

Review of Victoria Police Major Project Development MOUs

Review of Victoria Police Major Project Development MOUs

under s11(1)(e) of the Commissioner for Law Enforcement Data Security Act 2005

Commissioner for
Law Enforcement Data Security

24 August 2010

Commissioner for Law Enforcement Data Security



24 August 2010

Level 9 Yarra Tower
PO Box 281
World Trade Centre
Melbourne
Victoria 8005
Australia
DX 210096
www.cleds.vic.gov.au
Telephone: 61-3-9247 3857
Facsimile: 61-3-9247 6394

Our Ref: CLEDS/06/0153

The Hon. Bob Cameron MP
Minister for Police & Emergency Services
Parliament House
Spring Street
Melbourne VIC 3000

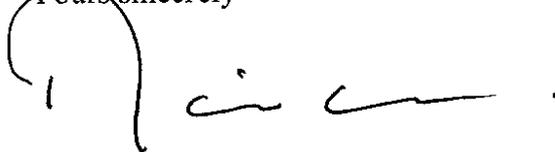
Dear Minister,

Review of Major Project MOUs

I refer to your request, dated 8 December 2009, pursuant to s11(1)(e) of the Commissioner for Law Enforcement Data Security Act 2005 that I undertake a review of Victoria Police Major Project MOUs.

The review you requested has been completed and is enclosed.

Yours sincerely



David Watts
**Commissioner for
Law Enforcement Data Security**

Review of Victoria Police Major Project Development MOUs

under s11(1)(e) of the Commissioner for Law Enforcement
Data Security Act 2005

Commissioner for
Law Enforcement Data Security

24 August 2010

Published by:

The Commissioner for Law Enforcement Data Security
PO Box 281
World Trade Centre
Melbourne Victoria 8005

August 2010

© Copyright State of Victoria, 2009

Contents

1	Executive Summary	5
1.1	Summary of key findings	6
1.2	Summary of key recommendations	7
1.3	Disclosure to Victorian Privacy Commissioner under s13 CLEDS Act	10
1.4	Glossary	10
2	Introduction	12
2.1	Ministerial Request for Review	12
2.2	The Factual Background	12
2.3	Review Process	13
2.4	Defining ‘Major Project Development MOUs’	13
2.5	Victorian Government Water Policy	14
3	What is an MOU?	16
3.1	Defining an MOU	16
3.2	Victoria Police MOUs	17
4	Information Sharing – The Legal and Regulatory Framework	21
4.1	Overview	21
4.2	Information Privacy	21
4.3	Information Security	21
4.4	Charter of Human Rights and Responsibilities	22
4.5	Victoria Police information release policy	22
4.6	Other legislation	23
5	Major Project Development MOUs – Desalination and Mt Sugarloaf	24
5.1	Introduction	24
5.2	The Desalination MOU	24
5.3	Desalination MOU Documents	24
5.4	Purpose	25
5.5	Enforceability	26
5.6	Structure	26
5.6.1	Roles, responsibilities and mutual assistance	26
5.6.2	General arrangements	26
5.6.3	Special arrangements	27
5.6.4	Information Sharing under the Desalination MOU	28
5.6.4.1	Clauses 5(k), (l), 8 and 9	28

5.6.4.2	Clause 9	31
5.7	The subordinate documents	31
5.8	Analysis and Comments on the MOUs	33
5.9	The Sugarloaf MOU	35
5.10	What information was shared?	36
5.11	The 10 March 2009 email – Victoria Police disclosure of persons charged	36
5.12	Other information release	37
5.13	DSE	37
5.14	Information provided by AquaSure	38
5.15	The consequences of recommending change	39
5.16	Whole of Government issues	40
6	Law Enforcement Data Sharing: The Way Forward	43
6.1	Developments in information sharing	43
6.2	Responsible information sharing for law enforcement – appropriate checks and balances	44
6.3	Information Sharing Risk Assessment	44
6.3.1	Proportionality Assessment	45
6.3.2	Privacy Impact Assessment	46
6.3.3	Threat and Risk Assessment	46
6.3.4	Human Rights Impact Assessment	46
6.3.5	When is an ISRA required?	47
6.3.6	External scrutiny of law enforcement data release arrangements	48
6.4	An overarching information policy and management framework	48
	APPENDIX 1 – The Regulatory Regime in Detail	50
	Attachment 1 – Reference from Minister for Police and Emergency Services	61

1 Executive Summary

This review has uncovered no evidence that Victoria Police has released sensitive personal information to AquaSure under the Desalination MOU. Victoria Police has, however, provided AquaSure with a limited amount of non-sensitive, non-personal law enforcement data under the MOU. It also released some sensitive information about offences committed by certain individuals to DSE before the execution of the Desalination MOU.

The Desalination MOU is a risk management tool. It was developed to manage the risk that protest action might unacceptably delay the construction of the Victorian desalination plant at Wonthaggi. The risk management approach that was taken involved the parties defining and documenting their mutual roles and responsibilities in responding to protest action, to describe how they would assist and cooperate with each other and to establish arrangements for sharing information.

There is nothing inappropriate about documenting arrangements that define roles, responsibilities and mutual assistance. Nor is it inappropriate for Victoria Police and those who have agreed to assist it to agree to share information provided the sharing arrangements are consistent with, and accurately apply, the relevant legal framework and establish mechanisms designed to support compliance with it. Victoria Police's ability to share information is limited by a number of laws, primarily Victorian human rights, information privacy and law enforcement data security laws, as well as its own documented policies and procedures.

This review finds that the Desalination MOU does not succeed in identifying and applying the correct legal framework for information sharing because of:

- inadequate and confusing Victoria Police policies and procedures relating to the development, oversight and implementation of MOUs
- drafting errors in the Desalination MOU, and
- failures to adequately cover the key regulatory requirements, i.e., human rights, information privacy and information security.

There is no evidence that Victoria Police shared, or intended to share, law enforcement data in breach of its legal obligations. That said, it entered into an MOU that purported to impose information sharing obligations that extended beyond the legal requirements.

At the core of the issues that have formed the backdrop to this review are important questions about how Victoria Police should share information. There is an increasing emphasis on the need for cooperation and information sharing between Victoria Police and other public sector organisations that have law enforcement responsibilities. In parallel, new policing practices and techniques emphasise the need for police to work in partnership with the community and to develop networks to fight crime. Central to the success of these initiatives is the need to appropriately share information. Sometimes this means that Victoria Police may need to share law enforcement data with individuals and organisations who are not part of the public sector. For example, Victoria Police routinely shares limited amounts of law enforcement data with local Neighbourhood Watch groups.

In the light of these developments and the imperfect approach that was adopted in the Desalination MOU, a significant focus for this review has been on describing an appropriate framework for information sharing for law enforcement purposes. The suggested framework involves adopting a broad risk management approach founded on a proportionality test to balance the need for the free flow of law enforcement data with community expectations that

sensitive personal information is not shared inappropriately. The review emphasises the need for an information sharing culture of compliance within Victoria Police where responsibilities and accountabilities are clear and the arrangements are subject to independent, external scrutiny.

More generally, the issues raised in this review highlight the need for Victoria Police to consider developing, as has been done in the UK, a holistic information policy and management framework that governs the entire lifecycle of its law enforcement data holdings and that comprehensively covers issues such as collecting, recording, evaluating, sharing and disposing of law enforcement data.

1.1 Summary of key findings

Chapter 3

Victoria Police law enforcement data release policies, procedures and training are inadequate and confusing. They fail to:

- adequately describe and support the relevant regulatory framework
- describe when an MOU or a less formal written arrangement is needed
- delineate between the circumstances where more complex and less complex information release arrangements are required
- describe the authorisation process for law enforcement data release
- establish minimum terms and conditions for MOUs or other arrangements for the release of law enforcement data
- provide precedents, templates and checklists to assist those who develop information release arrangements
- establish a central register of MOUs
- establish proper oversight mechanisms for MOUs
- establish sufficient guidance about the regulatory requirements, in particular, the CLEDS Standards and the Charter
- provide adequate education and training about information release requirements.

Chapter 5

The Desalination MOU is problematic because:

- it contains the drafting errors and oversights outlined in chapter 5
- as a consequence, it imposes obligations on Victoria Police that are inconsistent with legal and regulatory requirements
- it is legally unenforceable as against AquaSure, the consequence being that confidentiality and privacy obligations that should have been enforceable are not. This also means that information security obligations consistent with and supportive of the CLEDS Standards are not enforceable
- key regulatory obligations, in particular Charter obligations, are not mentioned
- governance and oversight mechanisms are inadequate

- the information sharing framework is not supported by corresponding compliance safeguards such as a privacy impact assessment, an information security threat and risk assessment and a human rights impact assessment
- when read in conjunction with the broader Desalination project documentation, the Desalination MOU may give rise to unintended consequences under the broader Desalination project documentation.

Chapter 6

The development of the Major Project Development MOUs was not informed by the use of appropriate compliance tools and mechanisms. No Privacy Impact Assessment, Information Security Threat and Risk Assessment or Human Rights Impact Assessment was undertaken.

1.2 Summary of key recommendations

Chapter 3

One of the themes of CLEDS' reviews of Victoria Police's law enforcement data security practices over the last few years has been the inadequacies of its security arrangements for data release and access for third parties. The findings in this chapter are consistent with the fact that CLEDS recommendations dating back to 2008 about these matters have not been fully implemented.

Any further delay in addressing these issues is unacceptable. Accordingly the recommendations that follow are designed to establish a reform process that will be subject to intensive supervision by my office.

Victoria Police must:

- finalise a central register of law enforcement data release MOUs as a matter of urgency
- urgently review those parts of the Victoria Police Manual and associated or related documents concerning law enforcement data release in a manner consistent with this review's findings and submit these to CLEDS for analysis and comment
- develop appropriate precedents, templates and checklists to assist Victoria Police members to develop law enforcement data release arrangements and submit these to CLEDS
- develop appropriate training and educational materials to assist and inform Victoria Police members to develop, implement and monitor law enforcement data release arrangements and submit these to CLEDS
- by no later than 14 days after the publication of this review, nominate a person and Division of Victoria Police responsible for implementing these recommendations
- by no later than 28 days after the publication of this review, provide CLEDS with a proposal and associated timelines for implementing the recommendations set out in this chapter and to report on implementation progress on a monthly basis until the recommendations are fully implemented.

Chapter 5

Although there are many problems with the Major Project Development MOUs, Victoria Police cannot unilaterally amend them. Any changes require the consent of the other parties and, on the basis of DSE's submission, perhaps the consent of a variety of financial institutions.

As the Desalination MOU does not compel Victoria Police to share any particular piece of information and the fact that Victoria Police is bound by the law not to share its law enforcement data in breach of those laws, no party to the MOU or any other relevant stakeholder could possibly assert that Victoria Police would breach any MOU obligation by strictly adhering to its information sharing legal obligations and by requiring the same of the other MOU parties.

In these circumstances it is appropriate that I make both general recommendations and more limited recommendations that apply only to the Desalination MOU and to the Mt Sugarloaf MOU to the extent that it continues to operate. In chapter 6, I have set out a recommended framework that Victoria Police should adopt whenever it contemplates sensitive information sharing arrangements. In my view, that framework should be applied to the Desalination MOU as soon as possible.

Recommendations about the Desalination MOU

Victoria Police should:

- Notify each of the parties to the MOU that:
 - despite the express words used in clauses 5(k) and 8 of the MOU, any sharing by Victoria Police of its law enforcement data will be strictly in accordance with its legal obligations
 - it proposes to forthwith undertake an Information Sharing Risk Assessment on all law enforcement data flows likely to fall within the scope of the Desalination MOU, and
- invite each of the parties to the MOU to cooperate and assist in the ISRA process
- provide my office with the finalised ISRA
- promptly implement the ISRA recommendations when made
- report to CLEDS on progress by no later than 6 weeks after the publication of this review.

General MOU Recommendations

Victoria Police should for any future Major Project MOUs:

- ensure that they do not embody the drafting errors identified in chapter 5
- restructure the MOU so that all of the provisions relating to governance and roles and responsibilities on the one hand and information sharing on the other are dealt with separately and in a consolidated form
- ensure that they properly reflect all relevant regulatory obligations
- excise the matters covered by clause 9 of the Desalination MOU and incorporate them in a separate, legally enforceable deed or agreement
- review all law enforcement data security provisions to ensure that they comply with the CLEDS Standards. In so far as these obligations should be passed on, incorporate these into a legally enforceable deed or agreement where that other party does not represent the Crown
- undertake the compliance and safeguard measures identified in chapter 6 before the MOU becomes operational

- review governance arrangements with a view to establishing mechanisms for oversight and dispute resolution and clear lines of accountability and authority for the release of law enforcement data.

The Department of Treasury and Finance should:

- review the linkages between Victorian Major Project documentation and other, cognate agreements or arrangements, whether legally enforceable in their own right or not, that might give rise to liabilities or other consequences under Major Project documentation, with a view to developing appropriate guidance and controls to manage those consequences.

Chapter 6

To ensure that Victoria Police information sharing arrangements are underpinned by appropriate compliance mechanisms, before any such arrangements are developed an Information Sharing Risk Assessment must be undertaken.

An ISRA consists of:

- a Proportionality test
- a Privacy Impact Assessment
- an Information Security Threat and Risk Assessment
- a Human Rights Impact Assessment.

The degree of detail of the ISRA process will depend on the risks involved. At a minimum, a formal, comprehensive process is necessary for information sharing in relation to:

- any Victorian major project development,
- any Victorian major event,
- any information sharing arrangement in relation to which law enforcement data may be released to a commercial (i.e., for-profit) organisation, whether the release is made directly by Victoria Police or through an intermediary, and
- any other information sharing arrangement that constitutes a significant risk to Victoria Police.

Authority to execute such an arrangement should be restricted to the Chief Commissioner or a Deputy Commissioner after the arrangement is certified as being suitable by the Director of IMSSD.

All other arrangements should be informed by templates, checklists, precedent documents and education and training developed for the purpose by Victoria Police. Authority to execute the arrangement should be confined to the relevant Assistant Commissioner subject to her or him being satisfied that the checklist and documentary requirements are certified in writing as having been undertaken, such certification to be provided by an appropriate officer.

Oversight of the implementation of the recommendations set out in this review should be undertaken by CLEDS who will report to the Minister on progress on quarterly basis.

More broadly, Victoria Police senior management should give urgent consideration to the development of an overarching information policy and management framework to govern its information handling practices across the complete lifecycle of its information holdings. Such a framework would incorporate the processes and compliance tools recommended in this chapter but would extend to cover a range of other whole of lifecycle information issues.

1.3 Disclosure to Victorian Privacy Commissioner under s13 CLEDS Act

Under s13 of the CLEDS Act, I intend to disclose the matters relating to an email dated 10 March 2009 provided by Victoria Police to DSE to the Victorian Privacy Commissioner for her to consider whether those matters warrant further investigation.

1.4 Glossary

The following abbreviations and expressions are used in this review:

AquaSure	Aquasure Pty Limited A.C.N. 135 956 393
Authorised Release	Release that is permitted by law and Victoria Police policy (see CLEDS Standard 11)
ATP	An Approved Third Party, being an organisation or individual external to Victoria Police that has been granted direct access to Victoria Police law enforcement data repositories
Charter	The Victorian Charter of Human Rights and Responsibilities
CLEDS Act	The Commissioner for Law Enforcement Data Security Act 2005
CLEDS Standards	Standards for Victoria Police law enforcement data security, July 2007
Data Sharing Review	The Data Sharing Review Report undertaken for the UK Government by Richard Thomas and Mark Walpole, dated 11 July 2008
Desalination MOU	The MOU between Victoria Police, The Secretary and AquaSure executed on 28 August 2009
DSE	The Department of Sustainability and Environment
HRIA	Human Rights Impact Assessment
IMSSD	Information Management, Standards and Security Division of Victoria Police
IPA	Information Privacy Act 2000 (Vic)
IPP	Information Privacy Principle asset out in Schedule 1 to the IPA
ISRA	Information Sharing Risk Assessment
ISTRA	Information Security Threat and Risk Assessment
Law enforcement data	has the same meaning as in s3 CLEDS Act
MOU	Memorandum of Understanding
Mt Sugarloaf MOU	The MOU between Victoria Police and Melbourne Water executed on 1 July 2008
Personal information	has the same meaning as in s3 of the IPA
PIA	Privacy Impact Assessment

Release	Any disclosure of law enforcement data by Victoria Police (see CLEDS Standard 11)
Secretary	The Secretary, Department of Sustainability and Environment
Sensitive information	has the same meaning as in the IPPs
TRA	Threat and Risk Assessment
VICPOL	Victoria Police

2 Introduction

2.1 Ministerial Request for Review

This review was initiated by the Minister for Police and Emergency Services who, on 8 December 2009, wrote to me to request that I undertake a review of Victoria Police Major Project MOUs pursuant to s11(1)(e) of the CLEDS Act.

'As part of this review, I would ask that you examine such MOUs to ensure that these documents:

- a. appropriately reflect your standards for law enforcement data security and integrity; and
- b. assure appropriate compliance, controls and arrangements are in place.' A copy of the Minister's s11(1)(e) request is Attachment 1.

The main purpose of the Commissioner for Law Enforcement Data Security Act 2005 (CLEDS Act), is 'to promote the use by the police force of Victoria of appropriate and secure management practices for law enforcement data' through, amongst other things, the development of a regime for the monitoring of law enforcement data security management practices.¹

The Commissioner's functions are set out in s11 of the CLEDS Act. They include:

- To establish appropriate standards for the security and integrity of law enforcement data systems
- To establish appropriate standards and protocols for access to, and the release of, law enforcement data, including, but not limited to, the release of law enforcement data to members of the public
- To conduct monitoring activities, including audits, to monitor compliance with the standards and protocols

Under s 11(1)(e) of the CLEDS Act a further function of the Commissioner is to 'undertake reviews of any matters relating to law enforcement data security requested by the Minister...' This review has been undertaken under that provision.

2.2 The Factual Background

During December 2009 the Age newspaper published a number of articles suggesting that Victoria Police had shared its law enforcement data with AquaSure, the corporation responsible for the development of Victoria's desalination plant. Central to the Age articles was a Memorandum of Understanding (MOU) between Victoria Police, the State of Victoria and AquaSure dated 28 August 2009 under which Victoria Police agreed that it 'will release law enforcement data to AquaSure.' It was reported that similar arrangements had been negotiated in respect of other '(g)overnment-backed projects such as the Grand Prix at Albert Park and the pipeline to bring water from northern Victoria to Melbourne.'

Since then, a number of additional articles have been published that canvass concerns about whether information has been shared and, if so, the extent of the sharing.

¹ See s1 CLEDS Act

2.3 Review Process

Implicit in the Minister's reference is whether the Major Project Development MOUs are fit for purpose. To answer that question it is necessary to understand their purpose and to assess whether they succeed, having regard to the regulatory framework. The key components of the regulatory framework are Victoria's laws relating to human rights, information privacy and information security together, in Victoria Police's case, with its policies and instructions. This review has involved assessing whether the MOUs are consistent with, and satisfactorily implement, those regulatory requirements. The outcomes of this analysis are central to the review findings and recommendations.

The focus of the review, therefore, is not on whether any individual's information privacy or human rights have been breached. These issues are matters for the Victorian Privacy Commissioner and the Victorian Equal Opportunity and Human Rights Commissioner respectively. That said, where I consider that an issue warrants further investigation by a regulatory or oversight body, I have recommended that the matter be referred accordingly.

The review has followed the usual form of a CLEDS review. The process is an informal one whereby information is sought, documents are requested and analysed and relevant persons are interviewed. Our experience is that this approach is best suited to isolating and understanding the key issues quickly and to producing practical recommendations for reform in a timely manner, particularly where the review focus is on the suitability or otherwise of documents.

At our request both Victoria Police and the Department of Sustainability and Environment (DSE) provided written information to the review. DSE provided a submission dated 23 December 2009 and Victoria Police responded to a request for information by letter dated 12 February 2010 and provided a submission dated 14 July 2010 in response to my request for it to comment on an advanced draft of the review report. These were supplemented by additional clarifying material as well as interviews with relevant staff.

2.4 Defining 'Major Project Development MOUs'

The terms of reference require an examination of Major Project Development MOUs. The definition I have adopted for a 'major project development' is that the term encompasses a Victorian major or critical infrastructure project. This definition has been adopted to distinguish Major Project Development MOUs from other Victoria Police MOUs, of which there are many.

I requested Victoria Police to identify all Major Project Development MOUs. They identified two:

- the MOU for the desalination project dated 28 August 2009 (**the Desalination MOU**), and
- the MOU for the Mt Sugarloaf pipeline construction corridor dated 1 July 2008 (**the Sugarloaf MOU**)

Mindful of media reports that similar arrangements had been entered into for the Australian Grand Prix at Albert Park in Melbourne, I asked Victoria Police to provide me with information about any such arrangements. They provided me with a document entitled 'Critical Incident Response Protocol for the 2009 Formula 1™ Australian Grand Prix' (**Grand Prix protocol**). The parties are the Confederation of Australian Motor Sports (CAMS), the Australian Grand Prix Corporation and Victoria Police.

The Grand Prix protocol describes roles and responsibilities and operational procedures for dealing with a critical incident at the Grand Prix. A 'critical incident' covers incidents as a consequence of the motor racing component of the event that result in serious injury or death. Obviously, the race organisers, police and CAMS need to share information appropriately to respond to and manage life threatening critical incidents. Having examined the Grand Prix protocol, it clearly has nothing to do with managing protest action and does not establish information sharing arrangements about protests. It is not a Major Project Development MOU and therefore, is not analysed in this review.

While this review was nearing its final stages, Victoria Police advised me of a further MOU of which they had become aware. The MOU, dated 29 December 2004, is between Victoria Police and DSE and is designed to establish 'an arrangement for the management of protest events in State forests and the effective detection, identification and prosecution of persons who commit offences...' ² (the **Forest Protests MOU**).

The subject matter of the Forest Protests MOU does not directly relate to Major Project Development and therefore falls outside the scope of this review. That said, it contains some clauses that are so similar to those used in the Desalination and Mt Sugarloaf MOUs that it is reasonable to conclude that they were at least partially derived from the Forest Protests MOU. The Forest Protests MOU is clearly obsolete although, as it has no termination date, it may technically still be in force. If so, because it was developed before the enactment of the CLEDS Act and the Charter and does not comply with either piece of legislation, it should be terminated forthwith.

As is discussed in chapter 3, Victoria Police has, over the years, entered into countless MOUs but there is no central register of them. In the absence of a central register, no one can say with absolute certainty that the Desalination and Mt Sugarloaf MOUs are the only Victoria Police Major Project MOUs. Work is currently being undertaken to establish a central register. Once complete, I propose to assess the MOUs on the register in the light of this review's recommendations.

2.5 Victorian Government Water Policy

In June 2007 the Victorian Government released 'Our Water Our Future: the Next Stage of the Government's Water Plan'. The Plan documented the government's intention for Victoria to construct a major desalination plant to service Melbourne, Geelong and towns in the Westernport and South Gippsland region, to be operational by late 2011. Under the plan, desalinated water is to be transferred via an 85- kilometre pipeline to Melbourne's water supply system near Cardinia Reservoir. In July 2009 the government announced that the AquaSure Consortium had been awarded the contract to construct the desalination plant and associated infrastructure.

The plan also included a north/south pipeline – known as the Sugarloaf interconnector – to link Melbourne to the Goulburn river as part of an initiative to modernise Victoria's food bowl through the development of new water infrastructure. The project piped its first water to Melbourne in February 2010 and was delivered by the Sugarloaf Pipeline Alliance.

Construction of the desalination plant began in September 2009 at a site near Wonthaggi. When fully operational the plant is intended to deliver up to 150 GL annually to Melbourne's water system – around one third of Melbourne's water needs.

2 Recital A, Forest Protest MOU

Both the north/south pipeline and desalination plant projects have been the subject of community concern and protest action. One of the responses to the risk that illegal protest action might delay the projects was for those responsible for delivering the projects and those responsible for enforcing the law to develop arrangements about how to jointly handle protest action. They developed arrangements that sought to define roles and responsibilities, cooperative plans to deal with protest action and to share information as a means of managing risk. The means selected to document these arrangements was a Memorandum of Understanding (MOU).

3 What is an MOU?

3.1 Defining an MOU

An MOU is a flexible instrument that is most often used when two or more parties wish to document mutual arrangements that they intend will not be legally enforceable. 'An MOU is a document that records the common intent of two or more parties where the parties do *not* wish to assume legally binding obligations. An MOU is usually less complex and less detailed than a contract, but provides a framework and set of principles to guide the parties in undertaking a project or working arrangement.'³ An MOU can also provide commercial or administrative certainty or a framework to negotiations and can serve as a basis from which a legally binding agreement is later concluded.

For government departments or other agencies that represent the Crown, the position is different. Where they wish to document their mutual obligations about a joint project or undertaking an MOU or similar document is the only option available. They cannot enter into a legally binding contract with each other because the law considers that they are both the same legal entity – the Crown. The parties to an MOU who represent the Crown treat its terms *as if* they are enforceable.

MOUs often use general language to describe principles that will guide the parties' conduct, such as:

- the roles they will undertake
- how they will perform their roles and coordinate their activities
- how they will allocate responsibilities and
- if information is to be shared, how this will be done.

Where the collaborative or coordinated activities are complex, an MOU will often establish the governance arrangements that will apply, such as a management committee, project committees and other oversight or decision-making bodies and processes. These governance arrangements facilitate coordinated decision-making and an agreed process to resolve disputes. Strong governance arrangements are particularly important to underpin complex information sharing initiatives so that compliance issues can be dealt with in a timely and authoritative manner and lines of accountability for decision-making are clear.

Whether or not an MOU is legally enforceable, it is common practice for the finer details to be dealt with in other, subordinate documents as attachments or schedules. These can come in many forms, including specifications, standard operating procedures, guidelines, protocols, instructions, plans and templates. Typically, these documents cover specialised subject matter that cannot be communicated effectively using the formal legal language used in MOUs or binding agreements. Although it is not a legal requirement, common sense dictates that these issues are covered in documents that are purpose-built.

Given that both the Desalination and Mt Sugarloaf projects were anticipated to give rise to complex and sensitive policing issues, it was entirely appropriate for the parties to each project to document arrangements relevant to community safety. If they had not done so they would

³ Victoria Government Solicitors Office, June 2008 Client newsletter, www.vgso.vic.gov.au/resources/publications/CCL/MemorandaofUnderstanding.aspx, my emphasis

have failed to establish a proper framework that set out their roles and responsibilities. They would have left complex questions about information sharing to verbal understandings that would have been impossible to accurately describe and communicate to those responsible for implementing them. Moreover, in Victoria Police's case, the CLEDS Standards require certain information security issues to be documented.

One of the themes that emerge from this review is that Victoria Police should only share sensitive information if the sharing is supported, amongst other things, by a strong culture of regulatory compliance and accountability. It is difficult to imagine how this could be achieved in the absence of written arrangements. The focus of community concern should not, therefore, be on whether collaborative information sharing arrangements are documented. Best practice requires that they are. The real issue is whether the arrangements are suitable and embody proper compliance safeguards.

3.2 Victoria Police MOUs

Victoria Police, in common with many other police forces and government agencies, regularly uses MOUs to document the 'roles, responsibilities, expectations and arrangements for [parties] co-operating with each other to achieve an appropriate way of achieving common aims.'⁴ They are used to document arrangements with both public and private sector organisations. For example, there is an MOU between Victoria Police and the Commonwealth Department of Defence relating to the use of the HMAS Cerberus rifle range. There is an MOU between Victoria Police and Parks Victoria to promote the safe management of firearms. At one time there was an MOU between Victoria Police and the Australian Football League to establish a cooperative relationship on matters such as match fixing, illegal drug taking, sexual assault and family violence.

Victoria Police has entered into countless MOUs that document the establishment and operation of many different types of cooperative arrangements. Often, but not always, they involve Victoria Police releasing law enforcement data to the other party or parties to the MOU. In many cases the law enforcement data released is not personal information.

Victoria Police practice is to use MOUs or MOU-like documents whether or not the other party is a public or private sector organisation. It has been impossible to determine why this is the case or why the practice continues. The problem with this practice is that *in all cases* the MOU is legally unenforceable as against any private sector party to it. Thus, any confidentiality or information security obligations that are imposed cannot be enforced legally. Such a practice constitutes a risk to Victoria Police's ability to comply with its regulatory responsibilities.

None of the MOUs sighted by CLEDS, including the Major Project MOUs, have an end or termination date. This means that many obsolete MOUs might still apply even though the circumstances have changed. Good practice suggests that MOUs or similar arrangements under which law enforcement data is released should, at the least, be reviewed periodically – at least every two years - to ensure that they remain relevant and the arrangements remain appropriate. It would be sensible for the review point to coincide with appropriate audit or verification activity to ensure that law enforcement data release obligations under the CLEDS Standards have been observed.

The use of MOUs is not a uniform practice. Sometimes cooperative or collaborative arrangements are documented in instruments that are described differently, for example, 'protocols', 'guidelines' or 'operating procedures' or some other description. Sometimes the

4 Letter from Victoria Police to CLEDS dated 12 February 2010

arrangements consist of an exchange of correspondence that is given no label. This lack of uniform practice creates risks for Victoria Police because there is no assurance that key issues are dealt with consistently.

During the course of this review, members of Victoria Police expressed a variety of opinions about the use of MOUs. Some thought that they were more trouble than they are worth, particularly as there are so many of them and their use is so loosely controlled. For example, it is difficult to provide a precise overview of Victoria Police MOUs or MOU-like arrangements because there is currently no central register of MOUs and there has been no central oversight of them. MOUs or MOU-like arrangements have been developed across Victoria Police that presumably impose a variety of obligations – whether legally enforceable or not - on the organisation but it is impossible for anyone to determine their nature and extent and, accordingly, whether Victoria Police and the parties to MOUs have complied with them or not.

A number of causes have contributed to this unsatisfactory situation. Gaps in governance have permitted arrangements for the release of law enforcement data to be developed in the absence of any meaningful authorisation or oversight process and without the knowledge of senior management. Inadequate policies have provided little useful guidance to those faced with the task of developing and implementing law enforcement data release arrangements. Policy gaps have meant that there is no delineation between complex and sensitive information sharing and less sensitive, more straightforward arrangements. There are no standard form precedents and templates available to assist Victoria Police members to prepare documentation. There have been no useful and accessible education and training materials available to inform the MOU negotiation and drafting process. In breach of the CLEDS Standards, there has been no consistent process by which release arrangements are recorded, meaning that the release of law enforcement data cannot be effectively audited.

In these circumstances, it is understandable that some Victoria Police members are sceptical about the usefulness of MOUs. That said, the underlying problem is the lack of effective policies, procedures and training to support the MOU process, rather than the need to record the arrangements in writing.

MOUs are perceived as the accepted method to document cooperative arrangements and associated information sharing issues. By default, this practice means that all such arrangements are invariably legally unenforceable even though there are instances – as here – where private sector organisations are involved that should be bound to a legally enforceable agreement. The consequence is that confidentiality requirements and accountability mechanisms such as audit rights cannot be enforced through the courts.

Because of the inadequacies of the Victoria Police law enforcement data release policies, there is no guarantee that Victoria Police MOUs or MOU-like arrangements accurately reflect the applicable legal or regulatory requirements and include adequate legal mechanisms to enforce compliance. For example, no Victoria Police MOU that has been sighted as part of this review or the larger work undertaken by the CLEDS office, refers to Victoria Police's obligations under the Victorian Charter of Human Rights and Responsibilities. In many cases, relevant obligations imposed under the CLEDS Standards are overlooked.

Although this review is concerned with Major Project Development MOUs it is worthwhile noting that there is no Victoria Police policy that mandates when and in what circumstances an MOU or other written arrangement is required before law enforcement data may be released. This governance deficit means there is the potential for Victoria Police policy to be circumvented by the simple means of establishing informal, verbal arrangements to release law enforcement data. This policy gap requires urgent remediation.

Chapter 3 findings

Victoria Police law enforcement data release policies, procedures and training are inadequate and confusing. They fail to:

- adequately describe and support the relevant regulatory framework
- describe when an MOU or a less formal written arrangement is needed
- delineate between the circumstances where more complex and less complex information release arrangements are required
- describe the authorisation process for law enforcement data release
- establish minimum terms and conditions for MOUs or other arrangements for the release of law enforcement data
- provide precedents, templates and checklists to assist those who develop information release arrangements
- establish a central register of MOUs
- establish proper oversight mechanisms for MOUs
- establish sufficient guidance about the regulatory requirements, in particular, the CLEDS Standards and the Charter
- provide adequate education and training about information release requirements.

Chapter 3 Recommendations

One of the themes of CLEDS' reviews of Victoria Police's law enforcement data security practices over the last few years has been the inadequacies of its security arrangements for data release and access for third parties. The findings in this chapter are consistent with the fact that our recommendations about these matters have not been implemented.

Any further delay in addressing these issues is unacceptable. Accordingly the recommendations that follow are designed to establish a reform process that will be subject to intensive supervision by my office.

Victoria Police must:

- finalise a central register of law enforcement data release MOUs as a matter of urgency
- urgently review those parts of the Victoria Police Manual and associated or related documents concerning law enforcement data release in a manner consistent with this review's findings and submit these to CLEDS for analysis and comment
- develop appropriate precedents, templates and checklists to assist Victoria Police members to develop law enforcement data release arrangements and submit these to CLEDS
- develop appropriate training and educational materials to assist and inform Victoria Police members to develop, implement and monitor law enforcement data release arrangements and submit these to CLEDS
- by no later than 14 days after the publication of this review, nominate a person and Division of Victoria Police responsible for implementing these recommendations

- by no later than 28 days after the publication of this review, provide CLEDS with a proposal and associated timelines for implementing the recommendations set out in this chapter and to report on implementation progress on a monthly basis until the recommendations are fully implemented.

4 Information Sharing – The Legal and Regulatory Framework

4.1 Overview

This section is a high-level description of the Victorian regulatory framework that applies to Victoria Police's sharing of information. There is no single law that covers the field. For Victoria Police, information sharing decision-making involves considering and applying a series of laws and regulatory requirements. This chapter summarises them. A more detailed analysis is set out in Appendix 1.

4.2 Information Privacy

The IPA regulates the collection and handling of personal information by Victorian public sector organisations – such as Victoria Police – and for private sector organisations to the extent that they are parties to a 'State Contract.' Victoria Police can only collect personal information if the collection is necessary for one or more of its functions or activities.

For the use and disclosure of personal information, the general rule is that personal information collected for one purpose – the primary purpose of collection – can be used and disclosed for the same purpose. Use and disclosure beyond the primary purpose of collection – i.e., for a secondary purpose - is permitted in some limited circumstances. These are set out in IPP 2.1. For example, disclosure of personal information for purposes unrelated to the primary purpose of collection is permitted where:

- the organisation has reason to suspect that unlawful activity may be engaged in and discloses the personal information as part of its investigation or in reporting concerns to relevant authorities (IPP 2.1(e))
- a law enforcement agency reasonably believes that the disclosure is necessary for the prevention, detection, investigation or prosecution of a criminal offence (IPP 2.1(g)).

In addition, s13 of the IPA exempts a law enforcement agency from complying with IPP 2.1 if it believes on reasonable grounds that non-compliance is necessary for the purposes of its, or any other law enforcement agency's, law enforcement functions or activities or, in Victoria Police's case, for the purposes of its community policing functions.

This system of exemptions from the normal restrictions on the use and disclosure of personal information gives Victoria Police and other law enforcement agencies some latitude in disclosing personal information provided they satisfy the tests set out in the exemptions. These tests generally rely on an assessment of what is reasonable, i.e., an objective test of the organisation's belief in respect of the proposed personal information disclosure and must be applied on a case-by-case basis. Provided the relevant legal tests are satisfied, Victoria Police can lawfully disclose personal information in a broad range of circumstances and to a broad range of recipients.

4.3 Information Security

The CLEDS Act establishes a law enforcement data security regime that binds Victoria Police. The regime is set out in the CLEDS Standards which is a set of highlevel information security

standards drawn from international and national benchmarks. The CLEDS Standards apply to 'law enforcement data.' This term is defined broadly in the CLEDS Act to include any information obtained, held or received by Victoria Police for the purposes of its law enforcement functions. Thus the CLEDS Standards cover personal information as well as the overwhelming bulk of other information held by Victoria Police.

The CLEDS Standards that are of most relevance to the Major Project Development MOUs are in Chapter four of the Standards, which relate to information release. The objective of the information release Standards is to prevent the unauthorised release of law enforcement data by requiring that procedures be established that ensure that all disclosure is controlled and the recipients are informed of their responsibilities.

The primary obligation under Standard 11 is that release of law enforcement data must only occur if it is authorised. The protocols to Standard 11 require Victoria Police to develop and promulgate policies and procedures that cover a range of law enforcement data release issues, to establish mechanisms to monitor and audit the release of law enforcement data and to develop and publish training material relating to the release of law enforcement data. Any Victoria Police release or sharing of law enforcement data must comply with the relevant CLEDS Standards.

4.4 Charter of Human Rights and Responsibilities

The Charter requires that human rights be taken into account when Victorian laws, policies and procedures are developed, interpreted and applied. The Charter obligations apply to all Victorian public authorities, including Victoria Police.

Under s 38 of the Charter it is unlawful for a public authority to act incompatibly with a human right or, when making a decision, to fail to give proper consideration to a human right.

The human rights protected by the Charter are derived from a range of international human rights instruments. The most relevant to the Major Project Development MOUs are:

- privacy and reputation (s13) and
- peaceful assembly and freedom of association (s16).

A decision to collect or disclose information is a decision to which the Charter applies. It follows, therefore, that the Charter rights must be taken into account and applied by Victoria Police and by DSE when making decisions about sharing information.

4.5 Victoria Police information release policy

The Victoria Police Manual (VPM) contains policy rules about the use and disclosure of information. The current version was issued on 22 February 2010. These policy rules 'are mandatory and provide the minimum standards that employees must apply.'⁵

The rules emphasise that employees must not disclose Victoria Police information 'without appropriate authority.'⁶ The relevant authority is derived, according to the policy, from legislation and the policies and procedures in the VPM and other referenced documents.⁷

The current version of the relevant policy rules replaced amendments that came into effect in September 2008. It was these 2008 rules that applied at the time the Desalination MOU was executed.

5 VPM – Policy Rules – Use and disclosure of information – Application, p1

6 *ibid.*, Section 2, p2

7 *id.*

The current version of the VPM policy rules on the use and disclosure of information are incomplete. They only partially comply with the CLEDS Standards and omit key references to other regulatory requirements such as information privacy obligations. These are currently noted as being under development. They do not refer to the Charter at all.

4.6 Other legislation

For the sake of completeness it is necessary to briefly comment on other categories of information laws.

Some legislation specifically mandates the use and disclosure of certain categories of information. To the extent that it does so, it overrides the restrictions in the IPA. No such legislation applies in the current circumstances.

In addition, some legislation establishes secrecy provisions that prohibit staff from disclosing information they obtain in the course of their engagement. One such provision is s127A Police Regulation Act 1958. I have received no evidence that leads me to believe that this provision may have been contravened in the case of the Major Project Development MOUs.

5 Major Project Development MOUs – Desalination and Mt Sugarloaf

5.1 Introduction

Having examined the purpose of Victoria Police MOUs and the applicable regulatory and policy framework, this chapter examines the narrower question of how the Major Project Development MOUs operate. Although the focus is on the Desalination MOU, the analysis also applies to the Mt Sugarloaf MOU but with some noted exceptions. The key provisions are examined and analysed and a number of issues that either have not been covered or have not been covered adequately are highlighted.

5.2 The Desalination MOU

The Desalination MOU was executed on 28 August 2009 and came into effect on the financial close of the desalination project, 2 September 2009, when the project site was formally handed-over to AquaSure. The parties are Victoria Police, the Secretary to the Department of Sustainability and Environment (DSE) and AquaSure Pty Limited.

The Desalination MOU has no express termination date nor is there any timeframe within which the parties are to review it. Presumably, it continues in force until the completion of the desalination project.

5.3 Desalination MOU Documents

The arrangements consist of the Desalination MOU itself together with a number of schedules and other documents. These are set out in a disorganised and disjointed manner. For example, the Standard Operating Procedures refer to two appendices⁸ but the documents in question are headed as Annexures.

The documents that have been used as the basis of this review are:

Memorandum of Understanding for Victorian Desalination Project between Victoria Police, Secretary to the Department of Sustainability and Environment and AquaSure Pty Limited dated 28 August 2010 (Desalination MOU) together with:

Schedule 1 – Schedule 1 Acts

Schedule 2 – Standard Operating Procedures – Demonstrations – Protest action (undated) together with two annexures headed Range of protest actions (Annexure A) and Tactics (Annexure B) respectively

Schedule 3 – Project Incident Management Plan. Although headed as such, this document is not the Project Incident Management Plan designed for use in the Desalination project. Rather, it is a document that foreshadows the development of the actual Project Incident Management Plan and indicates what that document might contain. It states that the parties ‘will liaise in good faith to develop and settle the Project Incident Management Plan (using the existing Victorian Desalination Project Civil Disruption Management Plan (CDMP) V16 19 June 2009 (Annexure 1 to this Schedule 3) as a basis...’⁹

⁸ 8 SOP, clause 4.5, Range of protest action and responses

⁹ Preamble to Schedule 3 to the Desalination MOU. The CDMP was prepared for use by Victoria Police and DSE during the phase of

Thus, the Project Incident Management Plan did not exist at the date the Desalination MOU was executed. By letter dated 16 March 2010, DSE supplied me with:

- project Incident Management Plan (**PIMP**) dated 17 March 2010 together with two Annexures – Annexure 1 contains procedural flowcharts, Annexure 2 is headed ‘Table of relevant offences and who may enforce’
- protocols for Law Enforcement Data (and other MOU data) (**PIMP Protocol**) dated 17 March 2010.

Neither the PIMP nor the PIMP Protocol were finalised when the Desalination MOU was executed. The PIMP Protocol was not foreshadowed in the Desalination MOU. The MOU documentation itself notes that the PIMP would be derived from the CDMP. The PIMP and the PIMP Protocol dated 17 March 2010, were provided to me by letter dated 16 March 2010 and have, I am informed, been generally accepted¹⁰ by Victoria Police and AquaSure.

It is surprising that key documents that address important policies and operational procedures, in particular the important issues of the security of law enforcement data, were developed almost 6 months after the MOU was executed.

Overall, the MOU documentation reflects the normal practices for MOUs discussed in chapter 3. The MOU itself deals with higher-level issues and the Schedules and attachments are designed to cover operational process and procedures in more detail.

5.4 Purpose

Clause 3 states that the purpose of the MOU is to ‘facilitate arrangements between VICPOL, the Secretary and the Project Co in relation to the management of the proposed construction of the Project.’¹¹ Clearly this statement is wrong. Victoria Police has no expertise ‘in relation to the management of the proposed construction of the Project.’ Victoria Police’s role is not to manage large critical infrastructure construction projects.

This is not a pedantic legal point. Normally, a ‘purpose clause’ is one of the key matters taken into account when interpreting legal documents in cases of ambiguity or uncertainty because it constitutes express evidence of what the parties intended. Using clause 3 as an aid to interpretation would not produce a logical outcome. As will be seen, this is just the first example of inaccurate drafting in the MOU.

Recital C, in the Background section of the MOU, is a more accurate description of its purpose. It states:

‘C. VICPOL, the Secretary and Project Co wish to enter into an agreement for the management of protest action at construction sites or along the construction corridors in relation to the Project and the effective detection, identification and prosecution of persons who commit offences under the Acts set out in Schedule 1 hereto...’¹²

activities before the awarding of the Desalination project to AquaSure and related to activities such as preliminary investigation of the plant site and along pipeline and power corridors to inform environmental assessments and to provide technical data for potential project bidders. The CDMP ceased to operate from the effective date of the Desalination MOU, i.e., financial close of the project, 2 September 2009.

10 Letter to CLEDS from DSE dated 16 March 2010

11 Clause 3 – Purpose of this MOU – Desal MOU

12 Paragraph C, Background

5.5 Enforceability

Clause 14.12 of the MOU specifically addresses the issue of its enforceability. It states that:

‘This document is not intended to create legal relations or constitute a legally binding contractual agreement between the Parties. Notwithstanding this clause, the Parties will demonstrate good faith in complying with all of the terms of this MOU.’

There is little doubt that the MOU does not create any legally binding obligations between the government parties and AquaSure. However, some safeguards are built into the MOU that are designed to address privacy and confidentiality issues. These could have been made legally binding as against AquaSure. The fact that they are not is problematic. These issues are discussed in greater detail later in this chapter.

Although the Desalination MOU itself is not legally binding, other of the desalination project documents establish consequences for non-compliance. Under the project documentation, an ‘Intervening Event’ occurs if Victoria Police fails to comply. The consequences can be significant. Amongst other things, AquaSure may be entitled to an extension of time to complete the project and/or to compensation. That being the case, it was critically important that the MOU correctly addressed legal compliance issues, in particular information sharing obligations.

5.6 Structure

The key operative parts of the Desalination MOU fall into two main categories. The first relates to the parties’ roles, responsibilities and mutual assistance. The second is information sharing.

5.6.1 Roles, responsibilities and mutual assistance

The MOU delineates between two broad areas of cooperation between the parties. These are referred to as ‘General arrangements’ (clause 5) and ‘Special arrangements’ (clause 6).

5.6.2 General arrangements

Clause 5 sets out the roles and responsibilities of the parties in the face of protest action. It establishes who, as between VICPOL and the Secretary, is responsible for the prosecution of which offences, who pays for what and how each will assist the other.

In order to understand how law enforcement roles and responsibilities are allocated, it is necessary to understand the meaning of ‘Schedule 1 Acts.’

Schedule 1 Acts are a series of laws:

- the *Land Acquisition and Compensation Act 1986*
- the *Water Act 1989*
- any by-law under the *Water Act 1989*, and
- section 52 of the *Summary Offences Act 1966*.

These are the pieces of legislation that contain the criminal offences that are the most relevant to protest action against both the desalination plant and its associated infrastructure and the Mt Sugarloaf pipeline. At law the Secretary of DSE (effectively DSE) is a law enforcement agency in respect of offences under the Schedule 1 Acts.

In clause 5(a), Victoria Police agrees to ‘provide appropriate police assistance’ to the Secretary and AquaSure to enforce the provisions of the Schedule 1 Acts ‘at or upon the request’ of AquaSure or the Secretary ‘where protests or other incidents assessed as presenting an imminent breach of the peace, public disorder or offences against the person or property at the construction sites or along the construction corridors in relation to the Project are occurring or are about to occur.’

Under the next clause, 5(b), Victoria Police retains operational discretion to ‘determine the level, type and timeliness of police assistance, response to and resources required’ in relation to protest or other like activity.

Under clause 5(c), it is the Secretary, DSE who remains ‘the principal agency responsible for regulating and controlling offences under any of the Schedule 1 Acts including the compilation of briefs of evidence and prosecution of offenders.’ Under clause 5(f) ‘the Secretary will attend to all formalities in the prosecution of any offences committed under any of the Schedule 1 Acts. Such formalities include the issue of summonses and the prosecution of charges before a court (as well as the attendance to any subsequent appeal to any superior court).’ Under clause 5(h), the Secretary is responsible for paying any costs or expenses awarded in the prosecution of any of the Schedule 1 Acts, including where Victoria Police is the informant.

Victoria Police is allocated other responsibilities under clause 5(e):

‘Where a person commits an offence under an Act:

- i. the provisions of which are neither relevant to or enforceable by the Secretary; or
- ii. other than a Schedule 1 Act,

VICPOL will take appropriate action against such a person including his/her arrest where appropriate at the discretion of the Police Operational Commander.’

The remaining provisions¹³ cover other details of the parties’ roles and responsibilities, including arrangements about payment of costs of prosecutions and payment of overtime to police officers.

5.6.3 Special arrangements

Clause 6 of the MOU contains what are referred to as ‘Special arrangements.’ It is designed to cover the allocation of the parties’ responsibilities in somewhat greater detail than clause 5 but there is some duplication:

- AquaSure staff and contractors are to contact AquaSure itself or the Secretary, **not** Victoria Police if they suspect operations will be disrupted or the subject of a protest. Both AquaSure and the Secretary agree to attempt to resolve the situation but if they cannot, they will request Victoria Police support
- if VICPOL responds to a protest, a representative of AquaSure or the Secretary (as appropriate) will attend the scene to make any formal demands
- subject to operational priorities, VICPOL will make police resources available during the construction period to respond to protest incidents and breaches of the peace
- AquaSure and the Secretary will provide specialist advice or support to Victoria Police

¹³ Other than clause 5(k) and (l).

- protest law enforcement operations and ‘response to other incidents’ is to be managed in conformity with a number of documents. These consist of the Project Incident Management Plan (PIMP), Victoria Police operating procedures, the Victoria Police Manual and the law. Control of each operation depends on the circumstances. If Victoria Police assumes control, the Secretary and AquaSure will provide support if required
- the parties are to prepare operational plans for the areas where protests may occur.

Clauses 5 and 6 taken together constitute the framework under which two law enforcement bodies, Victoria Police and DSE, document their roles and responsibilities in the face of potential protest action directed at the construction of the desalination plant and related infrastructure. AquaSure’s obligations are of a more limited nature – for example, making a representative available and providing support.

5.6.4 Information Sharing under the Desalination MOU

The four key clauses in the Desalination MOU that cover information sharing are clauses 5(k), 5(l), 8 and 9.

5.6.4.1 Clauses 5(k), (l), 8 and 9

Clause 5(k) of the Desalination MOU states that:

‘Subject to clause 9, VICPOL, the Secretary and Project Co **will** share information held by each other in order to effectively implement and (sic) terms of this MOU.’ (my emphasis)

Clause 5(l) states that ‘(n)othing in this clause 5 is intended to abrogate or extend any responsibilities that VICPOL, the Secretary or Project Co have under general law.’ The effect of this clause is minimal. Clearly, the terms of an MOU cannot abrogate or extend the law.

Clause 8(a) of the Desalination MOU states that:

‘(a) VICPOL **will** release Law Enforcement Data to the Secretary and Project Co under this MOU. The release of Law Enforcement Data is subject to the Standards and Protocols for Law Enforcement Data Security, established under the Commissioner for Law Enforcement Data Security Act 2005 (Vic).’ (my emphasis)

The first point to note is that clause 5(k), under which all the parties are to share information, is subject to clause 9, which deals with confidentiality and privacy. Clause 8 imposes substantially the same obligation but only on Victoria Police.

However, clause 8 is not subject to clause 9. There is no apparent rationale for this distinction.

Secondly, as clause 5(k) obliges all of the parties to share information with each other, it is difficult to understand why clause 8(a) was necessary at all. The only reason for this is that the information security requirements mandated by the CLEDS standards which clause 8 attempts to cover were misapplied.

In both clauses 5(k) and 8 ‘will’ is used to describe the obligation to share information or release law enforcement data. Presumably ‘will’ was used deliberately, rather than mandatory terminology such as ‘must’ or ‘shall’ or discretionary terminology such as ‘may.’

The Macquarie Dictionary gives a number of meanings for ‘will’ depending on its usage. When (as here) it is used as a verb, it signifies a future likelihood or expresses a resolve or willingness to

do something. Used as a noun, it can express a wish or desire, or to decide by an act of will.¹⁴ In my opinion the natural and ordinary meaning of the word ‘will’ as used in both clauses is that Victoria Police intends or is willing to disclose personal and other information or release law enforcement data (which includes personal information). The problem with this approach to drafting is that these general obligations are not qualified or limited in any substantial way. This error lies at the heart of the MOU’s approach to information sharing.

Victoria Police contests this interpretation of clause 8. It argues that:

‘The opening sentence in Clause 8(a) is plainly not intended to represent an expectation on Victoria Police to hand over all its law enforcement data to the other parties. In fact, the clause specifically does not address the issue of ‘when’ or ‘whether’ information may or may not be disclosed by Victoria Police. As noted in this (sic) opening sentence of the clause, those issues are dealt with elsewhere ‘under this MOU’...’¹⁵

Clearly, the MOU does not require Victoria Police to hand over all its law enforcement data. But that is not the point. The problem is that the necessary limitations on law enforcement data release are **not** satisfactorily dealt with elsewhere in the MOU. On its face, the clause records Victoria Police’s willingness to release law enforcement data to the parties. An implicit restriction on this obligation is that any release would need to relate to the purposes of the MOU. This provides little reassurance given my earlier comments about the MOU’s defective purposes clause. That apart, there are no safeguards or checks and balances.

The problem is magnified by clause 8(b) which explains the definition of ‘law enforcement data’ in clause 1.1 of the MOU. It describes a broad catalog of the forms in which law enforcement data may be embodied and to whom the data might relate. Read in conjunction with clause 8(a) Victoria Police’s obligation is that it **will** release a very broad and potentially intrusive law enforcement dataset to the Secretary and AquaSure.

Victoria Police also argues that the MOU cannot require Victoria Police to release information in breach of the law. ‘The MOU does not impose and does not purport to impose any legally enforceable obligations, or any other obligations, on Victoria Police. Victoria Police at all times will act in accordance with the law, and in accordance with applicable Victoria Police policies and Chief Commissioner’s instructions, and upon independent operational considerations.’¹⁶ It is self evident that the Desalination MOU cannot oblige Victoria Police (or any other party to it) to breach the law. It is also clear that the Desalination MOU is not, of itself, legally binding. However, these arguments beg the question why Victoria Police chose to enter into the Desalination MOU at all. If Victoria Police’s arguments are correct, a letter to that effect to DSE and AquaSure would have sufficed.

I have no doubt that Victoria Police did not intend to unlawfully share law enforcement data. However, greater care should have been taken to ensure that the express words of the written arrangements it entered in to reflected that intent. Broad statements that Victoria Police **will** share information unaccompanied by qualifications that reflect the relevant legal limitations and which represent the parties’ shared understanding about **how** those legal obligations will be put into practice in the particular circumstances are inappropriate.

14 See Macquarie Dictionary, edn 5, p 1889

15 Letter to CLEDS dated 12 February 2010, p6

16 Letter to CLEDS dated 14 July 2010, p4

DSE would also disagree with my interpretation of clause 8. After noting that clause 8 is headed 'Data Security,' it argues that:

'Clause 8(a) was not intended to confer a separate obligation on VICPOL to share Law Enforcement Data with the Secretary or Project Co or, conversely, to confer a separate right on the Secretary or Project Co to receive such Law Enforcement Data. VICPOL will only share limited information with the Secretary and Project Co in accordance with clause 5(k) (and clauses 3(2) and 5.5 of the SOP), recognising that any such sharing of information is subject to the limitations in clauses 5(l) and 9. On a proper construction, based on the factual matrix, clause 8(a) was inserted at the express request of VICPOL in the context of imposing the compliance requirements of clause 8(b) and (c) and should be constructed as acknowledging that any sharing of information between VICPOL, the Secretary and Project Co in accordance with the other provisions of the MOU would be subject to the further limitations of clause 8. It was anticipated that VICPOL would retain primary responsibility for ensuring compliance with the limitations under clause 8.'¹⁷

Although clause 8 is headed 'Data Security,' under clause 1.3 of the MOU the headings used in it 'do not affect the interpretation of this document' and I have accordingly disregarded them.

I do not consider that DSE's interpretative approach, which involves imposing multiple glosses on the express words used in clause 8(a), is correct. The plain words of the clause state that 'Victoria Police **will** release law enforcement data...' However, even if the DSE approach to interpretation is correct, it does not produce the outcome suggested. The submission contends that clause 5(l) – which is expressly stated only to apply to clause 5 – and clause 9 – which is unenforceable – operate so as to limit clause 8(a). Clearly clause 5(l) does not apply to clause 8. Clause 9 is unenforceable but even if it was, it does not limit Victoria Police's obligation to share information – it only imposes confidentiality obligations on information already shared.

Moreover, it is difficult to understand how it could be said that it 'was anticipated that VICPOL would retain primary responsibility for ensuring compliance with the limitations under clause 8.' If this means that information security was a secondary priority for DSE and AquaSure, the express words used in clause 8(c) and Victorian whole of government information security policy are to the contrary.

In my opinion, Clause 8 is an example of the misapplication of a precedent clause. It was designed to serve one purpose – law enforcement data security protection - but has been used for another purpose. A provision similar to clause 8 was developed by Victoria Police to comply with new internal MOU guidelines. My office provided feedback on the proposed draft in 2008. As then drafted, the clause was designed to ensure that *if or where* Victoria Police authorised the release of law enforcement data, the recipient should be required to observe appropriate information security obligations. The original intent of the clause is reflected in clause 8(c) which imposes security obligations that include:

- how law enforcement data should be physically stored
- how data in an electronic form should be stored and protected
- the security of the transmission of law enforcement data
- security obligations for portable computing and storage devices
- the destruction of law enforcement data.

¹⁷ Submission dated 23 December 2010

As originally drafted, clauses 8(b) and (c) were designed to ensure that necessary security obligations applied to the broadest dataset possible. The clause was not designed to be combined with an obligation to, in effect, release everything. Clause 8(a) erroneously conflates data security with data disclosure.

As drafted, clauses 5(k) and 8 impose wide and significant information sharing obligations on Victoria Police. Their unqualified nature is not consistent with Victoria Police's legal obligations. The Desalination MOU is defective to the extent that its information sharing provisions do not align and support compliance with relevant Victorian laws.

Finally, as all of the clauses of the Desalination MOU are not legally enforceable, the law enforcement data security obligations established under clause 8 cannot be enforced by Victoria Police against AquaSure. If AquaSure was to breach the clause 8 requirements, Victoria Police would have no legal redress under the MOU. This is unsatisfactory as it is not consistent with the approach to the release of law enforcement data taken in the CLEDS Standards.

5.6.4.2 Clause 9

The obligation to share information in clause 5(k) is subject to clause 9. Clause 9 deals with confidentiality and privacy. The prime confidentiality obligation is that the parties 'may use the Confidential Information of the other Party only for the purposes of this MOU.'¹⁸The main privacy obligation is that the '(P)arties will cooperate to ensure they do not cause any other Party to breach any privacy obligations that Party may have at law.'¹⁹

As noted earlier, these provisions are not legally binding because of clause 14.12. The result is that confidential information communicated by a party under the MOU will not be protected by clause 9. Thus, one of the information sharing safeguards the parties decided to include in the MOU is ineffective. Similarly, each party's obligation not to cause the others to breach privacy is also unenforceable. This does not, of course, mean that they are not bound to comply with privacy law – it only means that the parties' obligation not to cause each other to breach privacy is not enforceable.

It would have been a relatively straightforward matter for the parties to have drafted an MOU that covered governance, roles and responsibilities and that established a coherent information sharing framework. This could have been supplemented by a legally enforceable Deed that addressed the law enforcement data security obligations dealt with in clause 8 and the confidentiality and the privacy matters dealt with in clause 9 that would have bound AquaSure as against both Victoria Police and the Secretary of DSE. These and the other defects in the MOU's information sharing provisions signify, in my opinion, real confusion about how the parties should have approached the complex and sensitive issues surrounding information sharing for the Desalination project.

5.7 The subordinate documents

These consist of SOPs, the PIMP and the PIMP Protocols.

The SOPs make a number of references to information sharing.

¹⁸ Clause 9.1(a)

¹⁹ See clause 9.2

Clause 3 delineates between low and high-risk protest action. Clause 3.2 requires DSE and AquaSure to notify Victoria Police of any protest action. It also states that:

‘(a)ny intelligence received by Victoria Police that indicates the possibility or occurrence of protest action will be assessed by Victoria Police prior to advising Project Co of the possibility or occurrence of such protest action.’

Clause 4.6, which is headed ‘Proactive Response’ states that:

‘Where intelligence has identified persons known or believed to be involved in organising or conducting protest action and proactive measures are considered appropriate, a joint operation is to be considered by the Secretary, Project Co’s manager and Victoria Police. Victoria Police resources which may be considered for use in such a joint operation include the Search and Rescue Squad and the Security Intelligence Group.’

The meaning of a ‘proactive’ response or measure is unclear.

Clause 4.8 is headed ‘Intelligence’ and states that:

‘The use of intelligence will play a significant role in enforcing the law at construction sites or along the construction corridors in relation to the Project. The Secretary and Project Co personnel, contractors and subcontractors will be relied upon to gather and disseminate intelligence to Victoria Police in a timely manner for the purposes of both proactive response and general enforcement.’

What is concerning about these clauses is that intelligence information is to be used and shared without any apparent consideration having been given to any countervailing safeguards or to whether this is a proportionate response. There is no indication about how long intelligence information might be kept. There is no mention about how intelligence gathered about persons who have never been charged with a criminal offence and who engage in entirely lawful protest action should be treated as against intelligence gathered about alleged offenders. It is also surprising that the use of the Victoria Police Security Intelligence Group is foreshadowed to deal with what is, in reality, the prospect of low-level crime.

The PIMP is ‘intended to provide more detailed guidelines...for the management of protest action.’ There is some overlap between the MOU, the SOPs and the PIMP. Primarily, these consist of duplicate statements about roles and responsibilities.

The PIMP also sets out to provide guidance to AquaSure’s contractors and subcontractors even though they are not parties to the MOU. They are collectively known as AquaSure Associates. Inexplicably, in Annexure 2 to the PIMP which is a table entitled ‘Offences and Who may enforce’, Melbourne Water, for the first time in any of the MOU documentation, is mentioned as an entity entitled to enforce Schedule 1 Acts. This appears to contradict the many statements made to the effect that this responsibility rests with the Secretary, DSE.

The PIMP Protocols are not foreshadowed in the MOU and appear to have been developed after this review was initiated. The document delineates between ‘law enforcement data’ and ‘Information Holdings.’ The definition of law enforcement data is the same as in clause 8 of the MOU. This is not a satisfactory definition. The definition that should have been used is the definition in the CLEDS Act. The definition of ‘Information Holdings’ is ‘(a)ny information collected from VICPOL (not including law enforcement data) or collected by DSE directly...’²⁰ This definition is also problematic. Under the CLEDS Act any information held by Victoria Police for law enforcement or community policing purposes is law enforcement data. It is

difficult to imagine how information DSE collected from Victoria Police under the MOU could be anything but law enforcement data.

The purpose of the delineation appears to be to distinguish between information shared by Victoria Police and information collected by DSE itself. Under the MOU Victoria Police imposes a variety of information security obligations in respect of law enforcement data it shares. These obligations do not, of course, apply to information collected by DSE and not shared with Victoria Police.

However, the PIMP Protocols overlook two important information security issues. The first is that DSE must abide by the Whole of Victorian Government Information Security Management Policy.²¹ The policy is not mentioned at all in the Protocol document. Other Victorian Government information security requirements, such as the Information Security Management Framework²² and Information Security – Data Classification and Management²³ are similarly overlooked. Secondly, no consideration is given to the information security position where law enforcement data and Information Holdings are aggregated and commingled.

Irrespective of either definition, data must be handled in accordance with its security classification. Appropriate security classification lies at the heart of any robust security framework. The PIMP Protocol does not refer to security classification.

There are other problems with the PIMP Protocol, including:

- under clause 3.2(r), the Compliance Liaison Manager ‘will appropriately manage any Law Enforcement Data security incidents and ensure they are appropriately managed and reported to VICPOL...’ However, there is no reference to the generation and retention of audit logs and trails. There is no definition of a security incident
- there are no references to audit capabilities for physical security
- there are references to file encryption²⁴ but no detail about the standard to be adopted
- ‘authorised person’ is referred to throughout the document but there is no definition of the term nor is there any mechanism under which persons are authorised or are de-authorised. There is no reference to the need for security checking.

Overall, the information security arrangements established under the Protocol have not been thought through with sufficient rigour and are unsatisfactory in their current form, particularly in view of the fact that the sharing of sensitive intelligence data is foreshadowed in the MOU and other documents.

5.8 Analysis and Comments on the MOUs

It was entirely appropriate for two law enforcement organisations – Victoria Police and DSE – to seek to document their roles and responsibilities and the assistance they would provide to each other in the face of potential protest action that could lead to breaches of the law where their law enforcement functions might intersect.

21 [www.gsgjctonline.dtf.vic.gov.au/CA257310001D7FC4/WebObj/InformationSecurityManagementPolicy9 September05v1/\\$File/Information%20Security%20Management%20Policy%209%20September%2005 %20v1.2.pdf](http://www.gsgjctonline.dtf.vic.gov.au/CA257310001D7FC4/WebObj/InformationSecurityManagementPolicy9%20September05v1/$File/Information%20Security%20Management%20Policy%209%20September%2005%20v1.2.pdf)

22 [www.gsgjctonline.dtf.vic.gov.au/CA257310001D7FC4/WebObj/WoVGStandardInformationSecurityManagementFrameworkSECSTD01/\\$File/WoVG%20Standard%20Information%20Security%20Management%20Framework%20SEC%20STD%2001.pdf](http://www.gsgjctonline.dtf.vic.gov.au/CA257310001D7FC4/WebObj/WoVGStandardInformationSecurityManagementFrameworkSECSTD01/$File/WoVG%20Standard%20Information%20Security%20Management%20Framework%20SEC%20STD%2001.pdf)

23 [www.gsgjctonline.dtf.vic.gov.au/CA257310001D7FC4/WebObj/WoVGStandardInformationSecurityDataClassificationandManagementSECSTD02/\\$File/WoVG%20Standard%20Information%20Security%20Data%20Classification%20and%20Management%20SEC%20STD%2002.pdf](http://www.gsgjctonline.dtf.vic.gov.au/CA257310001D7FC4/WebObj/WoVGStandardInformationSecurityDataClassificationandManagementSECSTD02/$File/WoVG%20Standard%20Information%20Security%20Data%20Classification%20and%20Management%20SEC%20STD%2002.pdf)

24 Clause 3.2(i) and (l)

The MOU:

- assists in demarking operational responsibilities
- safeguards against duplication and waste
- sets out who pays for what
- establishes the roles and responsibilities of the parties, and
- sets out areas of cooperation and assistance.

In the circumstances, it is also appropriate for the responsibilities and contributions of the private sector organisation likely to be directly effected by protest action be documented, particularly where their cooperation and assistance may be needed to ensure that law enforcement operations are undertaken effectively and efficiently.

That said, in my opinion the Desalination MOU does not deal with key issues of roles and responsibilities as well as it might. My comments fall into two main areas:

- a need for more comprehensive governance arrangement, and
- a fragmented approach to roles, responsibilities and information sharing.

The MOU is an important document that regulates the parties' approach to and implementation of their roles and responsibilities and their provision of mutual assistance over the period of time during which the desalination plant is built. It also establishes sensitive information sharing arrangements. No document can anticipate and provide answers to all of the issues that might arise in the face of that complexity.

The MOU fails to establish formal oversight mechanisms to oversee the management of the parties' relationship so that operational or other issues can be raised, decisions made and disputes or uncertainties resolved. This governance deficit also has important implications for information sharing issues and is dealt with in greater detail in the next section. The only reference in the MOU to the establishment of governance arrangements is in clause 4(b) which states that '[T]he parties will work together to cooperate within the principles specified in this MOU and agree to undertake appropriate joint planning and management in relation to the Project.' The principles are not explicitly stated in the MOU. Key statements relevant to governance appear in clause 4.2 of the Standard Operating Procedures (SOPs) which states that Victoria Police, the Secretary and AquaSure will ensure 'that there is ongoing and effective consultation, coordination, planning and management in relation to protest action' Such a provision should have been included, together with related material, in the MOU itself and formal structures built-in to implement these arrangements.

Although the MOU addresses a wide range of operational and practical issues, it does so in a fragmented way. Clauses 5 and 6 cover many important issues but do not do so thematically. Some of the material in the MOU is duplicated in the schedules and attachments. The result is a complex set of documents that do not group together issues that involve the same subject matter. A good example of this is that the key issue of information sharing is not dealt with in consolidated provisions that comprehensively articulate the principles that should guide the disclosure and handling of sensitive information. Instead, information sharing obligations are sprinkled across the MOU and its subordinate documents.

Another example of this fragmented approach is the MOU's treatment of information security. Clause 8 imposes a range of high-level security obligations on DSE and AquaSure as likely recipients of Victoria Police law enforcement data. These are set out in clause 8(c). The security

obligations are high level obligations. For example, clause 8(c)(i) states that ‘the storage of electronic Law Enforcement Data must only occur on a computer system which is appropriately protected against unauthorised access, including the use of passwords, encryption, firewalls, and other appropriate protections.’ There is nothing in the subordinate documentation that applies these high-level requirements to on the ground operational circumstances or that spell out what compliance with these high-level obligations requires in practice.

There is no evidence that the development of the MOU or its implementation has been informed by what I would regard as standard information-sharing risk management practices. There is no evidence that a privacy impact assessment was undertaken. There is no evidence of an information security threat and risk assessment. There is no evidence that the obligations set out in Victoria’s Charter of Human Rights and Responsibilities have been addressed. Had these techniques been applied, it is likely that many of the MOUs shortcomings would have been addressed before it was finalised.

Victoria Police argues that it was unnecessary for the Desalination MOU to specifically mention the Charter. ‘It is not relevant whether or not the Human Rights Charter itself is mentioned in the MOU, the test is whether the MOU is consistent with the Charter.’²⁵ It points to clause 2 of the SOPs where reference is made to the fact that the parties each recognise the right to free speech, peaceful assembly and protest.²⁶

I disagree with this argument. The Desalination MOU is the framework chosen by the parties to, amongst other things, describe how they will approach information sharing issues. This requires them to not only identify the relevant laws but to set out their approach to complying with them. If Victoria Police’s argument was correct there was no need to refer specifically to any of their legal obligations. Provided there was nothing in the MOU that contradicted those obligations, all would be well.

In my opinion such an approach is manifestly inadequate. The relevant laws are principle-based and need to be applied and interpreted having regard to the circumstances. Just as the parties thought it was necessary to explain how they would cooperate with each other, it was also necessary for them to turn their minds in detail to how they proposed to address the legal compliance issues associated with the complex information sharing arrangements they had created.

5.9 The Sugarloaf MOU

The parties to the Sugarloaf MOU are the State of Victoria represented by Victoria Police and Melbourne Water. It was executed on 1 July 2008. The organisation contracted to construct the pipeline is not a party to the MOU. Therefore, unlike the Desalination MOU, there is no provision for information sharing between Victoria Police and a private sector organisation.

The Sugarloaf MOU is substantially similar to the Desalination MOU. One major difference is that the Sugarloaf MOU does not include an equivalent of clause 8 of the Desalination MOU. It has the same shortcomings as the Desalination MOU but:

- it does not include the unjustifiably broad obligation for Victoria Police to release law enforcement data found in clause 8(a) of the Desalination MOU
- the parties are government agencies

²⁵ Letter to CLEDS dated 14 July 2010, p10

²⁶ However, the clause omits any reference to the key relevant human right – the right to privacy.

- it doesn't cover law enforcement data security at all, and
- it does not include a PIMP or PIMP Protocol.

5.10 What information was shared?

I requested both Victoria Police and DSE to advise whether they had shared personal information with AquaSure under the MOU.

Victoria Police assigned an experienced Acting Inspector to conduct an inquiry which formed the basis of the following written responses from Victoria Police's Director, Legal Services:

'I am advised that no personal or confidential information has been released under this MOU to AquaSure.

Prior to the Desalination Project MOU being signed by the parties I am advised Victoria Police did not release any personal information to AquaSure.

To my knowledge, the only information that was released was an e-mail to an officer of DSE identifying nine protestors who had been charged with offences relating to entering and refusing to leave the desalination project site (copy email attached). The names of these people would have been publicly available on online court lists of the Magistrates' Court while their cases were pending, so I consider that disclosure of their names was permitted by s11 of the Information Privacy Act 2000. Additionally, I consider that disclosure was also permitted by s13(c) of the IPA, and Information Privacy Principles (IPP) 2.1(d), (e) and (f). I have made reference to this e-mail notwithstanding that it falls outside the scope of your review for the sake of completeness and transparency of policing arrangements at the desalination plant. In the circumstances, I request that the name of the VicPol officer or the protestors not be released.'²⁷

5.11 The 10 March 2009 email – Victoria Police disclosure of persons charged

The email referred to by Victoria Police was dated 10 March 2009. The email names nine individuals apparently arrested and charged on 14 July 2008, presumably in relation to protest activity about the Mt Sugarloaf pipeline. It was sent to DSE by Victoria Police unencrypted and over an insecure email network. There is no doubt that the email contains law enforcement data. The personal information provided appears to constitute 'sensitive information' as defined in the IPPs.

Victoria Police argues that this disclosure was permitted under the IPA for a number of reasons, including s11 of the IPA.

Section 11 states:

Nothing in this Act or in any IPP applies to a document containing personal information, or to the personal information contained in a document, that is –

(a) a generally available publication.

Section 3 of the IPA defines a generally available publication as 'a publication (whether in paper or electronic form) that is generally available to members of the public and includes information held on a public register.' Under this definition, it is important to note that it is the publication, not the information, that must be generally available.

²⁷ Letter to CLEDS dated 12 February 2010, p 5-6

Victoria Police's argument is that the personal information sought by DSE was published in an online list of pending cases published by the Magistrate's Court which is a publicly available publication. However, if the information was in a publicly available document it is not clear why it was necessary to ask Victoria Police for it. The persons named in the email were charged in July 2008 but the request for the information was made and answered almost nine months later, presumably when the cases had been determined and the names of the individuals removed from the online pending list. At the date of the request, therefore, the online list may not have been a generally available publication within s11 of the IPA.

Victoria Police argues that the disclosure was permitted under a number of the provisions in IPP 2.1. This might well be the case. It may be that the disclosure of the personal information was simply the legitimate provision of personal information by one law enforcement agency to another. However, the information available to me does not enable me to reach any firm conclusion. I am informed that the officer who sent the email is on sick leave and is not expected to return to work for some time and that there is no Victoria Police file relating to the request. In these circumstances, I have reached the view that I should disclose this matter to the Victorian Privacy Commissioner under s13 of the CLEDS Act for her further consideration.

5.12 Other information release

Apart from this, Victoria Police's written response leaves open whether other information, for example, law enforcement data that did not include personal information was disclosed to either DSE or AquaSure. On the basis of my interviews with relevant Victoria Police officers, very little non-personal law enforcement data has been provided to AquaSure by Victoria Police. Information provided has been general information about site security, suggestions about how AquaSure staff might respond to protest actions and the timing of protests.

The policing issues associated with the desalination plant are complex. Victoria Police is sensitive to the fact that some members of the local community oppose, and others support, the desalination plant. So, too, do local police officers. In order to retain the confidence of the local community, it is essential that Victoria Police not only discharges its functions fairly and impartially but is also seen to do so.

In my interviews with police officers what emerges is a reluctance to, in effect, outsource their core policing responsibilities to a private sector organisation that has no policing experience by providing it with sensitive operational police data. Victoria Police emphasise that there was never an intention to share its sensitive personal information with an organisation that they could not be sure would treat it in the same manner that Victoria Police does and which is not subject to the same regulatory restraints. For Victoria Police, the emphasis has never been on providing AquaSure with sensitive operational data. The reverse is the case – clause 4.8 of the SOPs clearly documents Victoria Police's reliance on intelligence from the other parties to the MOU.

5.13 DSE

DSE's written response to similar questions about its receipt or disclosure of personal information was:

'The DSE Capital Projects Division advises that to the best of its current knowledge no information whatsoever has been provided by the DSE Capital Projects Division, its servants or agents to any of the parties to the MOU pursuant to the MOU.

The DSE Capital Projects Division advises that to the best of its current knowledge no information whatsoever has been received by the DSE Capital Projects Division, its servants or agents to any of the parties to the MOU pursuant to the MOU.'

In a further letter dated 16 March 2010, DSE states that 'as of the current date, DSE has not received any law enforcement data from VICPOL.'

In the light of Victoria Police's response, DSE sought and received information from Victoria Police **before** the Desalination MOU came into existence. DSE's responses make it clear that its Division responsible for the desalination project – Capital Projects Division - had not, as at 23 December 2009, (the date of its written submission) received or provided any law enforcement data under the MOU and that DSE as a whole, as at 16 March 2010, had not received any law enforcement data from Victoria Police.

5.14 Information provided by AquaSure

In many respects AquaSure is in the same position as any other organisation or individual engaged in an entirely lawful undertaking that is the subject of community protest. It is contractually bound to deliver a project on time but unlawful protest activity may prevent it from doing so. Just like any other organisation or individual, it is entitled to seek the assistance of law enforcement agencies and can provide them with whatever relevant information it chooses provided it does so in accordance with the law.

AquaSure is bound, by virtue of provisions in the Desalination project documents that constitute a 'State Contract' within the meaning of s3 IPA, to comply with Victoria's information privacy legislation.²⁸ and must therefore must collect and handle personal information in relation to the Desalination project in accordance with the IPA. In particular, AquaSure 'must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.'²⁹

AquaSure's privacy policy indicates some of the personal information it captures.

Relevantly, it states that:

'We may collect personal information about you in a number of ways, including:

- if your image is captured as part of regular photography and videography carried (sic) at the Victorian Desalination Project site;
- from third parties, such as our contractors and stakeholders'³⁰

In addition, there is a real likelihood that AquaSure is covered by Victorian Charter obligations. The Charter applies to 'public authorities.' Under s4(3) of the Charter, a public authority includes 'an entity whose functions are or include functions of a public nature, when it is exercising those functions on behalf of the State or a public authority (whether under contract or otherwise.)' Some of the matters that may be taken into account in determining whether a function is of a public nature include:

- that the function is conferred on the entity by or under a statutory provision; and
- that the function is connected to or generally identified with functions of government³¹

28 See p 51 below

29 See IPP 1.2

30 See www.aquasure.com.au/contact/privacypolicy/index.htm

31 See s 4(a) and (b) of the Charter

The Water Act 1989 constitutes the statutory framework for the management of Victoria's water resources. The functions and powers it confers and the duties it imposes are essentially of a public nature and are undertaken by, or imposed on, public sector entities. Moreover, under an Instrument of Delegation dated 28 August 2009, Melbourne Water delegated a range of its functions to AquaSure under s 122B of the Water Act 1989 for the purposes of the Desalination project. The delegated functions are also of a public nature.

In these circumstances the prospect that, in relation to the Desalination project, AquaSure is a public authority for the purposes of the Charter is a real one. If so, the consequence is that any of AquaSure's decisions to disclose information to either Victoria Police or DSE must comply with the Charter.

AquaSure is a party to detailed arrangements under which it can seek and provide both assistance and information. The Desalination MOU's Standard Operating Procedures state that both DSE and AquaSure will 'be relied upon' to provide Victoria Police with intelligence.³² The Desalination MOU documentation can, therefore, be characterised as both establishing formal operational rules as between Victoria Police and AquaSure and the information linkages between AquaSure, Victoria Police and DSE under which AquaSure's role is to contribute to the information gathering necessary for Victoria Police to undertake its law enforcement functions in relation to the Desalination project. Given that one of the primary activities of Victoria Police is to gather information in pursuance of its law enforcement functions, the fact that it has entered into arrangements under which a private sector organisation's role in providing intelligence is explicitly stated, is an additional argument in favour of an interpretation that would categorise AquaSure as a public authority and subject to Charter obligations.

Under the CLEDS Standards, Victoria Police must only release law enforcement data to AquaSure if the release is authorised. Authorisation can be subject to a range of law enforcement data security requirements. Verification and audit mechanisms can be built-in.

Despite the fact that the PIMP Protocol was being developed as this review took place, AquaSure is not a party to the PIMP Protocol. Its focus is on DSE. There is therefore no document that directly and specifically covers the law enforcement data security obligations of AquaSure vis a vis Victoria Police in a manner that is consistent with CLEDS Standard 11. This gap in the MOU documentation must be remedied.

5.15 The consequences of recommending change

The DSE submission sets out in detail the consequences of Victoria Police failing to comply with the Desalination MOU and of any material amendment to it:

'[A]n 'Intervening Event' will occur if, during the design and construction phase of the Project, VICPOL fails to comply with the MOU in a material respect, or the MOU is revoked or materially amended...If an Intervening Event occurs, Project Co may be entitled to an extension to the Date for Commercial Acceptance and the Date for RT Finalisation (to the extent completion of the relevant design and construction activities by those dates is actually delayed due to the Intervening Event) and compensation for delay costs... The amount of any compensation for delay costs will be calculated in accordance with specified Change Compensation Principles.... Compensation will include increases in design and construction costs...directly attributable to the event, and any additional debt or equity

³² See clause 4.8, Standard Operating Procedures

financing costs that are required to be incurred (and are permitted under the Project Deed) to finance the delay.... Project Co may not vary a State Project Document without the consent of its banks. There are 34 local and international banks providing financial accommodation to Project Co'³³

I note this material. However, I do not believe that it is appropriate for me to modify or alter my conclusions in its light. There are a number of reasons for this.

First, key documents relevant to information sharing and information security, the PIMP and PIMP protocol, were developed long after the execution of the Desalination MOU. These documents materially affect the obligations of the parties. There is no suggestion that there has been any need to clear those documents with the project financiers.

Secondly, the substance of both the Victoria Police and DSE material that has been provided to me is that both are anxious to ensure that they share information in accordance with the law and in an appropriate and responsible manner. The fact that I have found that the MOUs they have adopted to give effect to their intent are inadequate provides an opportunity to put in place arrangements that reflect their intent. Moreover, given that I am assured by both Victoria Police and DSE that no personal information has been provided to AquaSure under the MOU, there is little likelihood that the risk management profile of the project would suffer any material change if the parties adopted the information sharing safeguards recommended later in this review.

The terms of reference for this review impose on me a responsibility to ensure that 'appropriate compliance, controls and arrangements are in place' under the MOUs. It is a matter for the parties to remedy the shortcomings I have highlighted in a manner that properly balances their obligations under the relevant MOU documentation.

5.16 Whole of Government Issues

Finally, I am advised that Victoria Police did not know, before it executed the Desalination MOU, that the consequences for the State of Victoria if it failed to observe the provisions of the MOU were potentially very serious.³⁴ The Desalination MOU itself is silent on these issues.

Victoria Police is not a party to the extensive and voluminous Desalination project documentation yet this documentation imposes significant risks on the State of Victoria if Victoria Police fails to comply with the Desalination MOU in a material respect. This liability exists despite the fact that the organisation whose noncompliance might crystallise the liability had no knowledge of those consequences. Moreover, in view of the comments I have made about the unsatisfactory nature of the MOU, there is significant potential for dispute about what might constitute material non-compliance.

Victoria Police cannot be regarded as just another generic supplier of goods or services to a major project. It is a public sector organisation that is required to undertake its law enforcement and other functions in the public interest. This might well, in certain circumstances, diverge from the private interests of a commercial entity such as AquaSure. In such circumstances, the public interest prevails. It is conceivable that Victoria Police may find itself in operational circumstances where the broader public interest justifiably requires that it not share some law enforcement data under the Desalination MOU. The desalination project documentation does not adequately reflect this reality.

³³ paras 23, 24, 25 and 27, pp3-4

³⁴ The question of whether the 'Intervening Event' mechanism in the project documentation is legally valid is beyond the scope of this review.

The open-ended risk consequences of this type of arrangement are, in my opinion, unacceptable. As Victoria Police did not know how the project documents dealt with non-compliance no steps were taken to control, manage and mitigate the noncompliance risks.

Clearly, the potential liability issues extend beyond Victoria Police to the State of Victoria and, as such, raise whole of Government risk and liability management issues. The Department of Treasury and Finance is the key central agency that has oversight of public/private partnerships in Victoria. It is therefore appropriate that these matters be examined by that Department.

Section 5 Findings

The Desalination MOU is problematic because:

- it contains the drafting errors and oversights outlined in this chapter
- as a consequence, it imposes obligations on Victoria Police that are inconsistent with legal and regulatory requirements
- it is legally unenforceable as against AquaSure, the consequence being that confidentiality and privacy obligations that should have been enforceable are not. This also means that information security obligations consistent with and supportive of the CLEDS Standards are not enforceable
- key regulatory obligations, in particular Charter obligations, are not mentioned
- governance and oversight mechanisms are inadequate
- the information sharing framework is not supported by corresponding compliance safeguards such as a privacy impact assessment or an information security threat and risk assessment and a human rights impact assessment
- when taken together with the broader Desalination project documentation, the State of Victoria is exposed to risks that have not been properly controlled or managed.

Section 5 Recommendations

Although there are many problems with the Major Project Development MOUs, Victoria Police cannot unilaterally amend them. Any changes require the consent of the other parties and, on the basis of DSE's submission, perhaps the consent of more than 30 financial institutions.

As the Desalination MOU does not compel Victoria Police to share any particular piece of information and the fact that Victoria Police is bound by the law not to share its law enforcement data in breach of those laws, no party to the MOU or any other relevant stakeholder could possibly assert that Victoria Police would breach any MOU obligation by strictly adhering to its information sharing legal obligations and by requiring the same of the other MOU parties.

In these circumstances it is appropriate that I make both general recommendations and more limited recommendations that apply only to the Desalination MOU and to the Mt Sugarloaf MOU to the extent that it continues to operate. In chapter 6, I have set out a recommended framework that Victoria Police should adopt whenever it contemplates sensitive information sharing arrangements. In my view, that framework should be applied to the Desalination MOU as soon as possible.

Recommendations about the Desalination MOU

Victoria Police should:

- notify each of the parties to the MOU that:
 - despite the express words used in clauses 5(k) and 8 of the MOU, any sharing by Victoria Police of its law enforcement data will be strictly in accordance with its legal obligations
 - it proposes to forthwith undertake an Information Sharing Risk Assessment on all law enforcement data flows likely to fall within the scope of the Desalination MOU, and
- invite each of the parties to the MOU to cooperate and assist in the ISRA process
- provide my office with the finalised ISRA
- promptly implement the ISRA recommendations when made
- report to CLEDS on progress by no later than 6 weeks after the publication of this review.

General MOU Recommendations

Victoria Police should for any future Major Project MOUs:

- ensure that they do not embody the drafting errors identified in this chapter
- restructure the MOU so that all of the provisions relating to governance and roles and responsibilities on the one hand and information sharing on the other are dealt with separately and in a consolidated form
- ensure that they properly reflect all relevant regulatory obligations
- excise the matters covered by clause 9 of the Desalination MOU and incorporate them in a separate, legally enforceable deed or agreement
- review all law enforcement data security provisions to ensure that they comply with the CLEDS Standards. In so far as these obligations should be passed on, incorporate these into a legally enforceable deed or agreement where that other party does not represent the Crown
- undertake the compliance and safeguard measures identified in chapter 6 before the MOU becomes operational
- review governance arrangements with a view to establishing mechanisms for oversight and dispute resolution and clear lines of accountability and authority for the release of law enforcement data.

The Department of Treasury and Finance should:

- review any linkages between Victorian Major Project documentation and other, cognate agreements or arrangements, whether legally enforceable in their own right or not, that might give rise to liabilities or other consequences under Major Project documentation, with a view to developing appropriate guidance and controls to manage those consequences.

6 Law Enforcement Data Sharing: The Way Forward

6.1 Developments in Information Sharing

Over the last decade there has been an increasing focus within government on the sharing of information between different agencies in order to improve the availability, quality and efficiency of public services and to enhance public safety.

This focus has been paralleled by the implementation of large networked information technology systems that have the capacity to collect, retrieve and communicate significant amounts of data. These developments have made sophisticated information sharing arrangements a practical possibility. The community has come to expect that public services will be responsive, coordinated, tailored to their needs and delivered efficiently. Appropriate information sharing underpins these expectations. However, individuals also expect that their personal information will be kept securely and will be protected from misuse.

In 2008, the UK Government commissioned a review of data sharing in the aftermath of repeated incidents of losses of sensitive personal data in both the public and private sectors (**Data Sharing review**). The Data Sharing review states that:

‘It is impossible to take a generic view of data sharing. Data sharing in and of itself is neither good nor bad. There are symmetrical risks associated with data sharing - in some circumstances it may cause harm to share data, but in other circumstances harm may be caused by a failure to share data. Data sharing needs to be examined in specific terms. Is the sharing of particular elements of personal information for a defined purpose in a precise fashion, likely to bring benefits that outweigh significantly any potential harm that might be associated with the sharing?’³⁵

Law enforcement raises difficult information sharing issues. Information is the lifeblood of policing. In its absence, law enforcement agencies cannot discharge their functions. The community understands and accepts that police collect information from a wide variety of sources in order to detect and prosecute crime and to safeguard public safety. What is less well understood is that policing and the techniques it employs have evolved beyond detection and prosecution to encompass new policing techniques such as crime prevention, community policing and partnership approaches to fighting and solving crime and protecting public safety. This has important implications for the way in which police collect and handle information, including personal information. To quote again from the Data Sharing review:

‘Personal information must often be shared to protect national security, help prevent crime, and identify the perpetrators of crime. Agencies, typically but not necessarily in the public sector, are increasingly sharing or pooling relevant information about people identified as presenting the risk of harming others. Public protection covers policing, crime prevention and detection, national security, and protecting vulnerable people considered to be at risk of harm from themselves or from others.

It is self-evident that personal data must be shared in order to achieve these purposes, but this begs questions about the scale and circumstances of sharing. Even with the best intentioned motives, sharing cannot be contemplated on an unlimited basis.’³⁶

³⁵ R Thomas and M Walport, Data Sharing Review Report, 2008, p i

³⁶ id

Information privacy law treats law enforcement as a special case. It exempts law enforcement agencies from needing to comply with some privacy obligations – in particular restrictions on information disclosure – that might otherwise impede their ability to discharge their functions effectively. However, privacy exemptions must be used responsibly and in the public interest otherwise police risk losing the community's confidence and trust in their information handling practices. If this occurs, police information sources are likely to diminish and/or become degraded.

The review terms of reference ask that I consider if Major Project MOUs embody appropriate compliance, controls and arrangements. For there to be proper compliance, controls and arrangements, strict legal compliance is necessary but not always sufficient. Arrangements for sharing Victoria Police law enforcement data need to be underpinned by policies, processes and procedures that support compliance and accountability and engender public confidence and trust.

In certain cases, particularly where highly sensitive operations are involved, it is inappropriate to require that the necessary information collection, use and disclosure be transparent. To do so risks revealing operational strategies and may impair police from being able to discharge their functions effectively. In those circumstances, accountability requires independent external scrutiny of the information sharing practices.

6.2 Responsible information sharing for law enforcement – appropriate checks and balances

Once again, the Data Sharing review contains a useful analysis of the broad issues:

‘There is no simple answer to the question of when it might be appropriate to share personal information for enforcement and protection purposes. In each case a proportionality test is the most appropriate consideration....We mean by this the application of objective judgement as to whether the benefits outweigh the risks, using what some might call the test of reasonableness or common sense. Proportionality involves making a considered and highquality decision based on the circumstances of the case, including the consequences of not sharing. Decisions must flow especially from the principles of relevance and necessity and the need to avoid an excessive approach.’

This approach amounts to the application of an objectively based risk management approach to information sharing decision-making. Added to that, in my opinion, is the need for the decision-making process to occur within a culture of regulatory compliance that respects community sensitivities associated with information sharing, that embodies accountability mechanisms and provides for external scrutiny so as to provide the necessary assurance that the key, competing public interests are properly balanced. There is a clear need to ensure that the free flow of law enforcement data is not limited to such an extent that legitimate law enforcement activities are impeded. Equally, the community is entitled to an assurance in each case that sensitive information, including but not limited to personal information, is handled appropriately.

6.3 Information Sharing Risk Assessment

These objectives are, in my view, best addressed by using a combination of approaches that draw upon existing and recognised good information and regulatory practice. The starting point is for Victoria Police to undertake a multidimensional risk assessment – an Information Sharing

Risk Assessment (**ISRA**) – as part of the information sharing decision-making process. The ISRA should consist of:

- a proportionality assessment
- a Privacy Impact Assessment
- an Information Security Threat and Risk Assessment
- a Human Rights Impact Assessment.

6.3.1 Proportionality Assessment

A proportionality assessment involves adopting a structured approach to information sharing having regard to questions such as:

- what is the purpose of the information sharing?
- what benefits are sought?
- can the purposes and benefits be achieved without, or with less, information being shared?
- what information is it necessary to share to achieve the purposes and realise the benefits?
- what harm will be prevented?
- with whom will the information be shared?
- what information will be shared?
- what are the controls and regulatory safeguards that apply?
- what information security measures are required?
- how will the information be stored?
- for how long will the information be kept?
- what methods will be used to communicate the information?
- for how long will the information be retained?
- can less information be shared or retained for shorter periods?
- what is the likely effect on individuals and society?
- what mechanisms are available to ensure that the recipient of shared information complies with information, security and other requirements?³⁷

It is important to understand that the outcomes of a proportionality assessment will vary significantly, depending on the proposed purpose and benefits. Where the purpose of information sharing is to fight serious crime, the assessment is likely to support broader information sharing but significantly higher information security controls than for low-level crimes. The point of the assessment is that there is no 'one size fits all' answer to information sharing issues.

³⁷ See generally UK Data Sharing Report p 14

6.3.2 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is the recognised means to assess the privacy impact of any new project or process. A PIA is defined as ‘an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated. A PIA considers the future consequences of a current or proposed action, and looks to prevent or minimise any negative impacts on privacy.’³⁸The Victorian Privacy Commissioner recommends their use so as ‘to give confidence to those taking action – and those who will be affected by it – that the impact on privacy has been considered, and any risks arising have been appropriately addressed.’³⁹

The processes recommended by the Victorian Privacy Commissioner in her publication ‘Privacy Impact Assessments: A guide for the Victorian Public Sector’ should form the cornerstone of any proposal for Victoria Police information sharing.

6.3.3 Threat and Risk Assessment

The recognised means by which information security issues are identified and addressed is in a Threat and Risk Assessment (TRA). A TRA is the process by which a security threat, whether deliberate or accidental, is assessed against the level of expectation that it may succeed and the potential damage that might occur. The result of this assessment is a risk rating. Where a risk rating is assessed as being unacceptable, control measures are recommended to reduce the likelihood of occurrence and any resulting damage. An Information Systems Threat and Risk Assessment (ISTRA) involves the application of the TRA process to an existing or proposed information technology system. The TRA process is well known and is used, in a variety of forms, by information security professionals for security assessment and threat mitigation.

Undertaking a TRA process is integral to Victoria Police understanding of the security implications of sharing information and to it developing the means by which security risks are managed and mitigated. It is also fundamental to ensuring that the recipients of shared law enforcement data adopt and implement the required information security measures. A TRA also underpins accountability mechanisms.

Good information management practice requires that audit trails and accountability mechanisms be built-in to provide objective assurance that security requirements imposed on information recipients are complied with.

6.3.4 Human Rights Impact Assessment

Finally, an essential part of an ISRA is a Human Rights Impact Assessment (HRIA). An HRIA is a relatively recent development following the enactment of the Charter. As with a PIA and TRA, it is designed to ensure that public authorities make decisions that conform with, and take proper account of, human right obligations.

Under the Charter, every new Victorian law must be accompanied by a statement of compliance to inform parliament whether or not the law meets the human rights standards established by the Charter. An HRIA serves the same purpose in respect of Victoria Police’s decisions to share personal information. It is an essential tool to demonstrate compliance with its obligations under s38 of the Charter.

³⁸ Privacy Impact Assessments: A guide for the Victorian Public Sector, edn 2-April 2009, p4

³⁹ id

The broad process used in an HRIA involves making an assessment of the following key issues:

- does the proposal/decision raise human rights issues?
- what is the scope of each of the human rights affected?
- does the proposal/decision limit, restrict or interfere with the scope of the rights?
- is the limit, restriction or interference justified under s7 of the Charter?
- if so, what steps must be taken to modify the proposal/decision to ensure compatibility?
- reassess the modified proposal/decision for compatibility.

6.3.5 When is an ISRA required?

Victoria Police is required to comply with all of parts of the regulatory framework whenever it makes a decision to share information. Thus, an ISRA process should inform and underpin all information sharing. That said, the risks vary, depending on the nature, scale and sensitivity of the information-sharing project. Some information sharing initiatives, for example, under Neighbourhood Watch programs, involve law enforcement data sharing with local community groups but the risks involved are usually comparatively minor. Some information sharing needs to occur in urgent, emergency circumstances. It is therefore important to ensure that risk management processes are applied so as to ensure that proper and essential information sharing to safeguard community safety is not unjustifiably impeded.

Good risk management involves getting the balance right.

In my view an ISRA approach should inform all Victoria Police information sharing decisions and practices. However, the formality of the process should be adapted to the circumstances, consistent with the recommendations made in paragraph 6.3.1 regarding the implementation of a proportionality test.

A formal ISRA process should be implemented and be finalised before the execution of any Victoria Police arrangement to release law enforcement data in relation to:

- any Victorian major project development
- any Victorian major event
- any information sharing arrangement in relation to which law enforcement data may be released to a commercial (i.e., for-profit) organisation, whether the release is made directly by Victoria Police or through any intermediary, and
- any other information sharing arrangement that constitutes a significant risk to Victoria Police.

Such an arrangement would require execution by the Chief Commissioner or a Deputy Commissioner after being certified in writing as being suitable by the Directors of Information Management, Security and Standards Division (IMSSD) and Legal Services Branch respectively.

For other, lower risk release arrangements, Victoria Police should prepare template documentation, checklists and educational and training material to assist decisionmakers. This material should be developed by IMSSD in conjunction with Legal Services Branch.

All such release arrangements should be executed by the relevant Assistant Commissioner subject to her or him being satisfied that the checklist requirements are certified in writing as having been undertaken by an appropriate officer.

6.3.6 External scrutiny of law enforcement data release arrangements

Many law enforcement data release arrangements do not involve the disclosure of Victoria Police's operational arrangements or other sensitive material. The risk that their public disclosure would compromise Victoria Police's law enforcement capabilities is, therefore, unlikely. Where the arrangements are so sensitive that their public disclosure is not in the public interest, the public is entitled to an independent assurance that the arrangements are appropriate and properly reflect regulatory requirements. The appropriate test is whether the arrangement would be exempt from disclosure under the law enforcement document exemption set out in s31 of the Freedom of Information Act 1982.

Given the functions conferred on CLEDS under the CLEDS Act, it is recommended that these oversight activities be undertaken by CLEDS and reported through the Minister for Police and Emergency Services on a regular basis.

6.4 An overarching information policy and management framework

One of the main contributing causes to Victoria Police entering into the unsatisfactory information sharing arrangements established under the Major Project Development MOUs was the absence of clear internal policies and guidance about how it should go about handling its law enforcement data. Its internal policies should have been aligned more closely with its regulatory obligations. They should have highlighted the need to undertake the various components of the ISRA process discussed in this chapter and provided linkages to the information and resources to assist police members to undertake those tasks.

The existence of these internal policy gaps combined with other work undertaken by CLEDS that also highlights law enforcement data security policy gaps within Victoria Police raises the issue of the need for Victoria Police to develop a more holistic approach to its information handling practices that covers the entire lifecycle of its information holdings from initial collection through to its ultimate disposal or destruction. Such an approach has been developed and implemented by the National Policing Improvement Agency in the UK with its recent publication of 'Guidance on the Management of Police Information'⁴⁰ which argues that effective policing depends on efficient information management. In my opinion Victoria Police urgently needs to develop a coherent and comprehensive information policy and management framework that covers the key areas of:

- collection
- recording
- evaluation, actioning and prioritisation
- sharing
- review, retention and disposal.

Effective management of Victoria Police law enforcement data needs clear and consistent policies and processes for collecting and handling information. The current approach used in the VPM is fragmented – the bulk of information policy is dealt with under the heading of 'Protective Security' but other important policy rules are scattered elsewhere in the VPM – and incomplete. Key policies appear to be in a constant state of rewriting, revision and consultation.

40 See www.acpo.police.uk/.../MoPI%202nd%20Ed%20Published%20Version.pdf

A comprehensive policy similar to the UK would be the most effective way forward for Victoria Police to address the information policy problems identified in this review.

Chapter 6 findings

The development of the Major Project Development MOUs was not informed by the use of relevant compliance tools and mechanisms. No Privacy Impact Assessment, Information Security Threat and Risk Assessment or Human Rights Impact Assessment was undertaken.

Chapter 6 recommendations

To ensure that Victoria Police information sharing arrangements are underpinned by appropriate compliance mechanisms, before any such arrangements are developed an Information Sharing Risk Assessment must be undertaken.

An ISRA consists of:

- a Proportionality test
- a Privacy Impact Assessment
- an Information Security Threat and Risk Assessment
- a Human Rights Impact Assessment.

The formality of the ISRA process will depend on the risks involved. At a minimum, a formal process is necessary for information sharing in relation to:

- any Victorian major project development
- any Victorian major event
- any information sharing arrangement in relation to which law enforcement data may be released to a commercial (i.e., for-profit) organisation, whether the release is made directly by Victoria Police or through an intermediary, and
- any other information sharing arrangement that constitutes a significant risk to Victoria Police.

Authority to execute such an arrangement should be restricted to the Chief Commissioner or a Deputy Commissioner after the arrangement is certified as being suitable by the Directors IMSSD and Legal Services Branch respectively.

All other arrangements should be informed by templates, checklists, precedent documents and education and training developed for the purpose by Victoria Police. Authority to execute the arrangement should be confined to the relevant Assistant Commissioner subject to her or him being satisfied that the checklist and documentary requirements are certified in writing as having been undertaken, such certification to be provided by an appropriate officer.

More broadly, Victoria Police senior management should give urgent consideration to the development of an overarching information policy and management framework to govern its information handling practices across the complete lifecycle of its information holdings. Such a framework would incorporate the processes and compliance tools recommended in this chapter but would extend to cover a range of other information issues.

APPENDIX 1 – The Regulatory Regime in Detail

1.1 Overview

There is no single source of law that regulates the collection, handling and sharing of information. That said, Victoria's regulatory framework for information sharing is the most comprehensive of all Australian jurisdictions. For example, only Victoria and the ACT have enacted human rights laws. A number of States have no information privacy laws. No jurisdiction has an equivalent to the CLEDS Act. In Victoria, these laws are supplemented by whole of government policies and, in Victoria Police's case, policy and procedural rules set out in the Victoria Police Manual and Chief Commissioner's Instructions. It follows that for Victoria Police information sharing, there is no single source of regulation that governs the process. Decision-makers need to apply a series of laws and regulatory requirements. This Appendix is a detailed outline of the key legislative and regulatory requirements that need to be navigated.

1.2 Information privacy

Victoria Police's ability to share personal information is primarily governed by the Information Privacy Act 2000 (IPA).⁴¹ The IPA establishes a regime for the protection of personal information in Victoria's public sector by requiring Victorian government agencies – such as Victoria Police, the Secretary and DSE – to collect and handle personal information in conformity with a set of ten information privacy principles (IPPs).

The objects of the IPA are set out in s5:

- a. to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;
- b. to promote awareness of responsible personal information handling practices in the public sector;
- c. to promote the responsible and transparent handling of personal information in the public sector.

The IPA does not apply to private sector organisations such as AquaSure except to the extent that they provide services under a 'State contract.' My analysis of the desalination project documentation is that it is a State contract. It follows that the IPA binds AquaSure in so far as it provides those services.

The IPA applies to personal information, which it defines as:

'information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion...'

Some categories of personal information constitute 'sensitive information' and receive a higher level of privacy protection. 'Sensitive information' includes information about an individual's political

⁴¹ The Health Records Act 2001 covers the privacy of health information in both the public and private sectors in Victoria. It establishes a comprehensive privacy regime to protect health information privacy. However, as there is little likelihood that the Major Project Development MOUs would involve the collection or handling of health information, a detailed analysis of health information privacy has not been included.

opinions, membership of a political association, racial or ethnic origins and criminal record.⁴²

IPP 1 prohibits a public sector organisation such as Victoria Police from collecting personal information unless the information is necessary for one or more of its functions or activities.⁴³

1.2.1 Use and disclosure – information sharing

The general rule under the IPA is that personal information collected for one purpose – the primary purpose of collection – can be used and disclosed for the same purpose. Thus if Victoria Police collects personal information to establish whether an individual has committed an offence, it can disclose (or share) that information for the same purpose. Under this principle, Victoria Police is permitted to disclose personal information about an offence to another organisation that has corresponding law enforcement functions, such as DSE. Provided DSE's functions and activities extend to the collection of information in respect of that type of offence, DSE is, under IPP 1.1, entitled to collect the personal information disclosed to it by Victoria Police and vice versa.

In certain circumstances, the IPA permits the use and disclosure of personal information beyond the primary purpose for which it was collected, i.e. for a secondary purpose. In the case of law enforcement agencies, both the IPA itself and the IPPs provide Victoria Police with a number of exemptions to the normal restrictions on use and disclosure of personal information. The most relevant exemptions IPP 2.1 (a) and (e) are s13 IPA. These provisions are set out in full below.

'2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless-

a. both of the following apply-

- i. the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
- ii. the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

.....

e. the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;

.....

g. the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency –

- i. the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
- ii. the enforcement of laws relating to the confiscation of the proceeds of crime;
- iii. the protection of the public revenue;
- iv. the prevention, detection, investigation or remedying of seriously improper conduct;

⁴² See the definition of 'sensitive information' in Schedule 1 of the IPA.

⁴³ See IPP 1.1

- v. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Section 13 of the IPA states

‘13. It is not necessary for a law enforcement agency to comply with IPP 1.3 to 1.5, 2.1, 6.1 to 6.8, 7.1 to 7.4, 9.1 or 10.1 if it believes on reasonable grounds that the non-compliance is necessary –

for the purposes of one or more of its, or any other law enforcement agency’s, law enforcement functions or activities; or

- f. for the enforcement of laws relating to the confiscation of the proceeds of crime; or
- g. in connection with the conduct of proceedings commenced, or about to be commenced, in any court or tribunal; or
- h. in the case of the police force of Victoria, for the purposes of its community policing functions.’

IPP2.1 provides Victoria Police with some latitude in disclosing personal information.

If it wished to provide photographs of suspected offenders to AquaSure, it would be unlikely to be able to show it could satisfy the second limb of the test in IPP2.1(a) – i.e., that the individual concerned would reasonably expect the disclosure of the information for the secondary purpose. However, provided it met the requirements of IPP2.1 (e) or (g), it would be able to do so.

Section 13 of the IPA exempts Victoria Police from complying with IPP2.1 if it can satisfy a two-part test. The first limb requires that it ‘believes on reasonable grounds that the non-compliance is necessary.’ The belief required to satisfy this requirement must not be fanciful, imaginary or contrived – it must be based on reason, not irrational, absurd or ridiculous beliefs.⁴⁴ The second limb requires the disclosure to be only for one of the purposes set out in sub-sections (a) – (d) of section 13 which set out a broad range of police functions.

The most relevant of these are ‘law enforcement functions and activities’ in section 13(a) and ‘community policing functions’ in section 13(d).

There is no definition of either term. Both are broad descriptions that are capable of evolving over time. Law enforcement functions involve:

- investigating crime and prosecuting offenders
- policing laws and regulations
- investigating accidents and deaths which occur other than by natural causes
- searching for missing persons
- assisting the public in emergencies
- preserving the peace
- supporting courts and tribunals in the administration of justice
- preventing crime.

The list is not exhaustive.

⁴⁴ See Department of Industrial Relations v Burchill (1991) 33 FCR 122 at 125,6

The meaning of community policing functions was considered in *Smith v Victoria Police* [2005] VCAT 654, a decision of the Victorian Civil and Administrative Tribunal.

The Tribunal stated that '[F]undamentally community policing requires an open and consultative relationship between the police and the rest of the community. The cultural traits in policing essential to meet this expectation include a willingness to be service oriented, a genuine commitment to community consultation, a predisposition to problem solving and sensitivity to community expectations.' The Tribunal noted that community policing is a 'strategy that allows the police and community residents to work closely together in new ways to solve problems of crime...creative new ways to address neighbourhood concerns beyond a narrow focus on individual crime incidents.'⁴⁵The Tribunal also referred to evidence given in the case about community policing where it was said that by 'putting information out into the community, the Police could get information in return.'⁴⁶

Clearly, a wide range of activities can legitimately fall within law enforcement and community policing functions and can thus give rise to an exemption under s13 of the IPA.

It is impossible in the abstract to determine the boundaries of the personal information Victoria Police is permitted to disclose. The legal framework requires that the question be considered in context and on a case-by case basis. For present purposes, however, it is sufficient to say that the IPA's restrictions on the use and disclosure of personal information for law enforcement or community policing functions, do not constitute a significant barrier to Victoria Police either disclosing personal information to DSE or AquaSure provided it complies with the relevant tests in the IPA.

1.3 The CLEDS Standards

Another component of the regulatory framework applicable to Victoria Police's information sharing is the CLEDS Standards. The CLEDS Standards establish standards and protocols for the security and integrity of Victoria Police's law enforcement data systems. 'Law enforcement data' is defined broadly in s3 of the CLEDS Act⁴⁷ to encompass any information obtained, held or received by Victoria Police for the purpose of one or more of its law enforcement functions. The definition of 'law enforcement data' includes, and extends beyond, personal information.

Under s 11(1) of the CLEDS Act, one of the Commissioner's functions is to 'establish appropriate standards and protocols for...the release of law enforcement data.' Under these provisions, in July 2007 the Commissioner published the CLEDS Standards.⁴⁷ The CLEDS Standards are derived from a range of international and national security benchmarks and bind Victoria Police. Since the development of the CLEDS Standards, a significant part of the work of the Commissioner has involved reviewing Victoria Police's compliance with the CLEDS Standards and in making recommendations about achieving compliance with them.

The CLEDS Standards are organised into fifteen chapters that establish a high-level information security framework that applies to Victoria Police's law enforcement data and law enforcement data systems. These are:

- Internal Security Organisation
- Roles and Responsibilities
- Access Control

⁴⁵ See paragraphs 76 and 77.

⁴⁶ See paragraph 74

⁴⁷ www.cleds.vic.gov.au/retrievemedia.asp?Media_ID=49898

- Release
- Physical Security
- Remote and Mobile Access
- Electronic Data Storage Devices
- Cryptographic controls
- Law Enforcement Data Systems Acquisition and Development
- Security Classified Law Enforcement Data
- Risk Management
- Security Incident Management
- Business Continuity Management
- Relationships between Victoria Police and Approved Third Parties
- Compliance.

The most relevant of the CLEDS Standards to the type of information sharing contemplated in the Major Project MOUs are those set out in Chapter 4 of the Standards, in particular Standard 11 and its associated protocols.

The key obligation in Standard 11 is that '(r)elease of law enforcement data must only occur if that disclosure is authorised.' The objective of the standard is 'to prevent the unauthorised release of law enforcement data by requiring that procedures are established that ensure that all disclosure is controlled and the recipients are informed of their obligations.'⁴⁸ Protocols 11.1 – 11.5 inclusive expand upon and explain the primary requirement set out in Standard 11. In essence, they require Victoria Police to develop policy, operating procedures and mechanisms that address matters such as:

- what constitutes unauthorised release
- the process for approving and authorising release
- roles and responsibilities for all forms of release
- recording the release of law enforcement data
- monitoring and auditing the release of law enforcement data to capture information about what data is released, who authorised release, to whom it was released etc.

Protocol 11.5 also refers to the extensive guidance about the release of law enforcement data in the Victoria Police manual (VPM). These are discussed in detail later in this chapter.

The CLEDS Standards recognise that although there is no one size fits all information security solution to the release of law enforcement data by Victoria Police, there must be policies, procedures and mechanisms in place that deal with the issue and which ensure that security is considered appropriately for all information released by Victoria Police.

⁴⁸ See Statement of Objective for Standard 11, CLEDS Standards

1.4 The Victorian Charter of Human Rights and Responsibilities

The Victorian Charter of Human Rights and Responsibilities (**the Charter**) establishes a regime to ensure that human rights are taken into account when Victorian laws, policies and procedures are developed, interpreted and applied. The Charter applies to public authorities.

1.4.1 Public authorities

The Charter applies to two broad categories of public authority – ‘core’ and functional public authorities. Under s4(1)(a) of the Charter, a public authority is ‘a public official within the meaning of the Public Administration Act 2004 (PAA).’ Under s4 of the PAA, a public official includes a public sector employee. This means that both the Secretary and DSE staff are covered. Under s4(1)(d) of the Charter, Victoria Police is expressly included as a public authority. It follows that both Victoria Police and the Secretary/DSE must observe the Charter’s human rights obligations.

Functional public authorities are covered by section 4(1)(c) of the Charter which provides that a public authority is ‘an entity whose functions are or include functions of a public nature, when it is exercising those functions on behalf of the State or a public authority (whether under contract or otherwise).’ Whether or not AquaSure falls within this definition is an open question that is not necessary to determine in this review.

1.4.2 Public authorities’ Charter obligations

Part 3 Division 4 of the Charter sets out the obligations of public authorities. The key requirement is s38(1) which states:

‘Subject to this section it is unlawful for a public authority to **act in a way** that is incompatible with a human right or, **in making a decision, to fail to give proper consideration to a relevant human right.**’ (my emphasis)

Under this requirement, both Victoria Police and DSE are required, in making and implementing information sharing arrangements, to give ‘proper consideration’ to relevant human rights. As they must not act in a way that is incompatible with human rights, decisions about sharing information must be informed by and take account of those obligations.

Part 2 of the Charter sets out the human rights that are protected. The most relevant are the right to privacy (s13), freedom of expression (s15) and the right to peaceful assembly and freedom of association (s16):

‘13. Privacy and reputation

A person has the right –

- a. not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and
- b. not to have his or her reputation unlawfully attacked.

15. Freedom of expression

1. Every person has the right to hold an opinion without interference.
2. Every person has the right to freedom of expression which includes the freedom to seek, receive and impart information and ideas of all kinds, whether within or outside Victoria and whether –

- a. orally; or
 - b. in writing; or
 - c. in print; or
 - d. by way of art; or
 - e. in another medium chosen by him or her.
3. Special duties and responsibilities are attached to the right of freedom of expression and the right may be subject to lawful restrictions reasonably necessary –
- a. to respect the rights and reputation of other persons; or
 - b. for the protection of national security, public order, public health or public morality.

16. Peaceful assembly and freedom of association

- 1. Every person has the right of peaceful assembly.
- 2. Every person has the right to freedom of association with others, including the right to form and join trade unions.’

Charter rights can be limited but only to the extent permitted by the Charter. Section 7 provides that a ‘human right may be subject under law only to such reasonable limits as can be demonstrably justified in a free and democratic society based on human dignity, equality and freedom and taking into account all relevant factors.’ Section 7(2) sets out a non-exhaustive list of the factors that may be taken into account. For example, ‘[f]reedom of assembly is not an absolute right and is confined to peaceful, non-violent assemblies (for example) riots would not be protected. However, civil disobedience manifested without force may be protected.’⁴⁹

Neither MOU mentions the Charter obligations. Neither establishes any mechanism under which s38 requirements are considered. It is clear to me that the collection sharing of personal information could affect an individual’s Charter rights. For example, if a person is deterred from engaging in lawful free speech or from peaceful protest against a government initiative because of a reasonable fear that their personal details might be recorded through overt or covert surveillance, kept and later used to their prejudice, Charter rights may be violated. Relevant prejudice could encompass failing to obtain a security clearance for employment purposes or to obtain a visa. It is difficult for anyone to obtain legal redress in either circumstance.

Similar issues, involving the collection and use of photographic surveillance data by police in the UK, were recently considered by the Court of Appeal in *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414. The case involved police photographing and questioning Mr Wood, the media coordinator of the Campaign against Arms Trade, as he left the annual general meeting of a corporation of which he was a shareholder and whose subsidiary had organised a trade fair for the arms industry. Mr Wood had never been arrested and had no previous criminal convictions. He asked a question at the meeting then left. The police took the photographs in order to identify possible offenders at the meeting or trade fair in case offences had been or would be committed. The police kept a database of such images for intelligence purposes although Mr Wood’s image was not added to the database. Mr Wood took legal action

⁴⁹ Human Rights Law Resource Manual, chapter 5,p35, www.hrlrc.org.au/resources/manual

under the European Convention of Human Rights (ECHR) on the basis that the conduct of police was in violation of a number of his human rights, including his right to privacy.

The Court decided that the taking of the photographs was a violation of the right to privacy. Although the taking of a photograph in a public place is not in itself sufficient to breach the right to privacy, the taking of photographs must be considered in context, which was that the police would keep and use them. Despite the fact that the police action was in pursuit of a legitimate policing aim – the prevention of crime and to maintain public order – its actions were not proportionate given that no explanation was given for the photographs being taken in circumstances that conveyed a reasonable impression that the images would be kept and used. The Court indicated that what might be considered proportionate in the case of an investigation of, for example, terrorism would not be considered proportionate in the case of low-level crime.

Although there are differences between the ECHR and the Victorian Charter, they are not such that Victorian public authorities can disregard the thrust of the Court's reasoning. In particular, the decision's interpretation of the right to privacy means that Victoria Police must act proportionately when collecting and retaining surveillance data whether the data is derived from Victoria Police officers or employees or from elsewhere.

I have not been provided with any material that shows that either Victoria Police or DSE have addressed their obligations under s38 of the Charter in the Major Project MOUs. This is an oversight that requires attention.

1.5 Victoria Police policy

Under s17(b) of the Police Regulation Act 1958, the Chief Commissioner is given the power to issue, amend and revoke instructions 'for the effective and efficient conduct of the force's operations.' Under this power, the Commissioner has issued

the Victoria Police Manual (VPM) which, amongst other things, contains detailed policy guidance about access, use and disclosure of Victoria Police information. The policy rules 'are mandatory and provide the minimum standards that employees must apply.'⁵⁰

During the period covered by this review there have been a number of versions of the VPM that have applied to the release of Victoria Police information. Relevantly, these were:

- before 6 October 2008 – VPM 208 applied to information release. This VPM was originally developed in 2003 (**the 2003 VPM**). The 2003 VPM applied when the MT Sugarloaf MOU was being developed and executed
- from 6 October 2008 to 22 February 2010 – Substantially revised provisions relating to information release came into effect (**the 2008 VPM**). The 2008 VPM applied when the Desalination MOU was being developed and executed
- from 22 February 2010 – a further substantially revised VPM was issued (**the 2010 VPM**). This is the version of the VPM that currently applies.

For the purposes of this review it is unnecessary to undertake an analysis of all of the differences between each version of the VPM. Only the most relevant provisions are discussed in detail.

1.5.1 The 2008 VPM

The key policy rule was that Victoria Police employees must not disclose any information arising

50 Victoria Police Manual – Policy Rules – Use and disclosure of information

out of their employment except where the release is authorised by legislation and/or policy.⁵¹ The policy omits any reference to the Charter.

VPM 208-1 set out the general policy requirements applicable to information disclosure. Some of the key policy requirements were:

- before releasing any law enforcement data, the security classification of documents must be taken into account
- the recipient of law enforcement data must be informed of their responsibilities regarding the security of the information and ‘must provide the same level of security classification and protection assigned by Victoria Police...The information must be managed securely and must not be release to any other individual or organisation’
- law enforcement data must not be released without a written request being received and recorded on a correspondence database. ‘All written requests must justify that the information sought is reasonably necessary for a particular purpose and what legislation facilitates release.’

The 2008 VPM expressly covered various specific categories of information release. These included:

- release of information to the media (VPM 208-2)
- release and use of LEAP and related information (VPM 208-3)
- release and use of police records and criminal histories (VPM 208-4)
- release of Victoria Police personal records (VPM 208-8) None of these specific policies apply directly to the circumstances of the Desalination MOU. Thus, the general policy obligations referred to above should have been complied with for any release of law enforcement data by Victoria Police under the MOU.

In addition to these law enforcement data release requirements, VPM 203 contained a requirement that all ‘MOUs or protocols must be registered on the Victoria Police MOU Central Register managed by Corporate Policy, Corporate Strategy and Performance Department.’⁵²

Additional requirements were that:

- if required to prepare a protocol or MOU, Corporate Policy must be consulted for details concerning requirements, content, consultation and approval
- MOUs and protocols must be approved by the relevant Regional Assistant Commissioner/Department Head or higher
- the original copy of an MOU or protocol must be lodged with Corporate Policy.

1.5.2 The 2010 VPM

The general thrust of the VPM policy framework is that information must not be disclosed without proper authority. ‘Even if legislation or policy provides the authority to release Victoria Police information, employees must only disclose the information if:

- the information is within their area of responsibility
- the recipient has a legitimate business need for the information’⁵³

⁵¹ VPM 208-1

⁵² Paragraph 5.2.3, VPM 203, 6 October 2008

⁵³ id

However, the 2010 VPM omits key material that was included in the 2008 VPM.

Importantly, the requirement that all MOUs be registered on a central register was omitted as was the requirement to consult with Corporate Policy when developing an MOU. There are no references to the security classification of documents. There is no counterpart to the requirement for a written request being needed before information may be released. There is no requirement that the recipient of information must protect it in the same way as Victoria Police.

The following table sets out the policy when information is requested from government departments or statutory bodies.⁵⁴

Source of type of request	Conditions or procedures for release
Requests from Government departments or statutory bodies	Information may be released: <ul style="list-style-type: none"> • when there is specific legislation that supports or requires release • when there is a Memorandum of Understanding or other formal agreement in place which supports information release • if personal or health information, when release is in line with the <i>Information Privacy Act or Health Records Act</i> • For further guidance, refer to the Information sharing guidelines (under development by Privacy Unit)

Thus, Victoria Police policy provides a policy basis for approving the release of information under an MOU to government bodies. However, it does not specifically cover the release of information to private sector organisations. Presumably, such release is covered under the general rules – i.e., a legitimate business need must be established – referred to above, but this is not clear.

1.6 CLEDS Review of Access Control and Release of Law Enforcement Data – June 2008

In June 2008 CLEDS completed a review of Victoria Police’s compliance with the CLEDS Standards on Access Control and Release of law enforcement data. The most relevant sections of that review relate to CLEDS Standard 11 which requires that the release of law enforcement data must only occur if that disclosure is authorised. Standard 11 aims to prevent the unauthorised release of law enforcement data by requiring that procedures be established to ensure that all disclosure is controlled and the recipients are informed of their responsibilities.

Standard 11 includes five protocols. These cover matters such as:

- a requirement that law enforcement data must not be released unless authorised by law and/or Victoria Police policy (Protocol 11.1)
- policies and operating procedures must be developed that, at a minimum, address:
 - the types of release that exist
 - the forms of release

- what constitutes unauthorised release
- the process for approving and authorising release
- roles and responsibilities for all forms of release
- the need to record and maintain a formal record of the receipt of released law enforcement data (Protocol 11.2)
- policies, procedures and mechanisms to regularly monitor and audit the release of law enforcement data (Protocol 11.3)
- the development of guidance about appropriate and inappropriate release (Protocol 11.4)
- where release is not covered by an agreement, the development of controls and processes that ensure release is authorised and the recipient is aware of their responsibilities (Protocol 11.5).

The June 2008 CLEDS review highlighted substantial areas of non-compliance with these requirements and made a range of recommendations for improvement. These included addressing the need to:

- develop policies that specifically comply with the requirements of Protocols 11.2 and 11.3
- communicate release policies and procedures to all Victoria Police employees.

The recommendations were accepted by Victoria Police, which noted that a number of the shortcomings were being dealt with in a review of information release policies that had been initiated in April 2008.

In February 2010 CLEDS undertook an implementation review of the June 2008 recommendations. The implementation review found that, although some improvements had been made, Victoria Police release policy still did not adequately deal with Protocols 11.2 and 11.3. In addition, an organisation-wide education program that addressed the processes for information release and necessary monitoring activities had not been implemented.

1.7 Other regulatory requirements

For the sake of completeness, public sector organisations are sometimes bound by legislative secrecy provisions that prohibit staff and contractors from communicating information they have gained during the course of their duties. The most well known of these are in relation to the tax affairs of individuals and in relation to healthcare under s130 of the Health Insurance Act 1973 (Cth). In the case of Victoria Police, section 127A of the Police Regulation Act 1958 prohibits, in certain circumstances, Victoria Police personnel from disclosing information obtained in performing their functions. I am satisfied that this provision does not prevent appropriate information sharing by Victoria Police under properly constituted MOU or like arrangements.

Conversely, there are occasions when legislation specifically authorises particular categories of information collection, use and disclosure. Under s6 of the IPA, such legislation prevails over the provisions of the IPA to the extent of any inconsistency. There are no such legislative provisions directly relevant to this review.

Attachment 1 – Reference from Minister for Police and Emergency Services



Minister for Police & Emergency Services

121 Exhibition Street
Melbourne Victoria 3000
GPO Box 4356
Melbourne Victoria 3001
Telephone: (03) 8684 0900
Facsimile: (03) 8684 0910
DX 210077

8 December 2009

Mr David Watts
Commissioner for Law Enforcement Data Security
Victoria Police Centre
637 Flinders Street
MELBOURNE VIC 3206

Dear Commissioner

MAJOR PROJECT DELIVERY - MEMORANDUM OF UNDERSTANDINGS (MOUs)

I write to you in respect of the Victoria Police Major Project Delivery MOUs. I note that Marisa De Cicco of the Department of Justice spoke to you yesterday about this issue. As you will aware, Victoria Police has entered into MOUs with respect to how community safety, and critical project infrastructure project delivery, can be assured.

I understand from my Department that these MOUs have been signed by Victoria Police on advice from legal counsel, and do take into account appropriate state laws, guidelines and standards.

As Marisa De Cicco discussed with you, I have resolved that this matter should be reviewed more comprehensively and therefore I would ask that you undertake a review of such MOUs, as envisaged under s11(1)(c) of the *Commissioner for Law Enforcement Data Security Act 2005*.

As part of this review, I would ask that you examine such MOUs to ensure that these documents:

- (a) appropriately reflect the your standards for law enforcement data security and integrity; and
- (b) assure appropriate compliance, controls and arrangements are in place.

I would ask that you confer with whichever agency, regulator or other party that you believe appropriate in the conduct of this review.

I would be happy to discuss this matter further with you as required. Otherwise, I would ask you to liaise with Ms Marisa De Cicco from the Department of Justice.

Yours sincerely

Bob Cameron MP
Minister for Police & Emergency Services

cc. Mr Simon Overland APM, Chief Commissioner



