Recent Inquiries into the private security industry in Australia: Implications for regulation

Tim Prenzler and Alastair Milroy

Tim Prenzler (corresponding author) is a Chief Investigator in the Australian Research Council Centre of Excellence in Policing and Security (CEPS), and a Professor in the School of Criminology and Criminal Justice, at Griffith University. In CEPS he manages the Integrity Systems research program and works in the Frontline Policing program. He also teaches courses in criminal justice ethics and accountability, and situational crime prevention and security management.
Correspondence:
Australian Research Council Centre of Excellence in Policing and Security, Griffith University, Mt Gravatt Campus, Brisbane, Queensland, 4122, Australia. Ph/fax: (011-61) (0)7 373 55613/51033. E-mail: t.prenzler@griffith.edu.au

Alastair Milroy AM is an Executive-in-Residence in the Australian Research Council Centre of Excellence in Policing and Security (CEPS), at Griffith University. He served with the New South Wales Police, New South Wales Drug Enforcement Agency, National Crime Authority, the Royal Commission into the New South Wales Building Industry and the United Nations International Criminal Tribunal. He has worked in private security as a consultant and as the National Security Manager for Brambles Australia. Alastair was the Chief Executive Officer of the Australian Crime Commission from 2003 to 2009.
Correspondence:
Australian Research Council Centre of Excellence in Policing and Security, Griffith University, Mt Gravatt Campus, Brisbane, Queensland, 4122. E-mail: a.milroy@griffith.edu.au

Abstract

The private security industry has come under increasing scrutiny in line with growth in the number of security providers and increasing dependence on private providers for crime prevention, including at critical infrastructure sites. Inquiries and research have shown the industry is vulnerable to misconduct and many jurisdictions have enlarged licensing requirements to guard against abuses. This paper reports on recent inquiries into the industry in Australia, conducted by the Australian Crime Commission, the New South Wales Independent Commission Against Corruption, and the Fair Work Ombudsman. Using a variety of novel investigative techniques, the inquiries revealed a diverse range of problems, including criminal activity and infiltration by organised crime, corruption in security guard training, and the exploitation of security staff through under-award payments. The extent of the misconduct obliges an upwards revision of the risk profile for the industry and

demonstrates the importance of a more proactive and complex approach to regulation.

Context: Growth and Reform

Growth in private security has been recognised as one of the most significant developments in policing since the Second World War (Bayley & Shearing, 2001). A 2011 survey conducted in 70 countries concluded there were approximately 19.5 million people working in the industry. Across all countries the numbers were projected to include 25.5 million persons (Small Arms Survey, 2011). The industry was valued at up to $US165 billion, with a growth rate of approximately eight percent per annum. Across the 70 countries surveyed, private security personnel were estimated to outnumber police by a ratio of 1.8:1.

The phenomenon of security industry growth has been linked to a variety of factors including the failure of public police to stem the large increases in crime experienced in many countries from the 1970s to the 1980s, as well as health and safety legislation, increased litigation, the post-1960s terrorist threat, and pressure by law enforcement to make stakeholders take greater responsibility for crimes in their sectors (Small Arms Survey, 2011; van Dijk, 2008). The industry continues to grow, despite reductions in crime since the 1990s, on the back of improving security technologies and a culture of increased reliance on the self-provision of security.

Growth in security has been accompanied by the increased exposure of security company clients and the general public to misconduct by industry members. Prenzler and Sarre (2008a) analysed a variety of industry inquiries and scandals, and developed the following categorisation of the main types of illegal and unethical conduct:

1. Fraud (mainly in misrepresentation of tenders and failure to fulfil contracts)
2. Incompetence and poor standards
3. Under-award payments and exploitation of security staff
4. Corrupt practices (e.g., bribery in tenders, and kickbacks from police for priority emergency security referrals)
5. Information corruption (e.g., purchase of confidential information from police and public servants)
6. Violence (predominantly assaults and neglect of duty by crowd controllers)
7. False arrest and detention
8. Trespass and invasions of privacy
9. Discrimination and harassment
10. Insider crime
11. Misuse of weapons.

These problems have been manifest in different industry sub-sectors at different times, and they have driven closer regulation of the industry by governments around the world (Button & George, 2006). Regulation usually involves standard occupational licensing across two key domains: governments underwrite probity – through character reference checks and

disqualifying offences – and competency – through mandated minimum training standards. Internationally, the application of these standards varies enormously, but few jurisdictions have required training beyond a few days, with up to a month in exceptional cases (Button & George, 2006; CoESS, 2008).

The Australian security industry has seen some of the most advanced regulation internationally in recent years (Sarre & Prenzler, 2011). Licensing was introduced in a piecemeal fashion across the six states and two territories in the 1980s and 1990s as a consequence of exposés of malpractice and deficient training (Prenzler & Sarre, 2008b). Reform in this period was focused on security companies, guards, private investigators and crowd controllers; with the introduction of criminal history checks, disqualifying offences, character checks, and pre-licence training requirements. Legislation was administered by specialist government agencies tasked with investigating complaints and inspecting security firms and licensed premises. These arrangements were exposed as inadequate by a fresh series of scandals in the 2000s (Prenzler & Sarre, 2008b). Concerns grew over the alleged infiltration of the industry by criminal gangs, especially outlaw motorcycle gangs. One signal event was the death of cricketer David Hookes in an altercation with a crowd controller in Melbourne in 2004. The same year also saw national attention focused on the shooting of a fleeing armed robber by a cash-in-transit guard in Sydney. Scandals also erupted in Sydney over the theft of firearms from security firms, and fraud in tendering by a major security firm. A number of other examples of security failures were highlighted in the press in this period, including at airports, and there were continuing concerns about violence by crowd controllers (or 'door staff') at clubs and pubs.

All Australian jurisdictions modified their regulatory systems in response to these problems (Prenzler & Sarre, 2008b). Disqualifying offences were expanded to include firearms offences and drug offences, and there was a move to suspend licences when licensees were charged with an offence. South Australia and Victoria introduced checks on licence applicants' associates, with discretionary powers to deny or withdraw a licence when involvement with criminals was evidenced. South Australia introduced drug and alcohol testing of crowd controllers and fingerprinting of applicants. Amendments in New South Wales (NSW) included restrictions on firearms and firearms storage requirements. Nationally consistent certificate-level training standards were also introduced, with more attention in the curriculum to communication, conflict management, management of intoxicated persons, and legal and procedural requirements. Where they could be quantified it appeared that minimum training hours had been doubled from approximately one to two weeks.

The remainder of this paper provides a follow up study to Prenzler and Sarre's (2008b) account of industry scandals and regulatory reform in Australia in the 2000s. By 2008 the reform measures had been largely put in place, although there was little indication of any immediate positive effects – with ongoing problems of violence, unresolved issues in airport and seaport security, and the announcement of a major inquiry into criminal infiltration of the industry. From 2008 to 2010 there were a number of reviews and media exposés of problems in the industry, but three in-depth government-based inquiries stood out as particularly significant.

Inquiry 1: The Australian Crime Commission (ACC) Inquiry into Criminal Infiltration of the Private Security Industry

In 2007 the Australian Crime Commission launched a 'special intelligence operation' into the nature of criminal infiltration and exploitation of the private security industry. The 'Private Security Industry Determination' was approved by the Commission's Board in September 2007, then extended in June 2008 and completed in June 2009 (ACC, 2009a, p. 54). No report has been made public. Both authors of the present study had input into the operation but are prohibited by law by revealing anything not disclosed publicly by the Commission (*Australian Crime Commission Act 2002*, s.51). The remainder of this section is therefore dependent on sources in the public domain.

The context for the ACC inquiry included concerns by various law enforcement agencies that the security industry 'was increasingly a focal point for organised crime' (Maley, 2009, p. 3; also ACC, 2007, p. 55). These concerns overlapped with mounting evidence of criminal activities at airports and seaports – which led to the Wheeler (2005) report on airport security – and also increased activity by outlaw motorcycle clubs (Prenzler & Sarre, 2008b; Prenzler, Lowden & Sarre, 2010). The latter issue had been particularly salient in Adelaide, Perth and the Gold Coast in the mid-2000s, with allegations of motorcycle clubs providing nightclub security while engaged in money laundering and illicit drug sales (Chambers, 2006; Office of Consumer and Business Affairs, 2004). The ACC carried out investigations into the transport sector and the maritime sector between 2005 and 2008 (ACC, 2009b). These investigations revealed how criminal gangs engaged with staff at transport hubs willing to overlook illegal activities or provide information. In some cases, rosters were altered to avoid detection of contraband – including illicit drugs, weapons, tobacco and counterfeit goods. Theft of goods was also a major criminal activity.

The 2007-8 federal budget included a special allocation of $8.741 million to the ACC for the Private Security Industry Determination (ACC, 2008, p. 56). The determination was classified as a Special Intelligence Operation – involving coercive powers and focused on 'the gathering of intelligence surrounding particular criminal activity so that informed decisions can be taken about the true extent, impact and threat of that criminal activity' (ACC, 2008, p. 31). The operation was therefore not directly concerned with shutting down criminal operations or identifying and prosecuting offenders; and it excluded the use of listening devices. The final revised purposes were listed as follows (ACC, 2009a, p. 54):

- advise government on the nature of criminal infiltration and exploitation of the private security industry
- undertake intelligence development work in relation to the threat to the private security industry from criminal infiltration and exploitation and better inform partner agencies and stakeholders through the dissemination of intelligence products
- work in a collaborative manner with partner agencies to advance appropriate law enforcement responses to, or protection against criminal infiltration and exploitation of the private security industry, and

- support national law enforcement investigative efforts into the security industry and serious and organised crime groups that are active in that industry through use of the ACC's coercive powers and operational capabilities.

The approach adopted by the ACC was a 'multi-faceted engagement strategy' (ACC, 2008, p. 58). Table 1 summarises key activities in quantitative form. It can be seen that this was an extensive operation which proceeded through investigative interviews and examination of documents. The Commission also undertook data-mining exercises, comparing information on 52,000 security industry licences, held by State and Territory licensing agencies, with criminal history data held by the Commission (ACC, 2008, p. 56). Data-matching was also carried out with Centrelink (the main welfare distributor) and the Australian Taxation Office.

Table 1: Australian Crime Commission Private Security Industry Special Intelligence Operation Actions

Action	2007-08	2008-09	Total
Summonses to attend examinations	93	99	192
Examinations held	84	89	173
Notices to produce documents	11	34	45
Intelligence product disseminations	21	144	165
Operational intelligence disseminations	7	844	851

Source: adapted from ACC, 2009a, p. 55.

The ACC also took the unprecedented step of advertising for persons to come forward with information. The wide advertising campaign included security industry magazines and websites, national newspapers, and the Commission's website (ACC, 2008, p. 58). This 'resulted in 25 industry submissions reporting serious and organised criminal activity and regulatory-related issues of significance' (p. 58). However, only six submissions 'contained relevant information' (p. 58). In addition, stakeholder consultations were conducted with a large number of organisations, including the Australian Federal Police, the Australian Taxation Office, the Australian Security Industry Association Limited and the Institute of Security Executives. The investigation devolved into two 'projects':

> The first project focussed on the presence of organised crime members who both own and operate security companies providing crowd control and other services within the entertainment sector. Criminal activity of interest that is being explored under this project includes tax evasion, money laundering, extortion and drug distribution. The ACC liaised with the ATO and other relevant government agencies on these matters.
> The second project explored matters associated with the protection of critical infrastructure through the use of the ACC's coercive powers. High level liaison with Australian Government agencies has been established and is ongoing for this project (ACC, 2008, p. 57).

Table 1 shows that in terms of specific products, a large number of intelligence summaries were generated. These were disseminated to relevant stakeholders in the consultation process. Furthermore, 'operational intelligence disseminations' were made on specific individuals, with potential for action through prosecutions or licence revocations. The Commission's 2008-09 *Annual Report* summarised 'notable outcomes' from the operation as follows (ACC, 2009a, p. 55):

> Intelligence in relation to methodologies pertaining to the use of unlicensed security guards supported intelligence assessments of vulnerabilities in the security industry in a number of jurisdictions.
>
> Extensive data sets containing information on security licence holders, security master licence holders and staff lists were disseminated to relevant agencies to identify tax evasion, Centrelink [welfare] fraud and potential immigration breaches.
>
> In Victoria, examinations were used to develop intelligence around the incidence of current visa holders obtaining residential status through false references as security guards. The ACC continues to work closely with both Victoria Police and the Department of Immigration and Citizenship on these enquiries.

The 2008-09 *Annual Report* also included the following private security industry 'case study' (ACC, 2009a, p. 55):

> The Private Security Industry Determination collaborated extensively with the Australian Taxation Office, Centrelink, the Department of Immigration and Citizenship and the Fair Work Ombudsman to gain a multi dimensional understanding of the Private Security Industry. These partnerships have resulted in the identification of a significant cash economy with a high potential economic cost within the private security industry.
>
> Extensive qualitative operational intelligence reporting disseminated by the Private Security Industry determination has informed our partner law enforcement agencies of criminal threats and vulnerabilities to criminal infiltration and exploitation posed by serious and organised crime groups.
>
> ACC activity under the private security industry determination has also assisted Centrelink identify suspected fraudulent claimants, potentially resulting in very significant savings for government.

Elsewhere, the cash economy component was described as involving 'a potentially high cost to the Australian economy' (Lawler, 2009, p. 6).

The somewhat circumlocutory language used in these official accounts was repeated in a four page report, 'Private Security Industry Criminal Infiltration', produced as part of the Commission's *Crime Profile Series*. The report included a background summary of secondary literature on misconduct risks in security work, and provided a summary profile of opportunity factors in security (ACC, 2011, p. 1):

The vast majority of companies and individuals working in the private security industry are legitimate and provide an excellent service to the Australian community.

However, the nature of the industry – with its access to firearms, licensed premises, major events and a range of public and private assets – provides both an incentive and an opportunity for organised crime groups to infiltrate and exploit its activities and operations.

The report went on to state that 'it is difficult to determine an exact percentage of criminal infiltration of the industry', but noted that examples of criminality were uncovered 'across all states and territories', including infiltration by organised crime and by outlaw motorcycle gangs (p. 3). The report concluded, in fairly general terms, that:

Organised criminals are motivated by profit and will move into sectors where they identify there is a high profit to be made at relatively low risk. They will always look to target sectors that have the least regulation.

Organised criminals may become involved in the private security industry by owning security firms, being employed as individuals or bribing or corrupting security firms or employees. There is a broad range of crimes they can commit through these methods including fraud, property theft, illicit commodity distribution (such as drugs), money laundering, trespass, assault, misuse of firearms, extortion, tax evasion, welfare fraud, breach of industry regulations and workplace legislation and labour and visa exploitation (p. 4).

A somewhat clearer picture of criminal activity in the industry was provided in a 2009 newspaper account of the investigation, which made use of extensive quotations from the Commission's CEO John Lawler. The national newspaper *The Australian* reported that:

Organised crime groups have penetrated the private security industry, with some using their access to move drugs, launder money or run standover rackets.

Australian Crime Commission chief executive John Lawler said a two-year investigation had revealed a range of criminal practices, from visa and labour exploitation to organised theft.

'We have found examples of infiltration of the industry by organised crime groups, including outlaw motorcycle gangs,' Mr Lawler said.

'The nationally significant organised criminal activities are actually co-ordinated across multiple jurisdictions or, importantly, involved the infiltration or external influence of already recognised and known serious organised criminal groups.'

Mr Lawler described the types of criminality detected by the ACC as 'co-ordinated and sophisticated'.

Criminal groups were using their positions within the security industry to increase their market share and to muscle criminal competitors, he said.

The problem was exacerbated by the nature of the private security sector, Mr Lawler said, because of its ready access to drug markets and valuable commodities.

The result was a spectrum of offences.

'So, things like violence, intimidation and extortion, illicit commodity related activity, organised theft and money laundering,' Mr Lawler said…

As part of its investigation, the ACC uncovered exploitation of the cash-based nature of the industry, Mr Lawler said.

While most private security firms did the right thing, the ACC had uncovered a level of white-collar offending, he said.

'So what sort of offences are we talking about? We're talking about tax evasion (and) welfare fraud.

'We're talking about non-compliance with superannuation requirements, worker compensation requirements, industry awards and workplace legislation, labour and visa exploitation, extortion and intimidation for increased industry market share and breach and manipulation, or circumvention of state-based industry regulation.' (Maley, 2009, p. 3)

Inquiry 2: The New South Wales Independent Commission Against Corruption (ICAC) Investigation into Corruption in Security Industry Training

The Australian security industry has long been plagued by allegations of inadequate training of operatives under compulsory licensing systems. Surveys of security firm owners and managers have shown, at best, very mixed views about the adequacy of training standards (Sarre & Prenzler, 2011, pp. 60-71). Concerns have also repeatedly been expressed about auditing and accountability in the registration of training firms, issues of integrity in assessment of competencies, and lack of transparency regarding quality assurance processes. Specific findings about these problems were made in New South Wales as a result of investigations by police and regulators in the early- to mid-2000s (ICAC, 2009, p. 47).

Up to 2010, the NSW Security Industry Registry (SIR) issued licences under the *Security Industry Act 1997*. Key criteria included clearance through criminal history checks and completion of security training courses. The courses were conducted by Registered Training Organisations (RTOs), approved by the SIR and registered with the NSW Vocational Education and Training Accreditation Board (VETAB). In 2007 the licensing system was amended to increase the number of operative categories from three to seven (ICAC, 2009, p. 14). The amendments were aimed at improving specialist skills and required re-training by existing licence holders. At the same time, an 'assessment-only pathway' was made available through Recognition of Prior Learning (RPL) that also involved a mix of testimony from employers, presentation of work diaries and observations by trainers.

Issues of integrity in security training came to a head in New South Wales in October 2008 when the Independent Commission Against Corruption received a report from the Registrar of the SIR regarding possible financial corruption at a security guard training firm. The report on Roger Training Academy 'was based on a number of complaints received by the SIR from former Roger students, intelligence from NSW Police and statements made by former trainers at Roger' (ICAC, 2009, p. 10).

The Commission launched an investigation – 'Operation Columba' – into 'Roger' and a number of associated training and security firms. The Commission's coercive powers were used to obtain documents, including student files. Warrants were executed on the residences of several Roger training staff. Interviews were conducted and statements taken from 'a large number of witnesses' (p. 10). Five compulsory examinations were undertaken with key persons of interest, four of whom made admissions about corrupt activities. The examinations were made in a 'public inquiry' format that covered 10 days of hearings and included 28 witnesses. 'Extensive use' was also made of 'covert physical and electronic surveillance', including telecommunications intercepts (ICAC, 2009, p. 11). The initiation of an undercover operation was another innovative strategy:

> A controlled operation was authorised under the *Law Enforcement (Controlled Operations) Act 1997* NSW … The controlled operation involved a Commission undercover operative approaching a trainer at Roger to obtain a certificate of competency in a security course for the purpose of applying for a security licence (ICAC, 2009, p. 11).

The ICAC's *Report on Corruption in the Provision and Certification of Security Industry Training* was released in December 2009. The report found that Roger Training Academy provided students with answers to tests, primarily through an 'open book' exam format. Certificates of competency were issued to candidates in the two-week pre-licence training program 'without requiring them to attend any classes or undertake the relevant course' (p. 17). False documents were created to make it appear students had attended classes. In some cases, candidates with poor English language skills were assisted by an interpreter and paid additional money to pass. The ICAC's investigation included an examination of 1,200 student workbooks. Of these, 970, or 80 percent, appeared to have been falsified. Between September 1, 2007, and March 9, 2009, 44,680 training certificates were issued by RTOs. Roger was able to corner 25.6 percent of this market, while another corrupt firm was able to obtain 10.0 percent of the market (ICAC, 2009, pp. 6 & 49).

Fraud in training certificates also included the RPL process. Roger and other training and security firms conspired to falsely issue certificates of competency for licence holders upgrading to the new specialist classifications. The ICAC report (2009, pp. 18-21) also found that personnel at Roger had conspired with two other training companies in the issuance of false certificates in First Aid, Responsible Service of Alcohol, and Responsible Conduct of Gambling, required for some security work. These certificates could be bought by candidates for AU$100 or AU$150 without training or testing. Roger paid the firms a separate fee of between AU$20 and $AU40 for certificates.

A total of ten persons were named as engaging in corrupt conduct. The various scams allegedly netted Ahmed Moosani, the Principal of Roger, approximately AU$1.3 million between 2008 and 2009, although his corrupt activities began before this period. In its report the ICAC emphasised the potential harm from these corrupt practices:

The security industry in New South Wales is responsible for providing security in significant ways – for example at airports, hotels and concerts, and also at government facilities, including army bases. The Commission's investigation found that corrupt conduct in connection with the certification of security officers resulted in a significant number of those officers engaging in security activities, some of which posed risks to their own and public safety, without having undertaken appropriate levels of training (2009, p. 10).

The report included 16 recommendations under the heading 'corruption prevention' (ICAC, 2009, chapter 5). The Commission was critical of both the SIR and VETAB in failing to address previously identified problems in security industry training. In fact, it pointed out that the 2007 licence upgrade created a corruption opportunity that flooded the market with untrained licence holders. Key recommendations in the ICAC's report included review of all questionable qualifications and possible re-testing, and the adoption of corruption risk management procedures by all stakeholders and agencies involved in regulation of the industry; as well as more thoroughgoing investigations, much closer auditing, and more decisive enforcement of standards. There was also a recommendation that the SIR 'independently test and assess applicants prior to granting a security licence' (ICAC, 2009, p. 59).

Inquiry 3: The Fair Work Ombudsman's audit and campaign in relation to under award pay entitlements in the industry

The private security industry in Australia, as in many other countries, has been plagued by allegations of undercutting in tendering and fulfilment of cut price contracts through under-award payments to security staff (Prenzler & Sarre, 2008a; Sarre & Prenzler, 2011, p. 75). The Australian Fair Work Ombudsman was prompted to launch a security industry compliance campaign and investigation between July and December 2009 following numerous complaints, many of which held sufficient evidence for the Ombudsman to have initiated litigation against firms. Intelligence provided by the Australian Crime Commission and other government agencies stimulated specific concerns about the exploitation of 'vulnerable workers', including foreign nationals and immigrants (Fair Work Ombudsman, 2010, pp. 3-4).

The campaign involved 9,189 'educational letters' posted to employers alerting them to their responsibilities under workplace laws. In addition, 87 'industry stakeholders' were informed of the campaign, and meetings were held with 'key stakeholders' – including the Liquor Hospitality & Miscellaneous Union, and the Australian Security Industry Association Limited (ASIAL) (the largest industry association) and the Security Providers Association of Australia Limited (SPAAL). A total of 747 security businesses were targeted for auditing. Of these, 133 had no employees, 180 could not be contacted and 132 had ceased trading, while four were considered outside the Ombudsman's jurisdiction. The targeted businesses were required to provide records of time and wages and other information for a period that included a public holiday. The Ombudsman commenced a 'full investigation' in cases where firms did not cooperate or where records indicated 'serious and deliberate' breaches (2009, p. 5).

In February 2010 the Ombudsman released its report, *National Security Industry Campaign 2009: Report and Recommendations*. At the time of publication, 256 employers had been audited, with another 42 still under investigation. Of the 256, 51% were found to be compliant and 49% were considered non-compliant with the *Fair Work Act*. The audit identified 194 specific breaches, spread across the six states. Of the 126 firms that were non-compliant, the following breakdown of types of breaches was reported (Fair Work Ombudsman, 2010, p. 8):

- 66 (52%) had minor contraventions relating to time and wage records and payslips
- 60 (48%) had monetary contraventions relating to underpayment of wages, penalty rates and allowances
- 27 (21%) had both types of contraventions.

An amount of AU$452,824 was recovered on behalf of 652 security staff (2010, p. 9). In the concluding remarks the report asserted that:

The primary finding from the Campaign across all states was the common practice of employers paying flat rates. While these rates were sometimes significantly above the 'hourly rate' in the relevant industrial instrument, the rate failed to compensate for shift and weekend penalties, overtime or annual leave loadings (Fair Work Ombudsman, 2010, p. 13).

It was also strongly suspected that a significant proportion of firms that could not be audited were engaged in two types of illegal or unethical conduct. 'Sham contracting' involved 'disguising an employment relationship as an independent contracting arrangement'; while 'phoenixing' involved 'self liquidating an entity to avoid paying liabilities and replacing it with another to undertake the same function' (2010, p. 3).

At the same time that these criticisms were made, there were a number of affirmative comments made about the industry. The report noted that:

The Fair Work Ombudsman was pleased with the positive interest demonstrated by respective employer associations, including the security industry's support of the education seminars.

Similarly, the number of employers to respond positively to the Fair Work Ombudsman's intervention and to commit themselves to voluntary compliance was extremely gratifying. Among these compliant and committed employees was a feeling that poor practices among their competitors should be exposed and remedied (2010, p. 13).

Five recommendations were made, including a commitment from the Ombudsman to continue educating employers about their responsibilities in cooperation with employer associations, particularly in relation to the new national *Security Services Industry Award 2010* (Fair Work Ombudsman, 2010, pp. 3 & 13). The Ombudsman also made a commitment to continue investigations into the 42 outstanding cases and the employers suspected of

sham contracting and phoenixing, and to assess the level of change through a follow-up audit of a sample of non-compliant employers.

Implications

The three inquiries into the private security industry described in this article were unprecedented in Australian history. They also appear to be unusual in their depth and reach internationally (cf. Button & George, 2006). One comparable case was the exposé of criminality in security work in the United Kingdom by the investigative television program *Panorama* (2008). In Australia, the fact that there were three overlapping inquiries at once reflects the diverse nature of the problems under examination and the nature of Australian federalism, with overlapping State and Commonwealth jurisdiction. The Australian Crime Commission and the Fair Work Ombudsman inquiries were the first of any substance at the national level. The ACC and NSW ICAC inquiries were also unprecedented in the use of coercive powers, including compulsory examinations; and the ICAC inquiry was also unprecedented in the use of covert techniques. It is difficult to determine the adequacy of these approaches. For example, it could be argued that greater use could have been made of phone tapping powers and covert surveillance, and also anonymous surveys of industry operatives. Greater quantification of the scale of the problems, including across different industry sectors and companies, would also have been helpful. And it was unclear how unique these problems were to security work. Nonetheless, all three inquiries usefully revealed serious deficiencies in the existing regulatory system by confirming long held suspicions and allegations about diverse forms of misconduct in the industry. They also set precedents for the application of advanced techniques to identify and prevent misconduct on a permanent basis.

The ICAC and Fair Work Ombudsman investigations resulted in reports on the public record of considerable value and utility. Although the ACC provided information in a number of forums about the nature and outcomes of its investigation, legislative prohibitions on the publication of even a redacted account has left a large hole in the public accountability process. $8.7 million of taxpayers' money went into the inquiry with only limited disclosure. Information was also lacking about any criminal prosecutions and convictions that following from ACC referrals of intelligence to other law enforcement agencies. However, amendments to the *Australian Crime Commission Act* were introduced into federal Parliament in late-2011 to allow for dissemination of some Commission determinations (Personal Communication, Executive Assistant to the Chief Executive Officer, Australian Crime Commission, 13 December 2011).

The ACC investigation can be likened to the major inquiries into police corruption in Queensland (1987-89), New South Wales (1995-1997) and Western Australia (2002-04), which drove substantive change in oversight and corruption controls as a consequence of their detailed findings and specific recommendations (Prenzler, 2011). The initial brief to the ACC included 'options for early detection of illegal activities in the industry', and the threat assessment was intended to inform 'legal and regulatory reform and policy development' (ACC, 2008, p. 56). This was diluted in the later list of aims (cited above), with the focus placed instead on the threat assessment

and confidential intelligence reports for law enforcement. As a result, there are no detailed practical recommendations on the public record to support reform. An unprecedented opportunity to facilitate national action on industry regulation was lost, and this appears to be reflected in a lack of post-inquiry follow-up assessments.

In New South Wales, an initial review by the ICAC (2011) of the implementation of the 16 recommendations in the Operation Columba report indicated that most had been implemented as prescribed. Those relating to independent testing procedures were still under development, and there was an ongoing procedure to check and upgrade qualifications issued by the corrupt trainers. In line with one set of recommendations, in June 2010 the Security Industry Registry – renamed the Security Licensing and Enforcement Directorate (SLED) – was enlarged with an increase in allocated staff from 40 to 73 (see also Sexton, 2012). The regulator also became subject to direct control by the New South Wales Police Commissioner through the State Crime Command.

The enlargement of the New South Wales regulator will give it greater capacity to monitor the industry. However, criticism was made of a lack of specificity about the nature of enforcement (Cowan, 2010). Since then the State government has indicated that the SLED will 'get the power to raid companies and audit their books', and that there will be a much greater focus on intelligence gathering with a view to prosecuting criminal conduct (Sexton, 2012, p. 27). Nonetheless, there remains a major problem with lack of annual reporting on the regulator's activities and impacts, and the issue of ongoing responsibility for enforcement of training standards remains blurred.

Also in New South Wales, stakeholder support for the ICAC's recommendations degenerated into controversy when the state government abandoned the co-regulatory system (O'Malley, 2011). Co-regulation involved compulsory membership by security firms of professional associations, which conducted their own compliance reviews. While the ICAC report criticised aspects of the system, there was no recommendation to shut it down. The decision was based on an unpublished follow-up review conducted for the government by Deloitte (O'Malley, 2011). The restructure involved significant increases in licence fees to support the Deloitte recommendation for full industry funding of the enlarged regulator – estimated to cost an extra $AU4.7 million per annum. Some licence fees were increased by up to 500 percent, with the industry alleging there was little to show for this (ASIAL, 2010; O'Malley, 2011).

In terms of the fair work inquiry, the Ombudsman appears committed to maintaining the industry compliance program, with the introduction in April 2011 of a *National Security Service Industry Follow Up Campaign 2011*, including the auditing of approximately 600 firms. The continuation of the 2009 campaign up to 30 September 2010 included an additional 40 firms (Fair Work Ombudsman, 2011). This extended the findings to include 277 breaches (up from 194) across 52 percent of audited employers (up from 49%), with over AU$1.1 million in recoveries (up from $AU452,800) on behalf of 1,124 employees (up from 652).

One major overarching problem with the three inquiries examined here is that they remained firmly within in the tradition of crisis-driven ad hoc investigations and piecemeal reform. The limited focus of the inquiries has

meant that other problems in the industry have not been systematically addressed. The most serious of these is the problem of violence associated with crowd controllers in licensed venues. The media continues to report deaths and injuries from assaults and brawls resulting from negligence or aggression on the part of security staff at pubs and clubs (e.g., Carson, 2011; O'Malley, 2011). But there is still no national review of the issue. The security management deficit in licensing systems is another issue not addressed by the inquiries. Repeated scandals around security failures, including at critical infrastructure sites, have highlighted the absence of any requirement for the owners of security firms or the managers of security operations to hold credentials in security management (Prenzler, et al., 2010; see also Button, 2008, in the UK context).

In Australia, security associations have lobbied for many years for better regulation to reduce unfair competition and improve professionalism across all industry sectors (Sarre & Prenzler, 2011). While regulation of the industry is a state and territory responsibility, the cross-jurisdictional nature of the issues requires a much more coordinated response to ensure appropriate standards and national consistency. This requires a more proactive approach by the federal Department of Justice. It also requires regulatory systems with more sophisticated investigative methods, with better measures of the impacts of regulatory strategies, and enhanced research tools to identify gaps and weaknesses in industry standards.

Conclusion

Recent inquiries into the private security industry in Australia involved the use of unprecedented coercive and intrusive investigative techniques. The findings of diverse and serious forms of corruption and criminal conduct oblige a revision – upwards – of the risk profile for the industry. Given that security industry regulation internationally is generally passive and very limited, it would be instructive to see the results of similar inquiries in other locations and to assess how effective other regulatory systems are in countering these problems. Ongoing industry growth means that more and more people are dependent on private providers for protection from crime and violence. It is therefore imperative that governments underwrite integrity and competency in private security with more advanced regulatory systems.

References

ACC (2007). *Annual report 2006-07*. Canberra: Australian Crime Commission.
ACC (2008). *Annual report 2007-08*. Canberra: Australian Crime Commission.
ACC (2009a). *Annual report 2008-09*. Canberra: Australian Crime Commission.
ACC (2009b). *Australian Crime Commission submission to the Parliamentary Joint Committee on the Australian Crime Commission Inquiry into the Adequacy of Aviation and Maritime Security Measures to Combat Serious and Organised crime*. Canberra: Australian Crime Commission.

ACC (2011). Private security industry criminal infiltration. *Crime Profile series.* Retrieved from www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/private-security-industry-criminal-infiltration.

ASIAL (2010). *Response to the proposed changes to the regulation of the NSW security industry.* Australian Security Industry Association Limited. Retrieved from www.securityindustryaward.com.au/Assets/2645/1/Attachment1.pdf

Bayley, D., & Shearing, C. (2001). *The New structure of policing.* Washington, D.C.: National Institute of Justice.

Button, M. & George, B. (2006). Regulation of private security: Models for analysis. In M. Gill, (Ed.), *Handbook of Security*, pp 563-585. Houndmills, Hampshire: Palgrave-Macmillan.

Button, M. (2008). *Doing security.* Basingstoke: Palgrave.

Carson, V. (2011, September 3). Fight clubbing. *Daily Telegraph*, p. 39.

Chambers, G. (2006, September 25). Bikie crime fronts: Gangs in business on Coast. *The Gold Coast Bulletin*, p. 4.

CoESS (2010). *Critical infrastructure security and protection: The Public-private opportunity.* Wemmel, Belgium: CoESS.

Cowan, R. (2010). SLED hammering rogues costs industry. *Security Insider*, Oct/Nov, pp. 34-36.

Fair Work Ombudsman (2010). *National Security Industry Campaign 2009: Report and Recommendations.* Canberra.

Fair Work Ombudsman (2011). *National Security Service Industry Follow Up Campaign 2011.* Retrieved from www.fairwork.gov.au/about-us/audits-and-campaigns/current-campaigns/pages/national.aspx

ICAC (2009). *Report on corruption in the provision and certification of security industry training.* Sydney: Independent Commission Against Corruption.

ICAC (2011). *Plan for Implementation of Recommendations, Operation Columba.* Retrieved from http://www.icac.nsw.gov.au/images/investigations/implementation_plans/Columba/implementation%20plan%20operation%20columba.pdf

Lawler, J. (2009). Protecting government and economies. Address to the *Financial Review Defence Conference 2009.* 23 September, Hilton, Sydney. Retrieved from www.crimecommission.gov.au/media/speeches/2009/090924_john_lawler.htm

Maley, P. (2009, July 6). Criminal groups infiltrate security. *The Australian*, p. 3.

O'Malley, N. (2011, October 1) The Tough business of cleaning up security. *The Sydney Morning Herald*, p. 8.

Office of Consumer and Business Affairs (2004). *Statutes Amendment (Liquor, Gambling and Security Industries) Bill 2004.* Adelaide: Government of South Australia.

Panorama (2008). *Britain's protection racket.* BBC One, 21 January.

Prenzler, T. (2011). The Evolution of police oversight in Australia. *Policing and Society, 21*(3), 284-303.

Prenzler, T., & Sarre, R. (2008a). Developing a risk profile and model regulatory system for the security industry. *Security Journal, 21*(4), 264-277.

Prenzler, T., & Sarre, R. (2008b). Protective security in Australia: Scandal, media Images and reform. *Journal of Policing, Intelligence and Counter-Terrorism, 3*(2), 23-37.

Prenzler, T., Lowden, C., & Sarre, R. (2010). Aviation security issues in Australia post-9/11. *Journal of Policing, Intelligence and Counter-Terrorism, 5*(2), 9-22.

Sarre, R., & Prenzler, T. (2011) *Private security and public interest: Exploring private security trends and directions for reform in the new era of plural policing*. Sydney: Australian Security Industry Association Limited.

Sexton, J. (2012, February 5). Security firm crackdown. *Sunday Telegraph*, p. 27.

Small Arms Survey (2011). *Small arms survey 2011*. Retrieved from www.smallarmssurvey.org/publications/by-type/yearbook/small-arms-survey-2011.html.

van Dijk, J. (2008). *The World of crime.* Thousand Oaks, CA: SAGE

Wheeler, J. (2005). *An Independent review of airport security and policing for the government of Australia*. Canberra: Department of Transport and Regional Services.