)	Recognise	Monitor	Not defined
	• All adjacent car parks—entry/exit points for vehicles	Identify	Recognise (vehicles)	Not defined
Non-public access areas[b]	• Entry/exit to critical areas—restricted access/security areas	Identify	Recognise	Monitor
	• Entry/exit to non-critical areas —restricted access/security areas	Recognise	Monitor	Not defined
Operational areas[b]	• Traffic/operations control rooms—entry/exit points	Identify	Identify	Recognise
	• Operational area entry/exit points	Identify	Monitor	Not defined
	• Major plant rooms, fuel storage/power facilities	Recognise	Monitor	Not defined
	• Baggage handling areas(4)	Monitor	Monitor	Not defined

continued…

Location[a]	Area	Operational Objectives		
		Priority 1 transport security priority areas	**Priority 2 transport security priority areas**	**Priority 3 transport security priority areas**
Stabling yards Depots Maintenance areas[b]	• Perimeter	Detect	Monitor	Not defined
	• Entry/exit points	Recognise	Monitor	Not defined
	• Location of rolling stock/fleet	Monitor	Monitor	Not defined
On-board (mobile) CCTV—trains				
Mass transit trains	• Passenger areas	Recognise	Detect	Not defined
	• Entry/exit points	Recognise	Detect	Not defined
Other trains[b]		Not defined	Not defined	Not defined
On-board (mobile) CCTV—trams				
Mass transit trams[b]	• Passenger areas	Detect	Monitor	Not defined
	• Entry/exit points	Monitor	Not defined	Not defined
Other trams[b]		Not defined	Not defined	Not defined

a Security regulated areas, such as airports or ports, aircraft or vessels, may have different requirements set by the relevant security regulator (for example the Commonwealth Department of Transport and Regional Services).

b Subject to the specific needs identified in the risk assessment.

Table D.4 Operational Objectives for Aviation Areas, Airports and Aircraft

Location	Area	Operational Objectives		
		Priority 1 transport security priority areas	**Priority 2 transport security priority areas**	**Priority 3 transport security priority areas**
Areas, airports and terminals				
Car parks (public and staff)	• Entry/exit points (vehicles)	Identify	Identify	Not defined
	• Open-air car parks (persons)	Detect	Monitor	Not defined
	• Enclosed car parks (pedestrian access/exit points)	Recognise	Monitor	Not defined
Landside (public access areas)	• Public entry/exit (strategic 'choke' points)	Identify	Identify	Identify
	• Passenger check-in counters	Recognise	Detect	Monitor
	• Passenger screening points	Identify	Recognise	Recognise
	• Passenger waiting areas/lounges	Recognise	Detect	Not defined
	• Public access areas (general)	Detect	Monitor	Not defined
	• Departure/arrival gates	Identify	Recognise	Not defined
	• Baggage carousels	Detect	Monitor	Not defined
	• Restricted (non-critical) access areas (entry/exit)	Recognise	Detect	Monitor
Airside (sterile areas)	• Immigration/Customs screening points	Identify	Identify	Identify
	• Passenger waiting areas/lounges	Recognise	Detect	Not defined
	• Public access areas (general)	Detect	Monitor	Not defined
	• Departure/arrival/transit gates	Identify	Identify	Identify
	• Baggage carousels	Detect	Monitor	Not defined
	• Restricted (critical) access areas (entry/exit)	Identify	Identify	Identify
	• Staff/crew entry/exit points	Identify	Identify	Identify

continued…

Location	Area	Operational Objectives		
		Priority 1 transport security priority areas	**Priority 2 transport security priority areas**	**Priority 3 transport security priority areas**
Operational areas	• Vehicle entry/exit points	Identify	Identify	Identify
	• Staff/crew entry/exit points	Identify	Identify	Identify
	• Air traffic control / security control rooms—entry/exits	Identify	Identify	Identify
	• Major plant rooms Power facilities Aircraft catering facilities (entry/exit points)	Recognise	Detect	Not defined
	• Baggage handling areas (airside)	Detect	Monitor	Not defined
	• Cargo handling areas	Detect	Monitor	Not defined
	• Maintenance areas—entry/exit points	Recognise	Detect	Not defined
	• Aircraft—stand-off bays	Detect	Monitor	Not defined
	• Fuel storage facilities	Detect	Monitor	Not defined
On-board (mobile) aircraft				
Passenger jets (international and domestic)[a]	***Not defined by this Code.*** *Refer to the Department of Transport and Regional Services for advice.*			
Light passenger aircraft		Not defined	Not defined	Not defined

a Security regulated areas, such as airports or ports, aircraft or vessels, may have different requirements set by the relevant security regulator (for example, the Commonwealth Department of Transport and Regional Services).

Appendix E Recommended CCTV Performance and Storage Criteria

As indicated at Section 4.1, the definitions detailed in this Appendix are informed by the UK Home Office document *CCTV Operational Requirements Manual* and by the relevant Australian Standard, *AS 4806.2—2006: Closed-Circuit Television (CCTV)—Part 2: Application Guidelines*. Of specific relevance to this Appendix are Section 3.1 (Figure 4) of the UK manual and Figure 5 of the Australian Standard.

Table E.1 Performance Criteria for each Operational Objective

Operational Objective	CCTV Performance Criteria
	Monitoring viewed image resolution[a] (lines)
Monitor	20
Detect	40
Recognise	200
Identify	400

[a] As video images can now be presented in a number of display formats with resolutions varying from less, to far greater than a standard PAL monitor, the "% of screen height" has been replaced with the equivalent "lines of resolution". In order to achieve the required Operational Objective, this number of lines must be able to be resolved 'end-to-end' by the CCTV system, e.g. with a scaled test chart that emulates the target size and distance from the camera, as viewed in replay on the intended display device in the required display format (i.e. split screen/full screen).

Table E.2 Resolution Criteria

	ViDi Labs Test Chart (Figure E.4)		NIFS Test Chart (DRAFT) (Figure E.5)[c]	
Operational Objective	**Field-of-view width at test chart plane**	**Resolution requirement[a]**	**Test chart location**	**Resolution requirement**
Monitor	Chart at full width on the display device	Distinguish "Level 3" (Red text) Vertical Bars	-	-
Detect	Chart at full width on the display device	Distinguish "Level 2" (Green text) Vertical Bars	-	-
Recognise	Chart at half width on the display device	Distinguish 'C' or higher level Tilted Bars	Actual distance to target face	Distinguish vertical lines at 8 mm marker
Identify (Face)	Chart at full width on the display device[b]	Capture facial detail sufficient to identify an individual	Actual distance to target face/number plate	Distinguish vertical lines at 4 mm marker
(Number plate)		Read 5% size number plate		Distinguish vertical lines at 2.94 mm marker

a Use chart indicator details relevant to image type and format (SD/720HD/1080HD).

b Representing person occupying 100% of the picture height with face at 15%.

c Converging lines chart superimposed on a full-size face (15% of 1.6 m = 240 mm).

Table E.3 Live Viewing and Recording Criteria

Transport Security Priority Rating	Functionality	Live Viewing Requirement[a]	Recording Requirement[b]
Priority 1 locations	Live viewing	Routine live monitoring of selected cameras	Recording of all cameras. Capability to review recordings in response to a report of an incident or an alarm event
Priority 2 locations	Verify—incident or alarm	Live viewing in response to a report of an incident or an alarm event—other live viewing optional at operator discretion	Recording of all cameras where practicable. Capability to review recordings in response to a report of an incident or an alarm event
Priority 3 locations	Record only	Live viewing optional at operator discretion	Recording of all cameras where practicable. Capability to review recordings in response to a report of an incident or an alarm event

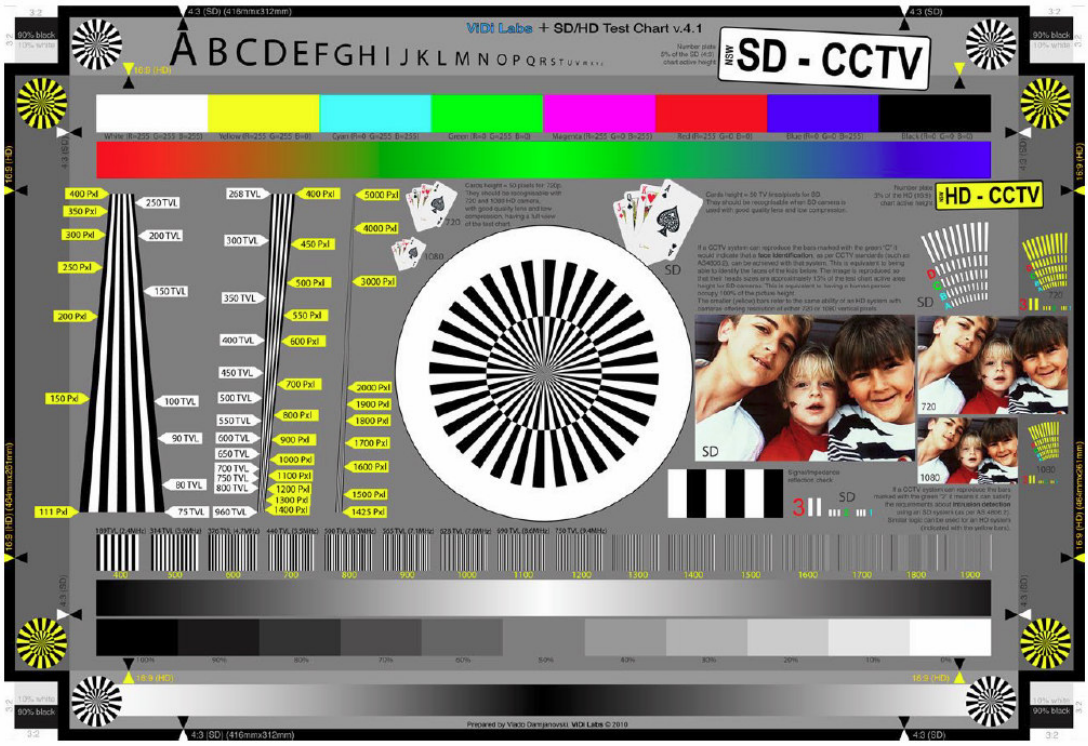
a Live viewing: live observation by operators in (near) real time of CCTV monitors showing selected camera views.

b Recording includes either continuous recording, activity detection or event triggered recording, on any form of storage device that can later be replayed as video imagery.

Recording time requirement of 24 hours × seven days/week—includes either continuous recording, or recording activated in response to an alarm device or imagery processing to ensure a record of any relevant activity within the camera field-of-view.

Recording time requirement for on-vehicle CCTV (train/tram/bus/ferry)—recording while operational.

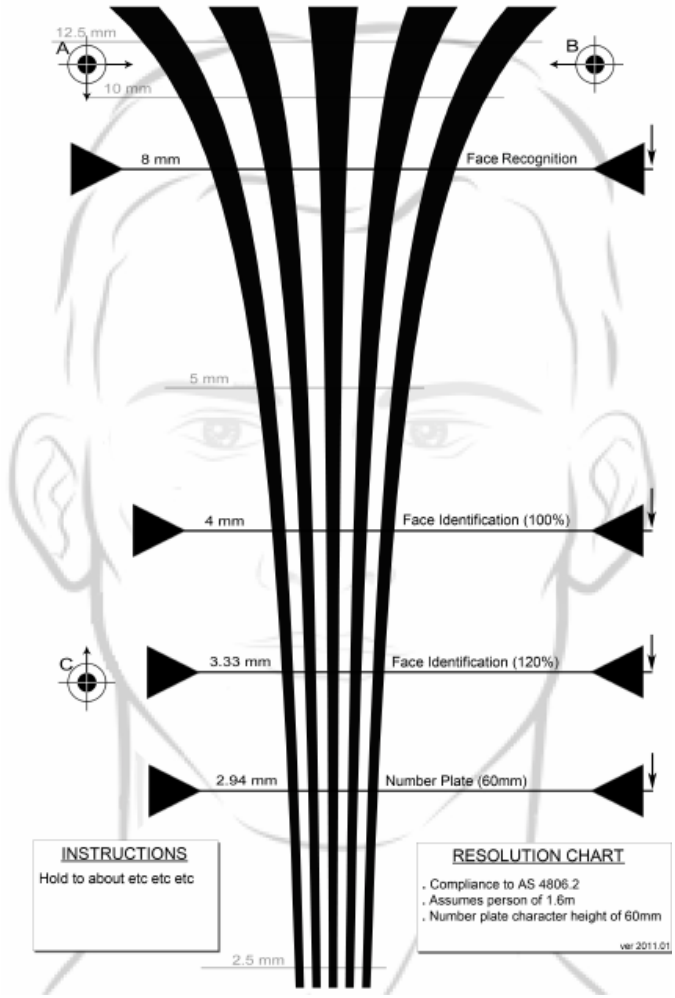
Figure E.4 Example of CCTV Test Chart



Prepared by V. Damjanovski © 2010 (www.vidilabs.com)

The CCTV test chart is produced in an A3 format, and comes on a hard foam board. It is printed on a special proof paper with minimum light reflection and high colour stability. The same chart comes in the book, *CCTV Test Chart*, in a smaller (A4) format.

Figure E.5 CCTV Test Chart (DRAFT)



Prepared by National Institute of Forensic Science, Electronic Evidence Specialist Advisory Group, 2011.

Appendix F Code Background, Objectives, Development and Application

Background

The Special Council of Australian Governments (COAG) meeting on Counter-Terrorism in September 2005 advised in its *communiqué* that:

> *COAG discussed the significant role that closed-circuit television (CCTV) played in the identification of the perpetrators of the July 2005 terrorist attacks in London and its potential to assist police counter-terrorism investigations. COAG noted that jurisdictions already have extensive CCTV networks across transport, public spaces and major facilities. COAG agreed that each jurisdiction would undertake and share across governments a review of the functionality, location, coverage and operability of mass passenger transport sector CCTV systems. This will be a first step towards a broader consideration of the use of CCTV in support of counter-terrorism arrangements.*
>
> *COAG also agreed to a national risk-based approach to enhancing the use of CCTV for counter-terrorism purposes, including the development of a National Code of Practice for CCTV systems for the mass passenger transport sector.*
>
> *The Code will set a policy framework, objectives, protocols and minimum requirements for the use of CCTV systems to enhance counter-terrorism arrangements so that future investment is based on appropriate risk analysis. It will also contain agreed requirements for fixed and mobile CCTV systems, and national guidelines for the collection, storage, access, use, privacy, disclosure, protection and retention of CCTV information.*
>
> *The Code will allow each jurisdiction to determine its own CCTV requirements having regard to the use of CCTV for local counter-terrorism purposes.*
>
> *COAG further agreed that a COAG Working Group, to be chaired by Victoria, would be established to develop the Code that will involve consultation with private industry. The Working Group will make an initial report to COAG in February 2006 with the draft Code.*
>
> *COAG agreed to identify necessary legislative measures to ensure consistent implementation of the Code, to encourage business and industry to comply with the Code, and to work cooperatively in research, development, trial and evaluation of new CCTV technologies.*

The COAG CCTV Working Group also facilitated arrangements for parallel and interrelated work on these matters, which are managed separately, through coordination by the National Counter-Terrorism Committee (NCTC).

Closed-Circuit Television in the Mass Transport Sector

CCTV has established uses in industry and in the community for a range of purposes, such as public safety, crime prevention or investigation, industry operational functions, and improving productivity.

All levels of government have some involvement in aspects of CCTV that affect transport:

- States and Territories have extensive CCTV systems in place for the operational management of transport infrastructure. In some cities, local governments, shopping centres and sports centres manage street and public space CCTV systems as a deterrent to criminal behaviour.

- Most jurisdictions have legislation regulating some aspects of CCTV usage for privacy reasons. Some have regulations for the use of CCTV in certain types of premises, such as casinos, or for liquor licensing.

- The Commonwealth regulates the security of airports and maritime industry participants (that fall within the Commonwealth's jurisdiction) consistent with international standards. The Commonwealth also manages CCTV systems for customs and other purposes.

Objectives

National Policy and Security: the Value of Being Prepared

In December 2005, the National Counter-Terrorism Committee noted that the national counter-terrorism alert level remained at 'Medium', which means that a terrorist attack could occur in Australia. Reasonable measures to prevent, mitigate and manage such a risk are essential. Mass passenger systems generally, and mass transit systems in particular, are highly vulnerable to terrorist attack. The only way to guarantee their complete security would be to stop and close them, but a careful risk-management approach can substantially reduce the potential for, or the impact of, terrorist acts, and put in place effective means to respond to any acts that do occur.

While preventive measures are important, the possibility of successful terrorist attacks must be considered. As shown overseas, successful attacks can result in a high casualty rate, significant short-term disruption and high-profile international media coverage. There is no data with which to define a statistically credible or predictable range of probability or impact. However, probability and impact can be described by reference to actual terrorist incidents, or changes in the assessed risk, in other western societies.

It has been observed that:

- Terrorist incidents generate substantial additional costs to a community, in both the public and private sectors.
- The short and long-term burdens on health systems created by terrorist incidents are substantial because of the characteristically severe injuries (extensive burns, eye damage, loss of limbs), physical and emotional trauma, and likely high mortality rates among the initial survivors. Other people affected by the consequences of terrorist acts, including through significant relationships, can also show high levels of emotional stress or psychological impact, and may need professional assistance for several years.
- Sustained reduction in total inbound travel has been estimated for New York after the September 2001 attacks, representing a substantial direct and indirect economic impact.

Conversely, improved counter-terrorism arrangements generate benefits to the community. These are unable to be easily quantified or monetised, but are nevertheless real and important.

Because of the difficulty in meaningfully and reliably quantifying the risk or the impact of a future terrorist attack, or the non-monetary benefits of CCTV, it would be inappropriate to use a cost–benefit analysis as the primary evaluation tool for investment decisions about CCTV systems for counter-terrorism arrangements.

Similarly, a cost–benefit analysis is unable to quantify community members' expectations for their protection from terrorist attacks as they go about their business.

Development

Principles for Formulation

Some principles that were adopted in the formulation of the Code were the need to:

- define the Code in ways that, over time, are technology neutral and functionally relevant and that specify practical outcomes
- ensure that law enforcement, national security and other relevant agencies have timely access to evidentiary-standard material, enabling an effective operational response consistent with national expectations
- adopt and implement protocols and minimum requirements for the collection, storage, access, use, disclosure, protection and retention of information across governments and industry, while ensuring that the privacy of personal information is appropriately protected
- develop a nationally-consistent approach to CCTV systems, which can be updated to accommodate new requirements and developing technologies
- efficiently and economically adopt and maximise the security benefits of emerging CCTV technologies, such as facial, behavioural and automatic number plate recognition
- utilise available technological solutions (such as planning tools for the placement of cameras) to ensure effective and efficient CCTV systems for counter-terrorism purposes
- ensure that future investment is based on appropriate risk analysis and prioritisation
- ensure that an appropriate risk-based balance is struck between the utility of CCTV as a counter-terrorism tool and the significant privacy and civil liberties issues entailed in its use.

Application

A Risk-based Approach

Resource commitments for CCTV initiatives by governments and transport operators are subject to determination and prioritisation along with broader requirements for counter-terrorism. A risk-based approach should be taken in the application of the Code.

Expected Benefits

Application of the Code will enhance the potential of CCTV systems in the mass passenger transport sector to:

- Assist in the response to a terrorist attack to:
  - improve the situational awareness of transport operators, police and emergency services to enable more rapid and effective response
  - improve the timely capacity to investigate criminal acts to enable prompt apprehension of the offenders and their associates and to prevent further acts by any of them
  - improve the availability and forensic value of CCTV imagery for investigations and in court proceedings.
- Contribute indirectly to counter-terrorism arrangements in order to:
  - reduce the likelihood of a terrorist attack on mass passenger transport systems
  - improve the detection of suspicious incidents to enable more rapid and effective response to such incidents
  - increase and retain public and staff confidence in surface transport security and safety, and so promote use of public transport, both before and after any incident or media speculation.

The potential benefits of adopting a nationally-consistent approach to CCTV systems also include:

- consistency of data quality, ensuring evidentiary-standard product
- consistency of operating standards and protocols
- capacity for upgrades as new technology becomes available
- consistency and compatibility of data formats, facilitating exchange between jurisdictions
- capacity to develop and maintain a national pool of technical expertise for interpretation and analysis, especially for major incidents requiring a national response.