

**IN THE MATTER OF THE ROYAL COMMISSION
INTO FAMILY VIOLENCE**

ATTACHMENT DW-4 TO STATEMENT OF DAVID WATTS

Date of document: 31 July 2015
Filed on behalf of: the Applicant
Prepared by:
Victorian Government Solicitor's Office
Level 33
80 Collins Street
Melbourne VIC 3000



This is the attachment marked '**DW-4**' produced and shown to **DAVID WATTS** at the time of signing his Statement on 31 July 2015.

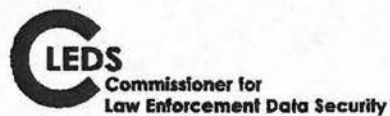
Before me:



An Australian legal practitioner
within the meaning of the
Legal Profession Uniform Law (Victoria)

COMMISSIONER FOR LAW ENFORCEMENT DATA SECURITY Annual Report 2013-2014





The Hon. Kim Wells, MP
Minister for Police & Emergency Services
GPO Box 4356QQ
MELBOURNE 3001

Dear Minister

I am pleased to present you with the Annual Report for 2013-14 in accordance with Part 3 section 17 (1) of the *Commissioner for Law Enforcement Data Security Act 2005*, for presentation to Parliament.

Yours sincerely

A handwritten signature in black ink, appearing to read 'David Watts'.

David Watts
Commissioner for Law Enforcement Data Security
8 August 2014

TABLE OF CONTENTS

Commissioner's overview	3
The role of the Commissioner for Law Enforcement Data Security	6
The Commissioner's key objective	7
Reflections on the past 8 years	9
Transition to the Commissioner for Privacy and Data Protection	12
The year in review	14
Strategic projects	17
Information security breach reporting	20
About the Office of the Commissioner for Law Enforcement Data Security	25
Compliance and accountability	29
Finances	31
Appendix 1: Disclosure Index	32
Appendix 2: Attestation on compliance with the Australian/New Zealand Risk Management Standard	34

COMMISSIONER'S OVERVIEW

During 2013/14 Victoria Police has continued to improve the security of its law enforcement data and law enforcement data systems. In the past, one of main our criticisms of Victoria Police has been its very slow progress in implementing our recommendations. This year that has not been the case: it implemented 32 of our outstanding recommendations and, as at 30 June, it had implemented almost 80% of our active recommendations. This significant achievement deserves acknowledgement.

It is no accident that these positive and encouraging outcomes have coincided with Victoria Police finally adopting each of the recommendations we made in our 2009 review of its information governance. Nor is it a coincidence that during the year Victoria Police finally cemented the structures and processes of its internal security organisation that were required to underpin the 2009 recommendations. The foundation of good security is good governance.

As we noted in last years' annual report, we expect the rate at which Victoria Police implements the remainder of our outstanding recommendations will slow over the forthcoming year as compliance with many will involve expenditure on improved or new ICT infrastructure. In many cases, this will involve Victoria Police in making difficult decisions about spending money to support and improve the security of out-dated information systems pending their replacement.

From an information management and security perspective, the most significant current challenge for Victoria Police involves the replacement of ageing and over-stretched law enforcement data systems. Core systems such as the Law Enforcement Assistance Program (LEAP) and the Interpose intelligence database are out-dated and stretched to capacity. They also lack the range of functionality needed to support a large, integrated and modern law enforcement capability.

Victoria Police's Blueprint for 2012-2015 identifies the need for it to develop business systems and processes to support effective police service delivery, one of the key priorities being the development of the PIPP project 'as a core driver of reform to information policy, practice and the processes used by operational police.'

The PIPP project has two streams. The first involves sustaining LEAP and Interpose for the next five years. The second, the Transform project, involves Victoria Police in developing an information system to support its future law enforcement activities as part of a long-term information strategy.

The Victoria Police Blue Paper published in May 2014 states that:

Over the decade to 2025, Victoria Police will need to become a more connected, intelligence-led and evidence-based organisation, that works closely with communities and partners to prevent, and reduce the harm done from crime, disorder and other public safety hazards. It will be challenged to do better with relatively less...

Achievement of Victoria Police's goals will require three related strategic directions:

- *Better matching of resources to demand by rethinking the traditional model*
- *Improving capability through workforce reform and technology*
- *Collaborating more closely through partnerships¹*

Echoing more general findings regarding Victoria Police's fragmented approach to strategic planning made in the Rush Inquiry, the Blue Paper notes that Victoria Police lacks 'a comprehensive, long-term strategy to guide the governance and business use of, and appropriate investment in, its information.'²

The Blue Paper's strategic vision cannot be achieved unless this strategy is put in place. Our observation is that the PIPP Transform project is hampered by a lack of strategic focus, the consequence of which is a lack of clarity about what systems and processes Victoria Police needs to develop and deploy to ensure that its next generation of law enforcement data systems are suitable to support evolving community expectations of policing and make more effective use of law enforcement data. The key task for Victoria Police is to translate the Blue Paper's strategic directions into concrete plans and projects.

Good information security consists of three main elements:

- Confidentiality
- Integrity
- Availability

Commonly, confidentiality (i.e., protecting information from unauthorised disclosure) is privileged over the other two, equally important, elements. The tragic case of the murder of Luke Batty in February 2014 serves to highlight the consequences of approaching security too narrowly.

¹ Victoria Police Blue Paper: A Vision for Victoria Police in 2025, p 23

² id, p 18

Luke was killed by his father at a time when there were a number of outstanding arrest warrants against him. It appears that police officers who visited the father shortly before he killed Luke were unaware of the existence of the outstanding warrants, allegedly due to shortcomings in information sharing processes. If they had been aware of the outstanding warrants, it is likely that the father would have been in custody at the time of the murder. Although it is inappropriate to comment further on this matter whilst a coronial investigation is underway, it is important to understand that if the facts are as stated, this tragedy highlights security shortfalls: relevant information was not accessible to operational police when it should have been.

In the meantime, the broader information security environment for Victoria Police has become more complex. Consistent with the increasing risk of cyber security attacks across the community, we have become aware of several that have targeted Victoria Police over the last year. We are currently assessing Victoria Police's response to and remediation of these attacks.

We have also, along with a number of others responsible for operational security, identified the growing risk of security breaches attributable to lapses in personnel security, in particular the risk of insider intrusion. The events surrounding the formation of Taskforce Keel, where it is alleged that a police member provided Victoria Police law enforcement data to members of an outlaw motorcycle gang, emphasise the need for ongoing personnel security risk assessments and more effective ICT audit and checking mechanisms.

Finally, the *Privacy and Data Protection Bill 2014* was introduced into parliament in June 2014. The Bill, when enacted, will see the replacement of the office of the Commissioner for Law Enforcement Data Security with a new Commissioner for Privacy and Data Protection who will assume the current role and functions undertaken by CLEDS but who will also have responsibility for establishing protective data security standards, and for monitoring compliance with them, across the whole of the Victorian public sector. The Bill maintains the current CLEDS Standards and the existing legislative focus on law enforcement data security. In anticipation of the Bill, CLEDS has undertaken much of the preliminary work needed to ensure that the new Commissioner for Privacy and Data Security can begin work as soon as the Bill comes into effect, which is expected in the coming months. This has included developing a draft of the protective data security standards together with related supporting material.

Although I incorrectly predicted that the CLEDS 2012/2013 Annual Report would be our last, it is highly likely that this will be the final CLEDS Annual Report. Again, I acknowledge the support for our work across government and thank all of the CLEDS team for the outstanding work they have undertaken. I wish to thank, in particular, Laurie Bebbington, the first Commissioner for Law Enforcement Data Security, whose work to establish the office and develop the CLEDS Standards has served as an enduring tribute to her foresight and vision.

THE ROLE OF THE COMMISSIONER FOR LAW ENFORCEMENT DATA SECURITY

The *Commissioner for Law Enforcement Data Security Act 2005* was passed by the Parliament of Victoria in November 2005 to promote the use by Victoria Police of appropriate and secure law enforcement data management practices. The Act seeks to achieve this objective by creating the office of the Commissioner for Law Enforcement Data Security and establishing a regime for monitoring law enforcement data security management practices.

The Act provides for the Commissioner to perform several functions. These functions are to:

- establish standards for the security and integrity of law enforcement data systems
- establish standards and protocols for access to, and the release of, law enforcement data
- monitor and audit compliance with the standards and protocols established under the Act
- consult with the Chief Commissioner of Police on the establishment of standards and protocols for law enforcement data security
- refer findings of monitoring activities to the appropriate bodies for further action
- undertake reviews concerning any matter relating to law enforcement data security requested by the Minister for Police and Emergency Services or the Chief Commissioner of Police

The Commissioner provides an annual report to the Minister for Police and Emergency Services, who is required to lay it before the Victorian Parliament.

THE COMMISSIONER'S KEY OBJECTIVE

As an independent statutory body the Commissioner's role focuses the attention of Victoria Police on compliance with high standards of law enforcement data security. This should in turn enhance community confidence in Victoria Police's ability to securely manage confidential information.

The Commissioner has defined the primary objective of the activity of the Office of the Commissioner for Law Enforcement Data Security, as follows -

All stakeholders have reasonable assurance that Victoria Police data is managed securely and accessed appropriately.

2013-2014 PRIORITIES

The Commissioner adopted the following key priorities for the 2013-2014 year:

- undertake further reviews of Victoria Police compliance with the Standards for Law Enforcement Data Security as required
- monitor Victoria Police implementation of recommendations made in compliance reviews
- examine Victoria Police information systems for overall compliance with CLEDS standards
- investigate and assess issues impacting on Victoria Police's approach to information management and security
- review the *Standards for Victoria Police Law Enforcement Data Security* for accuracy and currency
- prepare for the amalgamation of the Commissioner for Law Enforcement Data Security with the Office of the Victorian Privacy Commissioner.

VALUES

Five key values guide the work of the Office of the Commissioner for Law Enforcement Data Security

Independence

While working cooperatively with Victoria Police, CLEDS provides independent advice on and oversight of law enforcement data security

Credibility

CLEDS' work is based on sound evidence, undertaken with rigour and always able to stand close scrutiny for its expertise, objectivity and value

Integrity

CLEDS' conduct is focussed on the goal of improving the security of law enforcement data, providing impartial advice regardless of consequence

Respect

CLEDS respects

- the Victorian community's expectation that their information is secure
- the values of Victoria Police and its intent to provide the highest level of security for the data it holds

Leadership

CLEDS provides the expert knowledge and advice to assist in meeting the challenges of securing information in an evolving technological environment

REFLECTIONS ON THE PAST 8 YEARS

At the time of writing, the Privacy and Data Protection Bill 2014 is before Parliament awaiting enactment. The Bill, amongst other things, abolishes both CLEDS and the Privacy Commissioner and replaces both with a Commissioner for Privacy and Data Protection.

The establishment of CLEDS was in some ways an experiment, an innovation. While police oversight bodies exist in other jurisdictions, CLEDS is the only body established specifically to regulate data security and management within a policing environment. The establishment of CLEDS represented recognition that good information management sits at the heart of good contemporary policing.

CLEDS activities since 2006 have progressed through a series of phases.

Initially, our central task was to establish the *Standards for Victoria Police Law Enforcement Data Security*. Considerable effort was made to distill then national and international benchmark standards on information security into a single, easily comprehensible set of standards tailored for a law enforcement environment. The Standards published in 2007 have proved durable; a review of them during 2014 resulted in only minor updating.

The second phase of CLEDS' work was to review Victoria Police's compliance with the Standards. Overall the compliance reviews demonstrated poor security practices across Victoria Police. These compliance reviews resulted in a large number of recommendations as to how Victoria Police should act in order to be compliant with the Standards.

The third phase of our work was, naturally, a rolling series of reviews to assess Victoria Police's implementation of those recommendations. As these reviews reached their end, and in light of Victoria Police's then unsatisfactory level of implementation of recommendations, we established an Implementation Working Group to continue monitoring compliance, to establish the reasons why Victoria Police had not implemented recommendations made and to move the implementation process forward.

On completion of the formal implementation reviews, CLEDS had gathered enough evidence to understand that there were underlying issues impeding Victoria Police's progress in complying with the Standards. As a result we conducted a watershed review of information governance within Victoria Police, published in 2009.

The final phase of our work, since 2009, has been to address and further investigate the underlying causes which act as impediments to further progress and emerging issues for law enforcement data security.

CLEDS Achievements

- Through the series of implementation reviews carried out and the subsequent work of the Implementation Working Group, Victoria Police has now fully implemented 77% of active recommendations made by CLEDS and partially implemented a further 12%. Most of this improvement has occurred over the past two years, but nonetheless is a major achievement. This level of implementation is the result of a great effort on the part of Victoria Police, for which it should be commended.
- At 30 June 2014, all agencies external to Victoria Police, but with direct access to Victoria Police law enforcement data systems (Approved Third Parties) are bound by CLEDS compliant access agreements. This situation should be compared with that in 2008, when CLEDS conducted a review of Victoria Police compliance with those standards regulating relationships with Approved Third Parties. What was found at that time was totally unsatisfactory: there was a lack of governance around relationships with these external agencies, no central control – in fact at the time no single person in Victoria Police could provide a complete list of Approved Third Parties – and in some cases a lack of any agreement, let alone one that was CLEDS compliant, to govern the agency's access to Victoria Police data and data systems. Most of the CLEDS Standards include a clause that the security obligations they impose on Victoria Police must be passed on to Approved Third Parties by means of an access agreement. Getting Victoria Police 'across the line' with regard to CLEDS compliant agreements with Approved Third Parties has therefore been an achievement which has contributed significantly to Victoria Police's overall compliance with the CLEDS Standards.
- CLEDS review of Victoria Police information governance, carried out in 2009, made two recommendations which called for a profound shift in Victoria Police's approach to its information management and security.

First, CLEDS recommended that responsibility for information management policy and the assessment of business requirements be separated from that for IT service delivery – IT being just the enabler of policy. This recommendation resulted in the creation within Victoria Police of the Information Management, Security and Standards Division (IMSSD), which has played a pivotal role in promoting good information management practices. The importance of the establishment of this 'go to' division and the work it has undertaken since establishment should be commended.

Secondly, CLEDS recommended that Victoria Police develop and implement a cultural change strategy. Cultural change is always difficult, especially in a command and control organisation like Victoria Police. Notwithstanding the challenge posed, and after a false start, Victoria Police developed a comprehensive and sophisticated, multi-year cultural change strategy. Implementation of the strategy is now in its second year. Findings from the CLEDS survey carried out in 2014 suggest that the initial phase of the strategy – raising awareness of information management and security – is having a positive effect.

- In 2012 CLEDS conducted the first wave of a longitudinal survey of the attitudes and behaviours of members of Victoria Police with regard to information management and security. The survey is intended to be conducted in three 'waves' – 2012, 2014 and 2016. To the best of our knowledge, the survey is the only one of its kind to be conducted in a law enforcement environment, its importance being such that the survey process, methodology and high level findings of wave 1 were the subject of a presentation at the annual meeting of the Australian and New Zealand Society of Criminology in Auckland late in 2012.

The CLEDS survey is important also in that it is designed to track progress against Victoria Police's cultural change strategy. While informing CLEDS, the survey also provides Victoria Police with a useful tool to gauge its own progress and identify areas where further policy work or improved practices are required.

- Finally, the quantity and quality of CLEDS output should be noted. Over the past 8 years CLEDS has produced 40 individual reports of reviews. That is a significant body of work for a relatively small organisation.

Some of these reports are the result of many months of intense work and can be considered to be of major importance to Victoria and other law enforcement jurisdictions. The *Review of Victoria Police Major Project Development MOUs*, *Review of Data Flows between Victoria Police and CrimTrac* and *Social Media and Law Enforcement* stand out in this respect.

TRANSITION TO THE COMMISSIONER FOR PRIVACY AND DATA PROTECTION

The Victorian Attorney General announced in December 2012 that the offices of the Victorian Privacy Commissioner and the Commissioner for Law Enforcement Data Security would be amalgamated to form a new entity, the Commissioner for Privacy and Data Protection. Since that announcement, CLEDS has been leading the transition to the new entity.

Through the 2013-14 reporting period the Commissioner for Law Enforcement Data Security, Mr David Watts, has also acted as Privacy Commissioner, providing joint leadership across the two agencies. CLEDS also seconded 1.6 EFT of its own staff to the Office of the Victorian Privacy Commissioner and appointed a Manager Transition and Integration, who works between the two agencies.

Much of CLEDS time and a considerable part of its budget has been spent over the period on transition activities and issues of immediate concern to the new entity that will be formed at the time of full integration. This has involved all members of CLEDS staff in a variety of activities, most notably the following.

Administration

CLEDS' Manager Transition and Integration and Manager Strategic Projects spent considerable time preparing both agencies for administrative wind down and positioning for administrative amalgamation, particularly with regard to HR, finances and records management.

A major activity has been locating, securing and organising the fit out of new premises large enough to accommodate the combined staff of the two agencies.

ICT

We undertook evaluation of and preparation for the information management and ICT needs of the new entity. This included the engagement of specialist providers to implement a new ICT environment for the office of the Commissioner for Privacy and Data Protection. Significant planning was also undertaken to migrate critical information from legacy systems within the Office of the Victorian Privacy Commissioner and CLEDS to a new set of applications and ICT infrastructure that will support both current needs and expected future demands.

We continued efforts to provide connectivity between the Office of the Victorian Privacy Commissioner and the Department of Justice finance and HR systems and intranet in preparation for integration with the new entity. Such connectivity is essential for the efficient administration of the office. No progress was made throughout the reporting period, due principally to the lack of program management by CENITEX. We understand that other agencies are in the same position regarding connectivity.

Victorian Protective Data Security Standards

One of the key functions of the Commissioner for Privacy and Data Protection, created through the amalgamation of the Commissioner for Law Enforcement Data Security and the Office of the Victorian Privacy Commissioner, will be the development of a Victorian Protective Data Security Framework, which will apply across the Victorian public sector. At the heart of this framework will sit the Victorian Protective Data Security Standards.

CLEDS has had two dedicated staff members (20% of its total staff resources) working on the development of these Whole of Victorian Government standards and guidelines throughout the current reporting period.

The aims and objectives to which we have been working can be summarised as:

- develop standards and guidelines tailored to Victorian government needs that are flexible and adaptable yet durable, robust and written in an easily accessible manner
- reflect contemporary information security standards, locally and internationally, and, in particular, to harmonise with the Commonwealth's Protective Security Policy Framework
- support Victorian public sector service delivery functions
- facilitate appropriate information sharing – the right information to the right people at the right time – fostering a culture where security is seen as an enabler not an impediment
- promote the concept of Security by Design
- underpin cultural change with regard to information security and management within the Victorian public sector
- promote a risk-based approach to the implementation of practical information security measures, so as to support and not inhibit government business and service delivery.

The Victorian Protective Data Security Standards are in the process of development and will be subject to a robust consultation phase within the public sector following enactment of enabling legislation.

THE YEAR IN REVIEW

CLEDS carried out none of its standard compliance, implementation or IT systems reviews this year. Instead we intensified our activities around the follow up on the implementation of recommendations through the work of the Implementation Working Group (IWG). All of Victoria Police's major law enforcement data systems have been reviewed and the resulting recommendations are also subject to IWG monitoring. Further information about the activities of the IWG appears later in this report.

Site Inspections

CLEDS carried out two site inspections during the year. One was of a large regional police facility; the other of an operational unit located in the Melbourne CBD.

Our site inspection program is designed to assess information security process and procedures 'on the ground' in operational policing environments. We give approximately four weeks notice of the inspection and carry out pre-inspection briefings and post-inspection debriefings.

The scope of these inspections has expanded over time. The objective of the initial inspections was to provide a learning opportunity to Victoria Police as to the conduct and benefits of such 'on the ground' inspections. This year, the inspections have evolved, based on the assumption that the lessons learnt by Victoria Police from previous inspections would have been disseminated throughout police facilities.

This year's site inspection reports differentiated in their findings between security improvements that could be managed at local level and those that could only be addressed at senior command level.

At local level, incomplete or out of date information security documentation continues to be a common finding. That, coupled with the lack of a central point of contact for information security matters at each police facility, continues to hinder effective information security improvement.

Some issues affecting all sites inspected can only be addressed by senior command. First, unencrypted transmission across the Statewide Mobile Radio network is widely regarded as a safety concern at operational police level. Secondly, the high level of administrative access to IT service providers requires attention in order to ensure that only authorised people have access to law enforcement data. Finally, data stored on portable storage devices continues to pose a significant risk of unauthorised access due to the lack of effective software tools for the removal of data.

At both sites inspected, CLEDS observed an improved information security culture. This improved culture is effective in reinforcing information security policy.

Consultations and Provision of Expert Advice

This year saw a significant increase in requests to CLEDS for advice, both from Victoria Police and other public sector agencies.

A trend within Victoria Police has been recognition of the need to assess the security classification of law enforcement data in the light of the new Australian Government security classification and protective handling schema. This has resulted in increased consultation with CLEDS, notably with regard to information to be shared with other jurisdictions.

Other than consultations with Victoria Police, the Department of State Development, Business and Innovation (DSDBI) sought the Commissioner's advice on the development of a cyber security strategy (consultations are on-going).

The Commissioner also appeared before the Public Accounts and Estimates Committee to provide advice on department and agency responses to the Victorian Auditor General's review of information security across the Victorian public sector.

Implementation of CLEDS Recommendations

Due to slowness in implementing the CLEDS recommendations, a joint Victoria Police/ CLEDS Implementation Working Group (IWG) was established early in 2012. The following table shows the progress made by Victoria Police in implementing CLEDS recommendations.

	Pre IWG	30/6/12	30/6/13	30/6/14
Implemented	41	71	132	164
Not Fully Implemented	110	54	41	25
Not Implemented	62	56	41	23
Withdrawn	0	32	39	41
Total Recommendations	213	213	253	253
Total Outstanding	172	110	82	48
% of active recommendations implemented	19%	39%	62%	77%

The table shows that the considerable improvement in the implementation of recommendations noted in the 2012-13 reporting period has been substantially maintained. It should also be noted that at 30 June 2014 there was a further small number of recommendations close to full implementation.

As noted in 2013, the recommendations that remain outstanding are principally IT/ systems specific and include recommendations that require business cases to secure funding and/or are beyond Victoria Police's current resources. While further improvement is expected in 2014-15, the nature of the outstanding recommendations suggests that implementation will slow down.

STRATEGIC PROJECTS

Review of CLEDS Standards

The *Standards for Victoria Police Law Enforcement Data Security* (CLEDS standards) were published in July 2007. Victoria Police has been required to adhere to them since then.

Commencing in 2013, CLEDS undertook work to update the Standards. The principal objectives were:

- to ensure their currency
- to assess whether amendments were required in light of the Commonwealth's development of the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) and revisions to any other relevant protective security benchmarks
- to ensure that the CLEDS standards continue to capture best practices tailored for the law enforcement environment in Victoria.

Although the update process confirmed that the 2007 standards remain fresh and relevant, it also showed that a number of changes were needed to take account of the evolving protective security environment. The revised standards now align with the Commonwealth's approach to security classification/protective markings as set out in the Protective Security Policy Framework and incorporate a number of clarifications.

The updated Standards for Victoria Police Law Enforcement Data Security were issued in May 2014.

Survey of Victoria Police Members

Wave 2 of the CLEDS survey of sworn members of Victoria Police – examining information security culture and the use of personally owned equipment for operational policing purposes – was conducted in March/April 2014.

The response rate to wave 2 of the survey was lower than that for wave 1, but still over 17%, making for a robust data set.

Key high level findings of the survey were that:

- Victoria Police's cultural change strategy has generated a high level of awareness of change in the way law enforcement data is managed, with nearly two thirds of respondents noticing that change has occurred
- Of members who have noticed change, over half believe that it has impacted positively on data security awareness and improved functional efficiency
- Nevertheless, attitudes and behaviours have not changed significantly, with the exception of the capture and storage of law enforcement data on personally owned equipment, which is now seen as more serious and less likely to occur
- The use of personally owned equipment has continued to increase

The findings of the survey are not surprising. Cultural change in an organisation as large as Victoria Police, with a long history of a command and control culture, is necessarily slow. While there is evidence that Victoria Police's cultural change strategy is having a positive effect, it has yet to influence attitudes and behaviours.

Wave 3 of the CLEDS survey is scheduled to take place in 2016, by which time we will be better placed to judge the effectiveness of cultural change within Victoria Police.

Approved Third Parties

The Standards for Victoria Police Law Enforcement Data Security 2007 define an Approved Third Party as an organisation or individual external to Victoria Police that has been granted direct access to Victoria Police law enforcement data systems.

In 2008 CLEDS conducted a review to assess Victoria Police compliance with those standards governing relationships with Approved Third Parties. The findings of that compliance review revealed an unsatisfactory situation, notably:

- lack of clear policy and good governance surrounding Victoria Police's relationships with these external parties, particularly the process for granting access to law enforcement data systems
- lack of a central register of Approved Third Parties
- lack of CLEDS compliant documented access agreements with all Approved Third Parties.

It became clear when conducting the 2008 review that no single person or unit within Victoria Police had a complete understanding of the extent or nature of relationships with all Approved Third Parties.

CLEDS made a series of recommendations to Victoria Police and reviewed their implementation in 2009 and 2012. While Victoria Police had acted to implement adequate policy and governance arrangements, the lack of CLEDS compliant agreements with all Approved Third Parties remained a serious issue over the years since 2008.

By 30 June 2013, adequate access agreements were in place with all but three Approved Third Parties. By 30 June 2014, we are pleased to finally be able to say that such agreements are in place with all Approved Third Parties.

This has been a slow process. We acknowledge that it has been difficult for Victoria Police and that its Information Management, Standards and Security Division has made a considerable effort over the years to rectify what was a totally unsatisfactory situation in 2008.

The process has been equally frustrating for CLEDS, trying to get Victoria Police 'over the line'.

We believe that it is one of the principal, concrete achievements of the work of CLEDS to be able to say in 2014 that Victoria Police's relationship with its Approved Third Parties is now compliant with the *Standards for Victoria Police Law Enforcement Data Security*.

INFORMATION SECURITY BREACH REPORTING

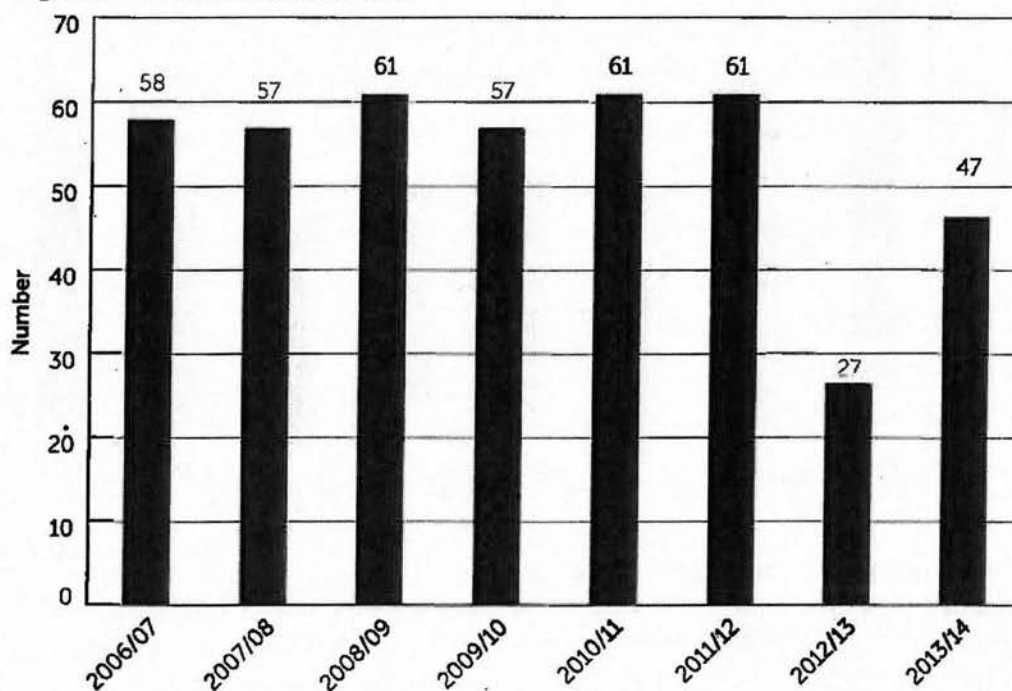
ROCSID

The Commissioner monitors incidents of misuse of law enforcement data or breaches of information security on an ongoing basis.

The primary source of notifications involving Victoria Police is the Professional Standards Command through the Register of Complaints Serious Incidents and Discipline (ROCSID) database.

The Commissioner was notified of a number of substantiated and alleged breaches of data security in Victoria Police during 2013-14 via ROCSID. The number of breaches is shown in Figure 1. The Number of confirmed breaches to date is 47 although with 77 alleged incidents still being investigated this number will likely increase.

Figure 1. Confirmed Breaches



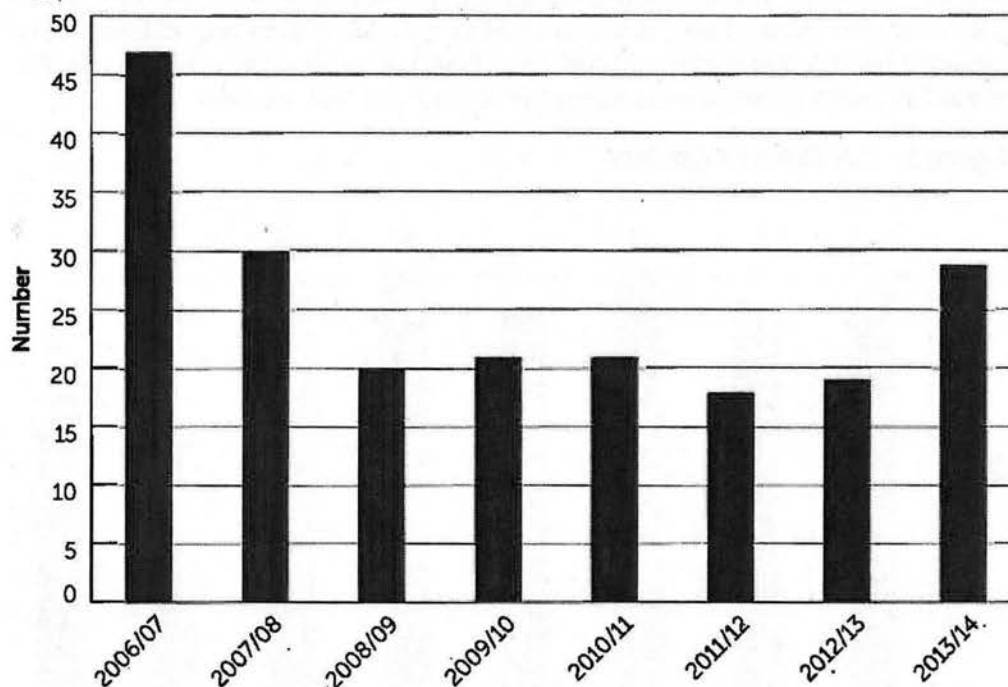
Trends and Issues

We noted in 2012-13 a dip in the number of confirmed information security breaches -- down to 27 confirmed breaches from an average 59 in previous years. We also noted that this low figure was likely to increase due to the larger than normal number of alleged breaches still under investigation at 30/6/2013.

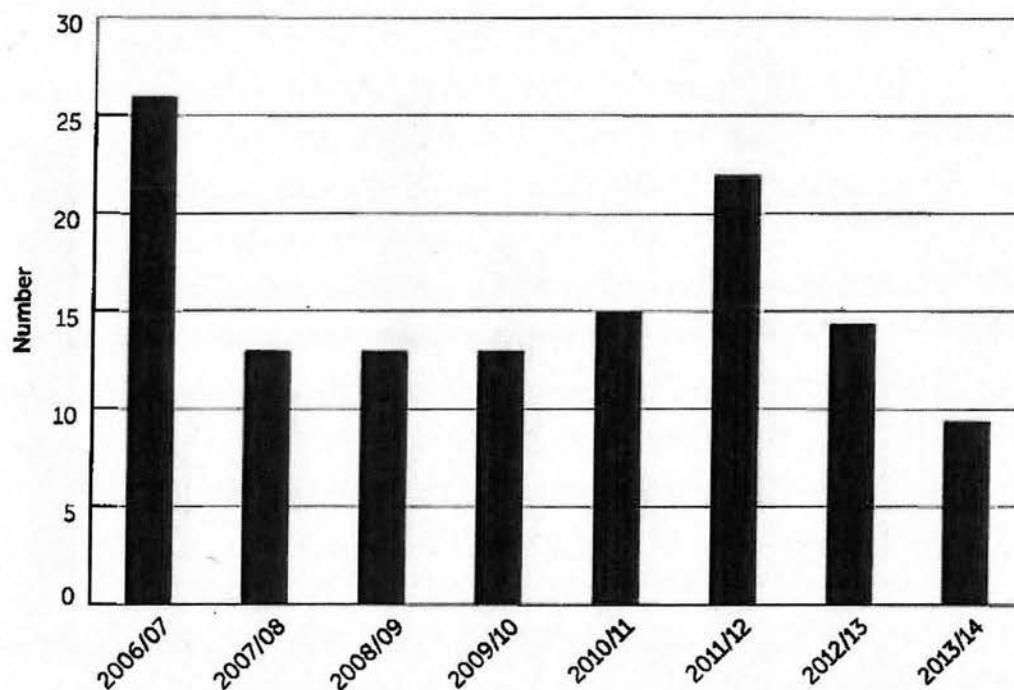
At 30/6/2014 there were 47 confirmed breaches, with 77 still under investigation. As some of the alleged breaches still under investigation will be proven, the figure of 47 is again likely to increase, suggesting a return to the pattern of earlier years.

Again we are reporting against the key breach categories. However it is important to note that some of the figures are so low and/or coming off such a low base, that their statistical use is questionable.

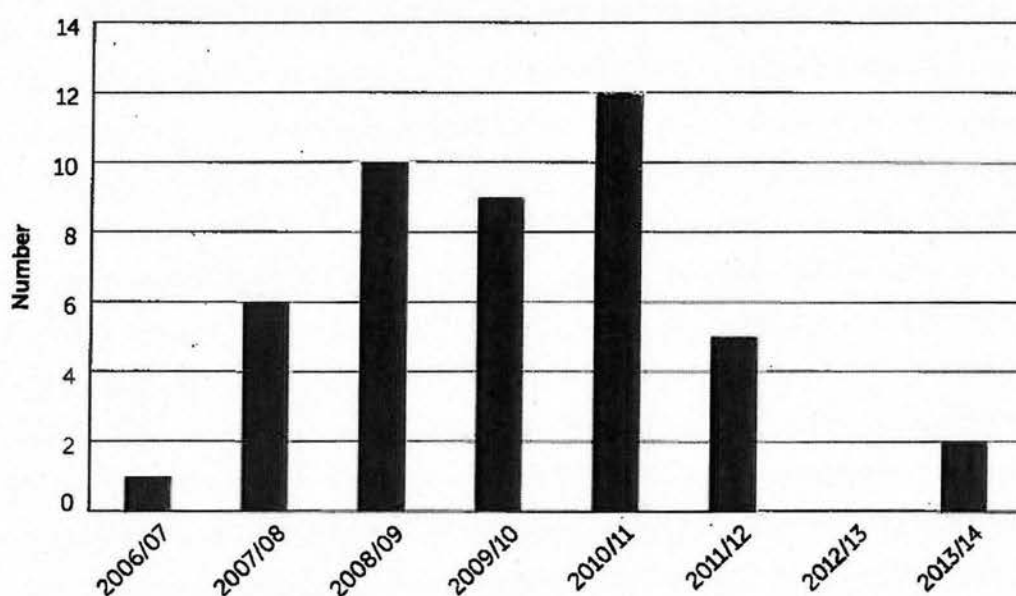
Figure 2. Misuse of LEAP



The number of confirmed breaches relating to the misuse of the LEAP system increased and returned to the level of 2007/08. However in reality this means only an increase from 19/20 to 29 breaches.

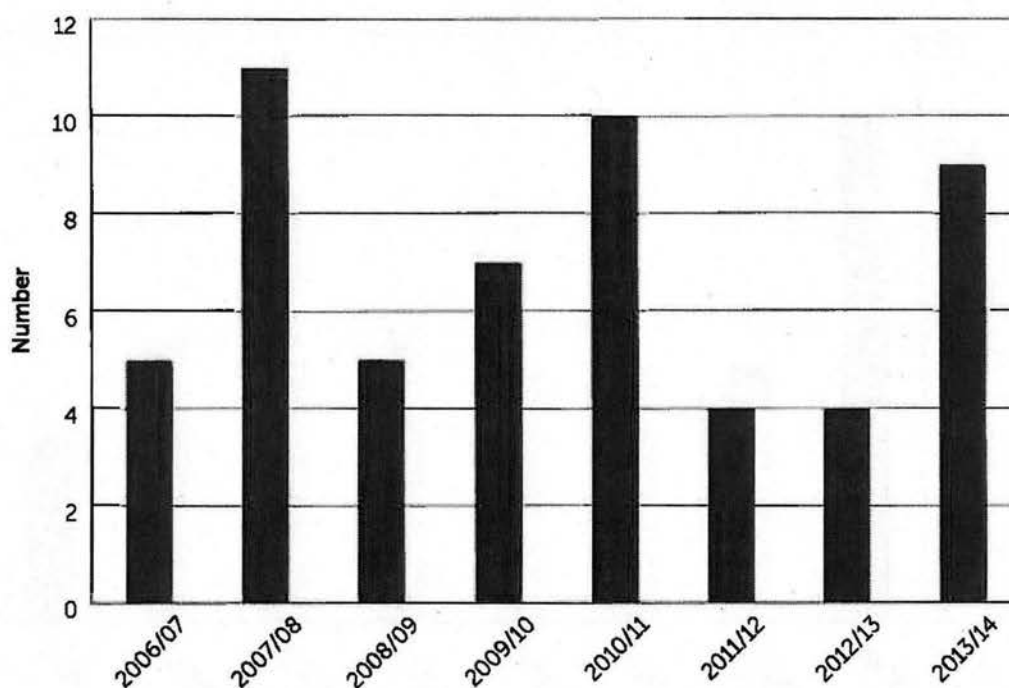
Figure 3. Personal Convenience

The number of breaches due to "Personal Convenience" (improper access to law enforcement data for private, personal convenience, such as checking a family member's vehicle registration details) declined in 2013-14. While the absolute numbers are small, this is the lowest level recorded since breach reporting started in 2006/07.

Figure 4. Improper release to the Media

No cases of improper release to the media were reported for 2012/13. While two cases were reported for 2013/14, the level remains historically low.

Figure 5. Improper Disclosure to Members of the Public



The downward trend in cases of improper disclosure to members of the public noted since 2010/11 has not been maintained. This particular breach category has fluctuated over the years, so it would be unwise to try to draw any conclusion from the increase this year.

The Commissioner will continue to monitor breach investigations and their outcomes during the coming year. Regular discussion of areas of risk, based on emerging patterns of information security breaches will also continue to be held with Victoria Police.

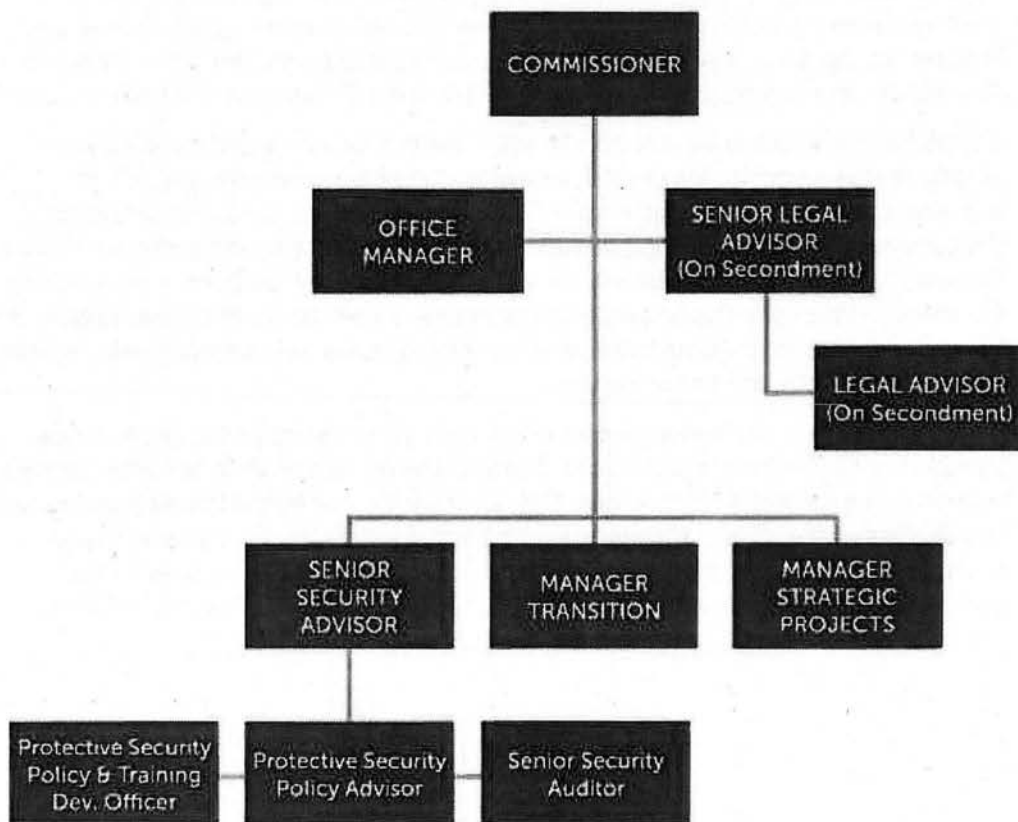
SECURITY INCIDENT REGISTER (SIR)

The CLEDS Standards require Victoria Police to monitor and improve information security incident management, including through a system for recording post-incident analysis of information security incidents. In 2013 Victoria Police took steps to comply with this requirement through the establishment of a security incident register. The security incident register is important in that it is designed to capture security incidents beyond ROCSID, being incidents that do not necessarily involve misconduct or illegal conduct.

CLEDS has previously expressed concern at the lack of an overarching policy and functional framework for the register, lack of documented processes and lack of awareness among members of Victoria Police of its existence. Developments during the current reporting period have started to address those issues. While the overarching framework is a work in progress and still lacks maturity, policy has been developed and is currently in the consultation process. Importantly, a communications plan to bring the SIR and the reporting process to the attention of all Victoria Police employees has been developed and implementation begun.

However the principal development to occur over the reporting period has been the transition of the SIR from a project to a standard component of Victoria Police business, with on-going funding and resources. This will assist Victoria Police to better understand its security threat environment and to take proactive mitigating steps to reduce and manage security threats and incidents. It is of vital importance that Victoria Police continues to support, resource and use the SIR as a centrepiece of its security work.

ABOUT THE OFFICE OF THE COMMISSIONER FOR LAW ENFORCEMENT DATA SECURITY



The Office of the Commissioner for Law Enforcement Data Security had a staff of 9.6 EFT at 30 June 2014, of which 1.6 EFT were on secondment to the Office of the Victorian Privacy Commissioner.

Period	On-going EFT		Fixed-term EFT	
June 2014	76		2	
June 2013	56		3	

	2014		2013	
	On-going	Fixed-term	On-going	Fixed-term
Gender				
Male	3	1	3	1
Female	46	1	26	2
Age				
Under 25	0	1	0	1
25-34	1	0	1	0
35-44	36	0	1	1
45-54	2	1	2	1
55-64	1	0	16	0
Over 64	0	0	0	0
Classification				
VPS1	0	0	0	0
VPS2	0	0	0	0
VPS3	0	1	0	1
VPS4	1	0	1	0
VPS5	26	0	1	0
VPS6	4	0	36	1
STS	0	0	0	0
Statutory Office Holder				

Staffing

As a Special Body under the *Public Administration Act 2004*, the Commissioner for Law Enforcement Data Security does not directly employ staff. Staff for the Commissioner's Office are appointed by the Commissioner, but employed by Victoria Police and provided to the Commissioner on secondment. For the purpose of their work for the Commissioner, the staff are independent of Victoria Police.

The Commissioner is committed to applying merit and equity principles when appointing staff. The selection processes ensure that applicants are assessed and evaluated fairly and equitably on the basis of key selection criteria and other accountabilities without discrimination. The Commissioner offers a supportive and flexible working environment and is committed to ensure the fostering of diversity in the workplace.

Service Level Agreement

Under the terms of the *Commissioner for Law Enforcement Data Security Act 2005*, the Commissioner may request the Chief Commissioner of Police to provide any assistance the Commissioner deems appropriate to perform his functions, including the provision of staff and facilities. A range of corporate support services are provided to the Commissioner by Victoria Police under a Service Level Agreement, specifically in the areas of human resources, business and financial management and information technology infrastructure and services.

Communications and Publications

During the year, the Commissioner and staff continued their program of speaking engagements and attendance at major conferences, notably the Security in Government Conference and the Australian Public Sector Anti-corruption Conference. Staff also attended a series of smaller conferences and workshops dealing with policing and social media and emerging technologies.

The Commissioner also continued to publish on the CLEDS website complete reports of reviews carried out by the Office, in order to further the Victorian public's understanding of the work of the Commissioner for Law Enforcement Data Security and demonstrate the Commissioner's public accountability.

Occupational Health and Safety

The Commissioner aims to provide employees with a healthy and safe workplace. No time was lost in 2013-14 due to workplace injuries. The Office OH&S representative conducted a workplace hazard inspection and completed an office safety checklist during the year. No unacceptable OH&S risks were identified.

Workplace Relations

The Commissioner is advised on industrial relations issues by the People Department of Victoria Police under the terms of the Service Level Agreement. No industrial relations issues concerning the Office of the Commissioner for Law Enforcement Data Security were registered in the course of the year.

No grievances were received by the Commissioner in 2013-14.

Public Sector Conduct

Staff of the Office of the Commissioner uphold the Code of Conduct for Victorian Public Sector Employees of Special Bodies (No 1) 2007. No breaches of the Code by the Commissioner's staff occurred in 2013-14.

Environmental Impacts

Under the terms of the Service Level Agreement, Victoria Police manages the provision of energy, water and waste disposal for the Office of CLEDS. Energy and water are not separately metered. As the principal environmental impacts of the Office are managed by Victoria Police, the CLEDS environmental impact is included within the Victoria Police annual reporting.

COMPLIANCE AND ACCOUNTABILITY

Risk Management

The Commissioner maintains a risk management policy which meets Victorian Government requirements and CLEDS operations take a risk management approach. CLEDS risk register was reviewed for accuracy and currency in June 2014.

As a Special Body, the Commissioner is not obliged to publish a risk management attestation in relation to the A/NZ Risk Management Standard AS/NZ4360. In the interests of transparency and good governance the Commissioner provides a risk management attestation as Appendix 2 to this annual report.

Freedom of Information

The Commissioner received no Freedom of Information requests in 2013-14.

The Commissioner maintains copies of all reviews undertaken by his office and relevant working papers and correspondence. The Commissioner also maintains a register of all recommendations made to Victoria Police.

Due to the nature of the functions of both Victoria Police and CLEDS, the Commissioner holds much information that would be considered exempt material under the *Freedom of Information Act 1982*.

Consultancies

The Commissioner contracted the following consultancies during 2013-14:

Consultant	Value ex-GST
Trusted Impact Pty Ltd	12,731.25
Sandra Beanham and Associates Pty Ltd	20,383.50
Convergence e-Business Solutions Pty Ltd	52,375.15
KPMG	50,545.45

Major Contracts

The Commissioner did not enter into any contracts above \$10 million in 2013-14.

Protected Disclosures

The Commissioner received no disclosures made under the *Protected Disclosures Act 2012* during 2013-14.

Gifts, Benefits and Hospitality

CLEDS maintains a register of gifts, benefits and hospitality. No declarable items were registered in 2013-14.

Statement of Availability of Other Information

The Directions of the Minister for Finance pursuant to the *Financial Management Act 1994* require a range of information to be prepared for the financial year being reported. The relevant information is included in this report, with the exception of a statement that declarations of pecuniary interests have been duly completed by all relevant officers, which is held by the Commissioner for Law Enforcement Data Security and is available on request to the relevant Minister, Members of Parliament and the public (subject to Freedom of Information requirements, if applicable).

FINANCES

The Commissioner for Law Enforcement Data Security is funded under the Victoria Police appropriation. The Government has determined a specific amount of money to fund the Commissioner and his Office, which is under the control of the Commissioner. Budget papers do not apply specific budgetary objectives or outputs to this office.

As a Special Body the Commissioner is not legally required to comply with the reporting requirements of the *Financial Management Act 1994*.

For purposes of transparency, the Commissioner has in the past provided an unaudited Operating Statement and Balance Sheet in his Annual Reports.

This year has been unusual in that, while the CLEDS budget was transferred from Victoria Police to the Department of Justice in the course of the year, some payments, including salaries, continued to be paid out of Victoria Police and other payments out of the Department of Justice. It is not possible to provide provisions and assets until they transfer to the Department of Justice.

In the circumstances, the Commissioner has taken the decision not to provide financial statements in this Annual Report.

APPENDIX 1: DISCLOSURE INDEX


The Annual Report of the Commissioner for Law Enforcement Data Security is prepared in accordance with all relevant Victorian legislation. This index has been prepared to facilitate identification of compliance with statutory disclosure requirements.

As a Special Body the Commissioner is not required to comply with the reporting requirements of the *Financial Management Act 1994*. The Commissioner for Law Enforcement Data Security includes relevant information in this report so as to provide the Parliament and the people of Victoria with a transparent and informative account of the Commissioner's operations for the year.

Legislation	Requirement	Page Reference
Ministerial Directions		
Report of Operations – FRD Guidance		
Charter and purpose		
FRD 22B	Manner of establishment and the relevant Ministers	Page 6
FRD 22B	Objectives, functions, powers and duties	Page 6
FRD 22B	Nature and range of services provided	Pages 9–24
Management and structure		
FRD 22B	Organisational structure	Page 25
Financial and other information		
FRD 10	Disclosure index	Page 32–33
FRD 12A	Disclosure of major contracts	Page 30
FRD 15B	Executive officer disclosures	Page 30
FRD 22B	Employment and conduct principles	Page 27–28
FRD 22B	Occupational health and safety policy	Page 28
FRD 22B	Summary of the financial results for the year	Page 31
FRD 22B	Application and operation of <i>Freedom of Information Act 1982</i>	Page 29
FRD 22B	Application and operation of the <i>Protected Disclosures Act 2012</i>	Page 30
FRD 22B	Details of consultancies over \$100 000	Page 30
FRD 22B	Details of consultancies under \$100 000	Page 30
FRD 22B	Statement of availability of other information	Page 30
FRD 24B	Reporting of officebased environmental impacts	Page 28
FRD 29	Workforce Data disclosures	Page 26
Legislation		
<i>Commissioner for Law Enforcement Data Security Act 2005</i>		
<i>Freedom of Information Act 1982</i>		
<i>Protected Disclosure Act 2012</i>		
<i>Financial Management Act 1994</i>		
<i>Audit Act 1994</i>		

APPENDIX 2: ATTESTATION ON COMPLIANCE WITH THE AUSTRALIAN/ NEW ZEALAND RISK MANAGEMENT STANDARD

I, David Watts, certify that the Office of the Commissioner for Law Enforcement Data Security has risk management processes in place consistent with the Australian/New Zealand Risk Management Standard and an internal control system is in place that enables the executive to understand, manage and satisfactorily control risk exposures. An independent auditor verifies this assurance and that the risk profile of the Office of the Commissioner for Law Enforcement Data Security has been critically reviewed within the last 12 months.



David Watts
Commissioner for Law Enforcement Data Security
30 June 2014

