Published as Prenzler, T & Sarre, R. (2008) Developing a Risk Profile and Model Regulatory System for the Security Industry. *Security Journal*. 21(4): 264-277.

Developing a Risk Profile and Model Regulatory System for the Security Industry

Tim Prenzler and Rick Sarre

This is a theory and policy paper that examines the security industry in order to develop a model form of regulation with cross-jurisdictional application. It begins by outlining the need for regulation based on a risk profile for conduct and standards of work. Different types of regulation are then reviewed – including civil and criminal law, market forces and self-regulation – elaborating on previous evaluations. The focus is then placed on the need to refine modern systems of government regulation through licensing. The core of these systems involves mandated entry-level competencies (via prescribed training) and disqualifying offences (via criminal history checks). These requirements and many other elements of regulation are, however, currently applied in highly variable ways. The paper emphasises the need for consistent standards and the inclusion of a range of "advanced" regulatory strategies for improved monitoring and professional development. It concludes by proposing a comprehensive model of what has come to be known as "smart regulation" that seeks to balance the needs and interests of the different groups holding a stake in security.

Keywords: security industry; private security; regulation; smart regulation

Introduction

The modern security industry in many countries is characterised by the evolution of increasingly interventionist forms of government control. However, this trend is by no means uniform in character. While some core methods generally apply, the types and degree of intervention remain highly variable, as shown in Button and George's recent (2006) international survey of regulatory systems.

The present paper provides a response to this continued diversity of practice and a response to the apparent lack of adequate regulation in many jurisdictions. It proposes a set of core principles that arguably should apply in any location where security, especially private security, operates. To date, the model has not been articulated in this form and at this level of applied detail. Consideration of its principles should, therefore, be of particular value to policy-makers in government and industry associations. Additionally, the model is designed to fill a gap in the academic literature, which often looks at private security in negative terms and deals with security industry regulation in a fairly abstract light (e.g., Johnston and Shearing, 2003; Zedner, 2006). Social scientists concerned with best practice regulation should seek to present a united front to governments and industry and to speak a common language. The model is, therefore, put forward as a reference point for this aspiration, and is proposed in prescriptive terms as a robust concept with long-term durability and cross-jurisdictional relevance. But it is also designed to encourage more informed and structured debate. Consideration of the model should, moreover, encourage further research that will lead to improvements to it, and its inter-relationships with a variety of regulatory strategies.

The need for regulation: An industry-specific risk profile

The case for government regulation of the security industry – or "special regulation" – has been driven by three factors. The first is a growing recognition of the powers security providers hold over citizens. The second is scandals over security provider misconduct and poor standards. These two factors have been greatly amplified by the third factor: the enormous growth of the industry. The expansion of private security (and associated public sector security services) has been one of the most outstanding features of the development of policing since the 1960s; and the more citizens encounter security personnel and security hardware in their normal routines the more their dependence on these services increases. Consequently, their vulnerability to malpractice also increases (de Waard, 1999).

The expansion of private security also poses a challenge for the principles of equality before the law and equal protection that have been central to the development of modern democratic criminal justice. Again, the larger the size of the private security sector, the more these principles are likely to be challenged, given that private security operates on a competitive profit-making basis with a focus on services that are exclusive to clients. This contrasts sharply with public policing, which is meant to provide free and equal service on the basis of need. One issue for security industry regulation, therefore, involves the extent to which private security firms are required, or empowered, to contribute to the "public good". This could be done through legal obligations – for example, to report crime or to come to the assistance of victims of crime or accidents – or by attaching specific authority and immunities to licences. For example, a particular licence might allow a security provider to access privileged information or to be excused for making a mistake such as a wrongful arrest. To date there seems to be little evidence of governments initiating such provisions except in particular circumstances such as security guard move-on powers in specific locations.

Instead, government licensing has been designed primarily to protect all persons who come in contact with security personnel or who rely on security services in some way. Under property laws, security personnel have enormous power to refuse entry to people and remove them from premises, with some force if necessary (Sarre, 2003). Within limits, they can also engage in surveillance, make enquiries about people's personal details, repossess property, and also make a citizen's arrest. In most cases these powers can be exercised without any special authority (Stenning, 2000). But it means that ordinary people engaging in ordinary activities – such as shopping, doing business, using public transport or going to entertainment venues – can have their freedom and safety severely curtailed by the interventions, or lack of interventions, of security providers.

Like public policing, security has a risk profile that derives from the pressures and opportunities inherent in the work. The following section sets out eleven types of misconduct apparent in security work. These have been abstracted from documented cases revealed by enquiries, media reports, court cases, and practitioner interviews and surveys (for details see, for example, Button and George, 2006; George and Button, 2000; Johnston, 1992; Jones and Newburn, 1998; King and Prenzler, 2003; Sarre and Prenzler, 2005, 1999; Zedner, 2006). The extent of these problems in any one jurisdiction can be extremely difficult to measure. Legally substantiated cases often represent the "the tip of the iceberg", while government enquiries or social science surveys have shown levels of misconduct that have become extensive and long term. What is important to note is that inadequate regulation can lead to any of these problems developing at any time or place given the common nature of security tasks. Some jurisdictions, however, can be more "at risk" than others. Since the collapse of the Soviet Union in 1989, for example, countries in transition to democracy and capitalism have been particularly vulnerable to the growth of unaccountable private security firms, some of which appear more like organised crime cartels than crime protection services (Button and George, 2006).

Areas of misconduct in security work

1. Fraud

Security is an area where clients can have great difficulty monitoring contract conditions. For example, a security patrol firm may undertake to check premises three times per night and agree to leave a business card under a door after each check. Instead of checking three times the guard might only check once and leave three cards. The owner is asleep and unlikely to "watch the watchers" to the extent required to uncover the deception. Fraud like this can also be perpetrated through falsification of data readouts on security patrol checks. In tenders for contracts, security firms may be tempted to understate alarm response times, the number of crews on patrol or their capacity to deal with multiple calls. Security advertisers may also be easily tempted to make exaggerated claims about the effectiveness of their products. For instance, alarms that simply ring when triggered but are not connected to a base rely on residents being on location or neighbours hearing them and deciding to intervene. Sales strategies might downplay these contingencies.

2. Incompetence and poor standards

Security is often characterised as an industry where it is very easy for people to set up business with little capital or ability, or gain employment with few skills or qualifications. The result is that security advice can be ill-informed and security vulnerabilities left unchecked. Security clients, their staff and customers may thus be overly exposed to burglary, theft, fraud, assault, graffiti, vandalism and other crimes. A further effect of poor alarm standards is that enormous amounts of police time (and hence taxpayer funds) are wasted responding to false alarms.

3. Under-award payments and exploitation of security staff

Fraud and poor standards can overlap with tendering that misrepresents labour costs. To fulfil cut-price contracts, employers are then obliged to pay security staff below-award rates. One way to do this is to hire unlicensed staff and pay them "cash-in-hand" to by-pass the taxation system. This is likely to attract unqualified staff and reduce the quality of work. It also leaves staff vulnerable to insecure employment conditions.

4. Corrupt practices

Security providers have varying opportunities for graft. One example is emergency security notifications. Police often develop systems for the fair allocation of work to firms who need to attend a burglary or fire scene to install emergency security. A bribe to police can mean that the firm paying the bribe receives preferential treatment. Bribery can also occur in tendering and security equipment purchases.

5. Information corruption

This is a specific form of corruption that largely involves the enquiry sector, such as private investigators, process servers and debt collectors. This sector requires information on people, such as their whereabouts, assets or contact details. It is easy for these groups to form networks or “rackets” in which public servants, police or private sector employees exchange private information for cash or other benefits. In extreme cases, information illegally obtained is used for extortion or by people wishing to inflict violence on other people.

6. Violence and associated malpractice

Probably the most protracted and widespread problem in security has been that of assaults on patrons, and neglect of patron safety, by security staff, especially in and around licensed premises. The problem can be exacerbated by steroid and other drug abuse by security personnel. Poor management of both security staff and serving practices leads to venues with recurring problems of uncontrollable violence. Guards and crowd controllers are also vulnerable to injury if inadequately trained or equipped.

7. False arrest and detention

Although security providers are often characterised as “prosecution adverse”, they do, at times, perform citizen’s arrests. Store detectives are particularly vulnerable to making arrests without sufficient evidence, and their decisions are rarely challenged by those who are detained. Store detectives and guards may also misrepresent their powers and inappropriately or illegally detain people for questioning without fear of legal admonition.

8. Trespass and invasions of privacy

Searches of bags or coats by guards or store detectives without clear agreement from the subject can amount to trespass or assault. Enquiry agents can also be tempted to engage in criminal and civil trespass and illegal eavesdropping, interference in mail (traditional or electronic) or other breaches of privacy. CCTV control room operators have been caught misusing equipment for their own voyeuristic purposes.

9. Discrimination and harassment

Like police, security providers who deal frequently with the public may be tempted to engage in behaviour that is racist or discriminatory. Particular ethnic minorities might be targeted for eviction, exclusion or arrest. Enquiry agents may also engage in intrusive questioning, threats, defamation, harassment or stalking.

10. Insider crime

Security skills and knowledge of clients' assets and vulnerabilities can be turned against clients. Career criminals and terrorists can access targets and gain specialist skills through employment in security. Cash-in-transit operators know when shipments are being made, the shipment's contents and critical points of vulnerability when robberies are most likely to succeed. A similar scenario applies to burglary and theft. Security guards doing rounds can steal cash and valuables with no witnesses. Enquiry agents may also possess privileged information on clients that can be useful for blackmail.

11. Misuse of weapons

The misuse of firearms, batons and dogs can result in the death or injury of innocent bystanders, offenders or other security officers. Inadequately secured firearms are vulnerable to theft by criminals for use in the commission of offences. Yet historically, security weapons' training has been considered to be perfunctory at best.

In summary, the potential for misconduct, abuse and incompetence in security work remains strong. For this reason regulatory vigilance is important, especially for the protection of third parties – visitors, shoppers, passers-by, commuters – who have not directly contracted or employed security staff but who are highly vulnerable to misconduct or negligence. The breadth and depth of the problems outlined above, however, are difficult to measure.

There are two further arguments that should be noted in favour of regulation in addition to the above risk profiles. One is that the size of the crime problem in most countries makes it imperative that police and private security work more co-operatively. Historically, the two have had limited contact. Indeed, police have tended to have a highly negative view of security personnel, based in large part on the wide disparities in recruitment and training standards (Sarre and Prenzler, 2000). More highly skilled and carefully selected security staff would clear the way, it is argued, for productive public/private partnerships (subject to the limitation, discussed above, of the different philosophies underpinning each service and the risk of mutual corruption). The second argument derives from the escalation of the threat of world terrorism since the attacks on the USA of September 2001. The 9/11 Commission (2004, p 20) estimated that the private sector in the USA controls 85 percent of "critical infrastructure". Moreover, security assessments now recognise that private security services provide a crucial frontline defence against terrorism at major public places, especially airports (for example, BJA, 2005). This has underscored the need for optimal standards in security personnel.

Types of regulation

There have been a number of critiques of different forms of accountability for security – or broad regulatory systems – most notably by Stenning (2000), Sarre and Prenzler (1999) and Zedner (2006). The following section briefly summarises the advantages and limitations of the main forms, organised in terms of the invoking of the civil and criminal law, market forces and self-regulation. The section focuses, finally, on special government regulation.

Civil law

Civil law provides all citizens with a public forum to resolve a grievance. The threat of civil action can be a powerful deterrent to security personnel who might otherwise act negligently, breach contracts, commit assaults or engage in actions that amount to false imprisonment. Where security providers do engage in such acts, a successful civil suit can provide redress to the victims (via the payment of damages) and/or provide specific deterrence (if punitive damages are awarded). Security firms will also want to guard their reputations against the negative publicity that civil legal suits attract.

Case law shows that clients and ordinary citizens have successfully sued security firms on a range of matters; including breach of contract, especially in relation to losses from theft, as well as false arrest. However, initiating civil action is also a high-risk strategy. It may involve embarrassment and further hurt to the plaintiff. There may be extensive legal costs that cannot be recovered, and unsuccessful plaintiffs may be required to pay the costs of the successful defendant. In addition, a defendant firm would usually be able to escape liability if it had out-sourced the work that attracted the legal claim. Moreover, the notorious problem of delays in court processes can also mean that firms found liable may have gone bankrupt are thus unable to compensate the plaintiff.

Civil law also has a very limited reach as a proactive regulatory tool. Civil actions do not identify improper or illegal behaviour by any systematic or open method. The details of cases that are dropped or settled out of court remain largely hidden from the public eye. Many third party victims of abuses may be too poor or ignorant of their rights to take actions, or may themselves have been involved in some illegal behaviour such as vandalism or drug taking. Fraud cases are largely dependent upon victims being in a position to identify deception. However, case studies of fraud in patrol and alarm services show that discovery of the fraudulent conduct often occurs not by clients or government trade practices inspectors, but by internal "whistleblowers" and investigative journalists being courageous and proactive. The same applies to information concerning security violations or invasions of privacy, where persons may not even be aware they have been victimised. In those circumstances, the power of the civil law as a regulatory tool is drastically minimized.

Criminal law

Criminal law provides another potential form of deterrence and redress against improper actions by security staff. Licensed security providers do not have any specific immunity from prosecution. Police can prosecute security providers for crimes such as theft, assault, unauthorised trespass or making threats. This regulatory tool is, however, vulnerable to the well-known limitations of the criminal law as a means of social control. Criminal cases have to be vetted by police and public prosecutors who might not share the same priorities as the victim or might consider the evidence to be insufficient to meet the criminal standard of proof "beyond reasonable doubt". This has been the case where citizens have been injured by bullets from guns discharged by security officers (Sarre, 2003). The circumstances have also made it difficult to prove criminal negligence. Even if prosecutors pursue a case, the decision-making processes of juries and judicial officers add a further layer of hazard. Despite recurring suspicions of insider crimes of theft, robbery and fraud by security operatives, very few cases have been proved to the degree of satisfaction required by criminal law. Alleged assaults by crowd controllers or guards are also extremely difficult to prove in the absence of witnesses or when witnesses are intoxicated.

Sources regularly indicate a systemic problem, but individual prosecutions are vulnerable to collapse.

Market forces

It has been argued that the free market is one of the best mechanisms to make security firms accountable. The theory relies on enforceable contracts operating in tandem with economic competition. Contractors who fail to meet client standards will gain a reputation for being unreliable and will thus lose customers. They will either need to improve their service or withdraw, leaving the market to the quality providers. However, this view assumes clients are fully informed about the performance profile of different security firms, when in fact the market provides few formal mechanisms to ensure this. Suspect performers can stay in business by taking on new clients as they lose dissatisfied clients, especially in a growth market. As well, as outlined in the section above on types of misconduct, intense competition may force margins down so far that companies are strongly motivated to undercut competitors by paying under-award wages and misrepresenting their capacity to fulfil contracts. Continuing clients may also be unaware of how they are being defrauded. In other cases, illegal or unethical conduct – such as assaults or intimidation – may be what the customers think they need in order to manage their security problem. Third parties are then put at risk with little opportunity for redress.

Self-regulation

Industry self-regulation works largely by placing pressure on security firms to join professional associations to obtain their seal of approval as a marketing tool. Associations, often managed by executives with many years experience in their field, do background checks on applicants and respond to complaints. If there is evidence of malpractice then membership will be denied or revoked. Self-regulation is important in showing that the industry has members who are committed to professionalism. Self-regulation can also serve to reduce the burden on taxpayers for government interventions. A major problem, however, is that associations cannot stop non-members from operating. Membership rates vary enormously between sectors and countries, which indicates many firms can succeed on their own. In addition, associations need to keep fees down and usually have a limited capacity to investigate applicants and members. There is little in the way of proactive surveillance or testing. Associations might also be tempted to hide misconduct rather than have their industry publicly impugned or professionally maligned.

Special government regulation

The benefits that flow from the above mechanisms make a case for their retention, while the weaknesses demonstrate the need for the addition of government regulation via industry-specific legislation. There is a fairly standard form of very basic government control of the industry that is followed around the world wherever regulation is introduced (Button and George, 2006; Sarre and Prenzler, 1999). The fundamental requirement is that security providers must hold a licence in order to operate legally. The two main pillars of licensing are:

1. suitability tests, largely through criminal history checks for disqualifying offences (such as theft, fraud or assault in a previous time period, e.g. five or ten years), and

2. minimum pre-entry training requirements (typically between eight hours and five days).

Other requirements likely to be in evidence are:

- an age limit (such as 18 years),
- character references from previous employers or respectable members of the community,
- a first aid qualification,
- a literacy test,
- public liability insurance,
- carrying or displaying a licence while working.

Under this system, licenses are usually issued in categories for specific functions such as guarding, crowd control, private investigation and consulting – with specialist training requirements for each category. To deploy weapons, such as firearms, batons, mace and dogs, a separate licence is normally required. Weapons licence holders often are required to show a specific need for a specific weapon (such as to deter armed robbers and provide self-protection in the cash-in-transit industry).

To retain a licence a security provider must not commit any disqualifying offences. Criminal history checks might be conducted when licences are renewed, such as on an annual basis, or more frequently. Inspectors might carry out checks on firms and operatives to ensure they hold a licence and comply with conditions, such as maintaining an incident log and displaying their licence. The regulatory agency that processes licences will also usually receive and investigate complaints, and make disciplinary decisions. These may include warnings or licence disqualification. Licensing agencies are typically located either within a police or a fair trading (consumer affairs) department.

This is what could be called a “minimal” licensing system. More advanced strategies have been developed in some jurisdictions after it was found that the minimal model was inadequate to reduce misconduct sufficiently (Prenzler, 2006). Advanced strategies can include:

- fingerprinting;
- drug and alcohol tests;
- psychological tests;
- a requirement that licence holders report any charges made against them;
- longer training periods with a wider curriculum;
- pre-licence on-the-job training or experience under a provisional licence;
- auditing of teaching and assessment standards in training institutes;
- widening of licensing to include groups such as “in-house” staff, bodyguards and consultants;
- declarations regarding criminal associates;
- the maintenance of an incident log (for groups such as guards or crowd controllers);

- high security storage of weapons;
- a requirement that operatives return weapons to secure storage after each shift (i.e., not store them at home);
- enforceable codes of conduct that specify particular behaviours (such as times of day when debt collectors can approach debtors).

As noted, special regulation does not mean that other mechanisms become redundant. Government intervention primarily serves as a supplement to the contractual, civil and criminal regulatory mechanisms discussed above. It also needs to engage industry associations to ensure their support and to make use of their expertise. Associations can retain a role in investigations and discipline in a form that is at least partially "co-regulatory". A wider forum of stakeholder groups – like trade unions, consumer advocate groups and client associations – can also be involved (on advisory committees for example) in what has been referred to as "regulatory tri-partism" (Ayres and Braithwaite, 1992). The involvement of such groups can be important to prevent industry and government regulators becoming too close, so that the regulator is inappropriately influenced by the industry ("regulatory capture") and becomes a mere facilitator of corporate security profit-making (Zedner, 2006). Government regulators must remain dominant as the interpreters and enforcers of the public interest, and to do that they must remain independent of the industry.

Challenges for Special Regulation

One of the big attractions of security personnel over police has been the low cost of labour. This cost advantage is threatened, however, by the panoply of government interventions mentioned above such as the imposition of licence fees, longer training periods, entry hurdles and compliance costs (Murray, 1996). It may also be claimed that enhanced government regulation might be perceived (wrongly) as granting specific legal authority to private security officers. However, such arguments against special regulatory intervention can be countered by the need for strong measures to address the risk profile for misconduct. The basic model usually receives very high levels of support from the public, security associations, security managers and operatives (Prenzler, 2004; Prenzler and Hayes, 1999). Opposition from some firms has at times been linked to a discernable interest in maintaining profitable sub-standard services or protecting criminal interests (Button and George, 2006).

One of the biggest problems for the idea of special regulation is the lack of interest from governments. However, government sluggishness does not appear to be clearly linked to philosophies of privatisation or deregulation, but indicative of a general culture of neglect and under-enforcement (Sarre and Prenzler, 2005). Almost all regulatory reform in security has been driven by crisis and scandal, not policy initiatives informed by planning and research. Furthermore, most regulatory systems, once they have been introduced, are also characterised by passivity. They operate mainly by the routine processing of licence applications, some adjudicating of complaints and some on-the-job checks to ensure operatives have licences. Otherwise, there has been very little in the way of active monitoring of security work or research on issues and needs in the industry.

Button and George (2006) have proposed criteria for evaluating regulatory systems around the key concepts of "width" and "depth". "Width" refers to the extent to which licensing covers all security occupations. "Depth" refers to the layers of requirements for licenses (as outlined above). Their survey of systems in Europe, Russia, North America and Australia show enormous variation across these dimensions, but with a tendency overall for licensing to lack breadth and depth. European countries appear to be the most advanced. For example, some countries, such as Spain and Sweden, have basic training requirements in the area of 200 hours; whereas many states in the US still require only eight hours (see also Hemmens, et al, 2001; Jaksa, 2004). The trend internationally is clearly towards more advanced regulation, but progress is slow and halting.

An additional problem, especially within federal systems like the United States and Canada, concerns regulatory fragmentation. Each state or province adopts its own system with the result that firms and individuals within a country may operate on very different standards, with “safe havens” for unscrupulous operators. Regulation of different sectors of security is also often split across government departments, and there is an issue about which area of government is most appropriate overall. Some argue police are inappropriate because of traditional rivalries, mutual corruption, and because business and occupational licensing is not core business for police. Others argue that police are best because of their expertise in criminal intelligence, criminal law and weapons.

Key principles of good security industry regulation

This final section sets out fifteen core “best practice” guidelines for government control of the security industry. They have been developed in order to address the problems and issues outlined above, with a focus on strategies most likely to benefit the widest range of stakeholders (see, for example, Button, Park and Lee, 2006; Button and George, 2006; Davis, et al., 2003; George and Button, 1997; Hyde, 2003; Lister, et al., 2001; Prenzler and Hayes, 1999). In some cases the principles are based on impact research (e.g., Prenzler and Hayes, 1999). In other cases they are more speculative and are more open to testing and modification. They are also formulated with a view to facilitating the highest standards without burdening industry with unnecessary or inhibiting procedures and restrictions. Because many of these strategies are information-driven and focused on measurable outcomes, they are consistent with the notion of “smart regulation” (Gunningham and Grabosky, 1999).

1. Licensing should be *comprehensive*. Licence requirements should cover all occupations involved in security work and reflect the risk-profile across the industry. Regulation should therefore include core groups – such as guards, investigators and crowd controllers – as well as groups often relegated to the margins, such as bodyguards, in-house guards, consultants and advisers, debt collectors, process servers, control room operators, trainers, locksmiths, and hardware and equipment installers. Licensing should cover firms and employees, and be consistent across the private and public sectors. This principle addresses the criterion of width and common aspects of the risk profile across the industry.

2. A regulatory monopoly by *one unit of government administration* will most likely ensure consistent and expert regulation of the whole industry.

3. In federal systems, regulation should be *nationally consistent*. Each jurisdiction should endorse a model national Act and Regulations in order to ensure that all citizens are equally protected from malpractice and to allow firms to operate freely

across state and provincial borders. This may also have the effect of shutting off the possibility of safe havens for unethical security providers.

4. Development and administration of legislation should be *consultative,* with standing industry and stakeholder committees advising the regulatory agencies. This will attract industry support for compliance and make best use of insider expertise. It will also provide a source of continuous feedback about the impact of regulation. A spin-off would be a check on under-enforcement by institutionalising regulatory tri-partism involving all stakeholders such as government and opposition politicians, unions, employers, academics and consumer groups.

5. Regulation should involve exclusion of inappropriate personnel through a *national system of criminal history checks.* The application of disqualifying offences appears to be a key strategy for keeping out persons predisposed to exploit the risk profile of security work, and to ensure media and public confidence in the industry. Disqualifying offences should cover a period of time sufficient to maintain public trust, such as ten years, but not so long in duration that they conflict with the opportunity for rehabilitation of offenders. Checks should be made internationally wherever possible.

6. All licence applicants should be *fingerprinted* in case they are, or become, suspects in criminal cases or have warrants under pseudonyms.

7. *Mandated training standards* should be based on close analysis of security tasks for all licence categories to ensure entry level competence and adequate knowledge of legal powers and responsibilities. The development of competencies should include a broad field of knowledge and skills, such as cultural sensitivity for guards and issues of responsible serving of alcohol for crowd controllers. Dissatisfaction with the system will quickly arise unless training curricula and testing standards are closely tied to the skills and challenges of specific security tasks.

8. Pre-entry qualifications should include a *first-aid certificate*, given that security providers are often frontline emergency response providers.

9. Regulators should help make available opportunities for *in-service training* linked to career path development. This should contribute to professionalism and improved commitment of skilled staff seeking a long-term career.

10. Regulatory systems should include an *enforceable code of conduct* that specifies ethical standards and appropriate behaviours when security providers are faced with ethical dilemmas. Disciplinary tribunals can then use the code when adjudicating complaints or reviewing licence holders’ suitability to work in the industry.

11. Regulators should make use of developments in technology to set up systematic *testing programs for drug and alcohol use* in high-risk areas of security work, such as crowd control work.

12. *Licence fees* should be appropriately set in consultation with industry associations and should not be used simply for revenue-raising. The fee should reflect the true cost

of administering the regulatory system so responsible providers can see value for their licence fee.

13. Consideration should be given to *granting certain licence-holders special powers* to assist them to do their job, especially where the public interest is concerned or where public safety is put at risk. Examples include private investigator access to confidential information and search warrants, greater protections from civil suit for guards and store detectives in arrest situations, and “move-on” powers for crowd controllers outside venues.

14. Regulatory agencies should be *proactive.* Compliance monitoring and complaints investigation need to be vigorous, including innovative approaches such as behavioural observation studies and other forms of research into the conduct of security staff that may be hidden from more traditional forms of inspection. This enlarges the capacity to deter and detect misconduct not prevented by entry screening and complaints and discipline systems.

15. Regulatory agencies should hold a *mission for professionalisation and continuous improvement* with standing research units that conduct policy-oriented research on issues affecting the industry such as safety, weapons deployment, protection against armed robbery, licensed venue management, drug issues for security staff, law reform (including the possibilities of special powers and immunities), and pay and conditions. Another area of research should focus on ensuring that regulatory compliance costs do not unfairly damage business turnover, employment levels and the capacity of the sector to deliver effective crime prevention services. Regulators should also publish annual reports accounting for their mission with detailed statistics on activities and performance measures.

Conclusion

With these key principles in place, and a strong research-based approach to professional development, governments and security industries alike will best be able to manage the balancing act required by those seeking optimal regulation: achieving the highest possible standards in conduct and competency while at the same time providing a minimal cost-burden on security businesses and staff. An ideal regulatory approach must be able to accommodate not only strict enforcement methods (involving, for example, inspection, investigation, prosecution and the imposition of enforceable and deterrent penalties, but also supportive strategies of providing legal support and proactive assistance. To achieve this, regulators need to engage with critics to guard against regulatory failure, especially by way of deference to business interests (Zedner, 2006). Research strategies and the implementation of measurable performance indicators will be crucial to this objective.

References

9/11 Commission. (2004) *Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, D.C.

Ayres, I. and Braithwaite, J. (1992) *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press.

BJA (2005) *Engaging the Private Sector to Promote Homeland Security*. Washington, DC: Bureau of Justice Assistance, Department of Justice.

Button, M. and George, B. (2006) Regulation of Private Security: Models for Analysis. In Gill, M. (ed.) *Handbook of Security*, pp 563-585. Houndmills, Hampshire: Palgrave-Macmillan.

Button, M., Park, H. and Lee, J. (2006) The Private Security Industry in South Korea: A Familiar Tale of Growth, Gaps and the Need for Better Regulation. *Security Journal*. Vol. 10, pp 167-179.

Davis, R., Ortiz, C., Dadush, S., Irish, J., Alvarado, A. and Davis, D. (2003) The Public Accountability of Private Police: Lessons from New York, Johannesburg, and Mexico City. *Policing and Society*. Vol. 13, pp 197-210.

de Waard, J. (1999) The Private Security Industry in International Perspective. *European Journal on Criminal Policy and Research*. Vol. 7, pp 143-174.

George, B. and Button, M. (1997) Private Security Regulation – Lessons from Abroad for the United Kingdom. *International Journal of Risk, Security and Crime Prevention*. Vol. 2, pp 109-21.

George, B. and Button, M. (2000) *Private Security*. Leicester: Perpetuity Press.

Gunningham, N. and Grabosky, P. (1999) *Smart Regulation*. New York: Oxford University Press.

Hemmens, C., Maahs, J., Scarborough, K. and Collins, P. (2001) Watching the Watchmen: State Regulation of Private Security 1982-1998. *Security Journal*. Vol. 14, pp 17-28.

Hyde, D. (2003) The Role of Government in Regulating, Auditing and Facilitating Private Policing in Late Modernity: The Canadian Experience. Paper presented at the *In Search of Security* Conference. Montreal, February.

Jaksa, J. (2004) Is the Guard Trained or Not? The Attempt to Legislate Security Guard Training in Michigan. *Security Journal*. Vol. 17, pp 67-76.

Johnston, L. (1992) *The Rebirth of Private Policing*. London: Routledge.

Johnston, L. and Shearing, C. (2003) *Governing Security*. London: Routledge.

Jones, T. and Newburn, T. (1998) *Private Security and Public Policing*. Oxford: Clarendon.

King, M. and Prenzler, T. (2003) Private Inquiry Agents: Ethical Challenges and Accountability. *Security Journal*. Vol. 16, pp 7-17.

Lister, S., Hadfield, P., Hobbs, D., Winlow, S. (2001) Accounting for Bouncers: Occupational Licensing as a Mechanism for Regulation. *Criminology and Criminal Justice*. Vol. 1, pp 363-384.

Murray, C. (1996) The Case Against Regulation. *International Journal of Risk, Security and Crime Prevention*. Vol. 1, pp 59-62.

Prenzler, T. (2004) Security Industry Report Card. Paper presented to the *National Security Industry Forum*. Australian Security Industry Association Ltd. Melbourne, 20 April.

Prenzler, T. (2006) Growth, Scandal and Reform in the Australian Security Industry, Paper presented to the *Sixth Australasian Security Research Symposium*, Brisbane, 20-21 April.

Prenzler, T. and Hayes, H. (1999) An Evaluation of the Queensland Security Providers Act. *Australian and New Zealand Journal of Criminology*. Vol. 32, pp 79-94.

Sarre, R. (2003) Sources of Private Security Law. *Canberra Law Review*. Vol. 7, pp 109-128

Sarre, R. and Prenzler, T. (1999) The Regulation of Private Policing: Reviewing Mechanisms of Accountability. *Crime Prevention and Community Safety: An International Journal*. Vol. 1, pp 17-28.

Sarre, R. and Prenzler, T. (2000) The Relationship Between Police and Private Security: Models and Future Directions. *International Journal of Comparative and Applied Criminal Justice*. Vol. 24, pp 92-113.

Sarre, R. and Prenzler, T. (2005) *The Law of Private Security in Australia*. Sydney: Thomson LBC.

Stenning, P. (2000) Powers and Accountability of Private Police. *European Journal on Criminal Policy and Research*. Vol. 8, pp 325-352.

Zedner, L. (2006) Liquid Security: Managing the Market for Crime Control. *Criminology and Criminal Justice*. Vol. 6, pp 267-288.