SPECIAL REPORT

ASPI

March 2008 — Issue 14

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Advancing Australian homeland security
Leveraging the private sector

by Anthony Bergin, John Azarias and Don Williams

Executive Director's introduction

The need for security to protect business, as well as the functions of government, has increased over the last decade. There's a greater recognition that security as an enterprise consists of more than the provision of 'guards, guns and gates': it involves the creation of integrated security management systems and mutually supporting relationships across the security market place.

The private sector has been innovative in pursuing research, products and services to actively support our national security efforts. The danger of international terrorism has presented new business opportunities for the security industry. The increased responsibility of the private sector in helping to combat terrorism is producing new technologies that can be applied by public sector decision makers in the future.

By working with the private sector governments can maximise the potential of business to provide creative solutions to our national security requirements. The authors of this *Special Report* reach the sobering judgement, however, that integration of effective security across all sectors of Australia is being hindered by a general lack of mutual understanding and respect between those who define security requirements and rely on security products and services and those who provide these goods and services.

The authors outline a framework that allows users, both public and private, access to a wider spectrum of advanced capability than they could otherwise achieve through current arrangements. They suggest there's a need to develop statements of capabilities to guide the requirements. To enhance communication between users and providers the authors recommend the establishment of focal points in the user and provider communities.

This *Special Report* has been undertaken by ASPI in conjunction with Deloitte. I am very grateful to Deloitte for generously supporting this project. The authors engaged in extensive consultations with security end users and providers. I thank the many officials and industry experts who generously gave their time, information and advice to the authors in the course of preparing this report.

Peter Abigail
Executive Director

Background

Australia must reduce the security threats it faces, protect its critical assets, its public and private sector operations, and recover quickly when disasters strike. No single organisation has the authority or capabilities to respond effectively to the range of challenges faced: homeland security therefore must be provided through a whole-of-nation effort.

Much work has already been implemented in Australia to reduce our vulnerabilities. The development of a secure Australia now faces the problem, however, that industry isn't necessarily well informed enough or committed over the long term to invest in homeland security capability solutions. That's despite the fact that there will be continued demand for sophisticated security technology solutions and security services focused on detection, prevention, response and recovery related to terrorism attacks and other major security or disaster events. This partly reflects an industry perception that the Australian homeland security market is opaque, fragmented and extremely complex, making it very difficult to understand and navigate its complicated dynamics. It's also because without clear guidance provided to industry by government on long-term user needs in this sector, there's not the high degree of business confidence necessary to make longer term investments.[1]

The lack of mutual understanding and respect for each other's knowledge is a key factor that has limited the successful interaction between the sectors. Some providers on-selling security equipment and services lack the detailed knowledge of their products and their correct application. This lack of professionalism on the part of some leads to the impression of security providers as ill-informed. Client organisations (users) that don't understand how security is applied to protect all assets, including reputation, personnel, profits, equipment and information, results in the perception that users are ignorant of the capabilities available. Until mutual education and maturity on both sides is achieved it will be difficult to improve the security market place.

This paper addresses homeland security elements as representing the security continuum: planning, prevention, response and recovery (PPRR). *Homeland security* is taken to include protective security in all forms, as well as response and recovery capabilities, including emergency response and business continuity. The paper proposes several steps to better link Australian providers and users and to develop a more efficient and robust security industry strategy.

Security in Australia is directly linked to the ability to connect efficiently and economically those who need security with those who provide the capability. Currently this free market relationship is not well formed: there's a need for a better dialogue between security users and providers. User unfamiliarity with what's available and the lack of cross-sector interaction is failing to harness the economies of scale and scope that could be offered for long-term security capability development programs. And there's a need for impartial, coordinated and publishable testing of security products and, where possible, services.

There are complex *many-to-many* relationships within the homeland security market place. There's no clear focal point, however, where users and providers meet to discuss capabilities and requirements. There's a general lack of clear and coordinated user statements of what's needed in homeland security capabilities.[2]

In the absence of robustly derived benchmarks supported by appropriate metrics, sound capability judgments are extremely difficult. It should be possible to gauge accurately the resource requirements of each capability, to set agreed capability levels for the various jurisdictions to maintain, to measure performance in those levels, and to determine the additional capability that the government and private sector must maintain in fulfillment of their obligations. Synergies should also be easier to identify and monitor, informing judgments on the migration of capabilities and associated benchmarking responsibilities between the jurisdictions.

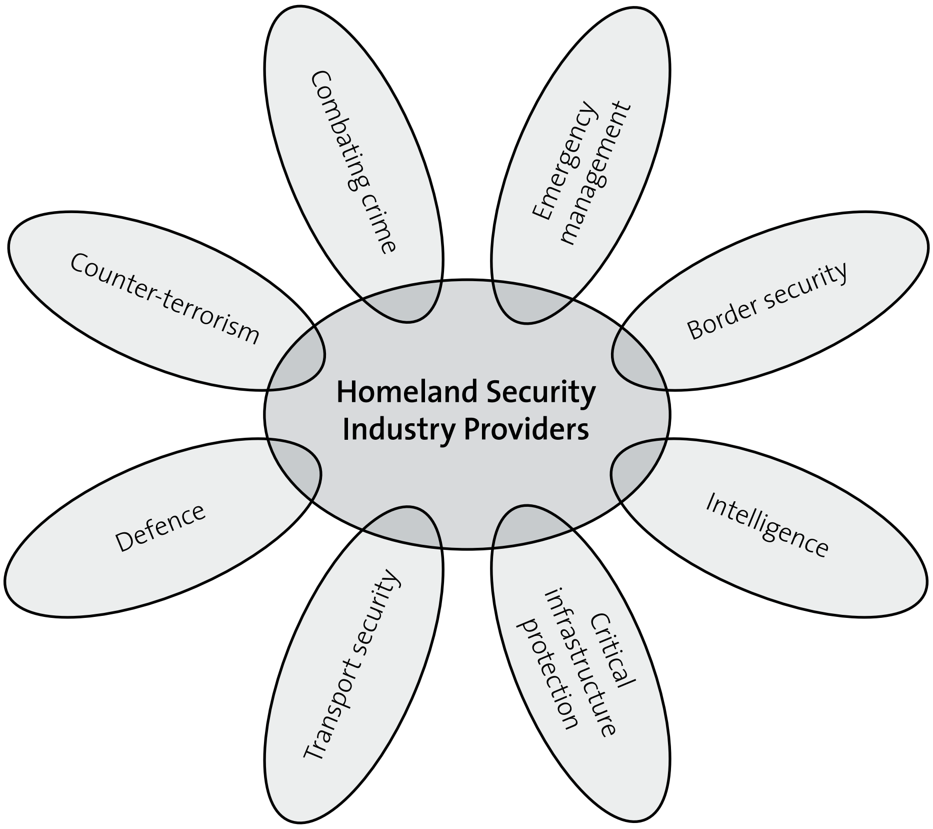
A lack of common understanding of the longer-term capabilities required to protect Australia at all levels carries the risk that users will focus on short-term, organisation-centred solutions, rather than the development and maintenance of coordinated capabilities.

Homeland security market

Australian homeland security products and services aren't just confined to businesses offering products and services such as alarms, baggage tracking devices and guards. Over the last five years, distinct homeland security sectors have evolved in Australia which now have critical mass. They comprise businesses exploiting new technologies to meet both civil and commercial security needs. See figure 1. The most effective of these technologies are those that are capable of being fully deployed across an enterprise in order to minimise vulnerabilities of key areas and/or are capable of being deployed across multiple locations with minimum advance notice.[3]

These businesses are offering solutions that can help detect, prevent, respond and

Figure 1: Scope of homeland security providers



recover from man-made and natural threats to civil and commercial life such as terrorism, attacks on critical infrastructure and natural disasters. Key sectors include border security, credentialing, informatics, data management and situational awareness, cargo and port security, critical infrastructure security and safety, protection and preparedness for chemical, biological, nuclear and radiological events, and disaster response and recovery.

Physical protection systems offered include products such as: access control systems, alarms, monitoring and reporting systems, transport security and cargo tracking, guards, security related IT and software, and emergency response and recovery equipment. *Security services* include security management, consulting related to security policies and procedures, risk analysis, design and integration of security systems, security training and security related research.[4]

The terms *users* and *providers* are adopted in this paper to depict different elements of the security market place. The homeland security market, even more than Defence, is a complex *many-to-many* structure: what differentiates this market is its complexity across the public and private sectors. Every organisation, public and private, has a responsibility to protect the assets and functions with which it has been entrusted by its stakeholders.[5]

Australia is now gradually moving away from segmented security functions towards a more integrated management concept to provide a safe and secure environment: the *resilience* of organisations is now a core concern.[6] The use of risk assessments to identify, analyse and manage security issues has changed the way industry thinks about security. Organisations are bringing together those responsible for a range of disciplines related to protection and recovery. Security technology and services are increasingly being incorporated into government and business operations.

Key change drivers

There are six key change drivers operating here. First, the recognition that security of *function* is as important as security of *assets*. Second, the interdependence of security considerations with safety, compliance, recovery and related disciplines in an enterprise-wide context. Third, the continuing and developing recognition of the threats to higher-value intangible assets such as corporate reputation, market value, and senior executive credibility. Fourth, the recognition of the increased commitment and capability of non-traditional threat agents, such as IT criminals, transnational crime syndicates, terrorists, and special interest protest groups. Fifth, the interdependency of organisations along the supply chain. And finally, recognition of the need to be pro-active with security, rather than developing event-based response measures.

Security users

Users of security can be grouped based on their role in defining and implementing security.

Policy makers: legislators, regulatory bodies and executives responsible for defining security policy.

Operational users: law enforcement and military personnel involved in activities such as bomb disposal, negotiation, hostage rescue; emergency response and recovery personnel; intelligence agencies which use overt and covert surveillance and recording equipment; border protection agencies using a range of surveillance, interdiction, investigative and related equipment; and systems, public and private sector guards, security supervisors, installers and other front line staff.

Security implementers and managers: security, emergency, business continuity, human resources, occupational health and safety, facility, IT, fraud, compliance and other managers responsible for implementing and maintaining security measures.

Security providers

There are a limited number of companies specialising in high-end specialist counter-terrorist, border security and emergency management technologies, with a larger number providing a broader range of homeland security products. In addition, there are security-specific consulting and training companies, as well as elements within larger consultancies offering specialists with security skills.

The provision of security products and services is mainly from the small and medium sized enterprises (SMEs), although some of the larger traditional defence and IT providers have diversified to exploit the new opportunities which homeland security offers. The majority of overseas specialist security equipment providers, such as companies selling bomb disposal robots, are represented by SMEs acting as Australian agents. The larger companies tend to be dedicated to providing security material such as security doors, locks, CCTV, access control systems and similar hardware. Manpower companies range from very small to very large.

Some Australian industry providers see themselves offering homeland security capability solutions, not just delivering a product or service.[7] Providers suggest that, on balance, they possess a much broader view of market trends and user requirements than the users themselves. Providers need to communicate with a wider range of participants whereas providers perceive that users tend to have visibility of only their own and closely related areas. Similarly users are faced with an array of would-be providers with conflicting claims of effectiveness, efficiency and relevance proffering considerable diversity and duplication of products and services. Providers have varying levels of evident competency ranging from highly skilled infrastructure security specialists to merely being importers, retailers and/or delivery agents.

In terms of research providers, the Australian Government has designated *Safeguarding Australia*, including critical infrastructure protection and protecting Australia from terrorism and crime, as one of its research priority areas. The Australian Government funds the *Research Network for a Secure Australia* (RNSA), a multi-disciplinary collaboration established to strengthen Australia's research capacity for protecting critical infrastructure from disasters. The Australian Government promotes collaboration on science and technology research related to terrorism through the *National Security Science and Technology Unit* (NSST) in the Department of Prime Minister and Cabinet (PM&C) and through the *Publicly Funded Agencies' Collaborative Counter-Terrorism Research Program*.[8] There's also the recently established *Australian Research Council Centre of Excellence in Policing and Security* headquartered at Griffith University.

Size of market

The Australian Government is the largest Australian homeland security market in the areas of border control, port and aviation security policy and compliance requirements, embassy/consular protection, intelligence and para-military functions.[9]

The bulk of the government security sector response is at the state level. State and territory governments have significantly increased their spending on security in recent years in specialised policing and response capabilities, infrastructure security and for major special events.

The majority of critical infrastructure owners are now private. The private sector is both a user of security technologies and services, as well as the main provider.

There are hundreds of Australian government departments, agencies and business entities with an Agency Security Advisor responsible for providing a secure environment and compliance with the requirements of the *Commonwealth Protective Security Manual* and the *Information Security Guideline Collection*.[10] Every state, territory and private sector entity requires security.

Speaking at the 2006 Australian Security Industry Association (ASIAL) Conference the then Attorney-General Philip Ruddock valued the Australian security industry at some $4.5 billion. ASIAL predicts that concerns over terrorism and stricter security regulations will generate robust demand for services such as investigations, employee screening and close personal protection of executives and families, training, systems integration and consulting.[11] See Table 1.

A November 2006 report, *The Homeland Security Market*, prepared by the US Civitas Group, estimates that in 2006 US$55 billion was spent worldwide on homeland security measures, with the US market accounting for US$31 billion. Civitas predict a growth rate of between 8 and 10% annually over the next five years and that the US market over the next five years will be in the range of US$140 billion. The Civitas forecast includes spending on elements such as border security, data management and disaster response and recovery.[12] Civitas estimates the Australian homeland security market at slightly over US$1 billion.

The variances in the industry estimates reflect the difficulty of defining both the range of the security industry participants and how their goods and services are costed. Some, such as locks and guards are easily identified, others such as CCTV, risk consultants, and life-safety systems that may have security and other functions are less easily captured in surveys related to security spending. The conclusion is that spending on security related issues in Australia is a multi-billion dollar investment.

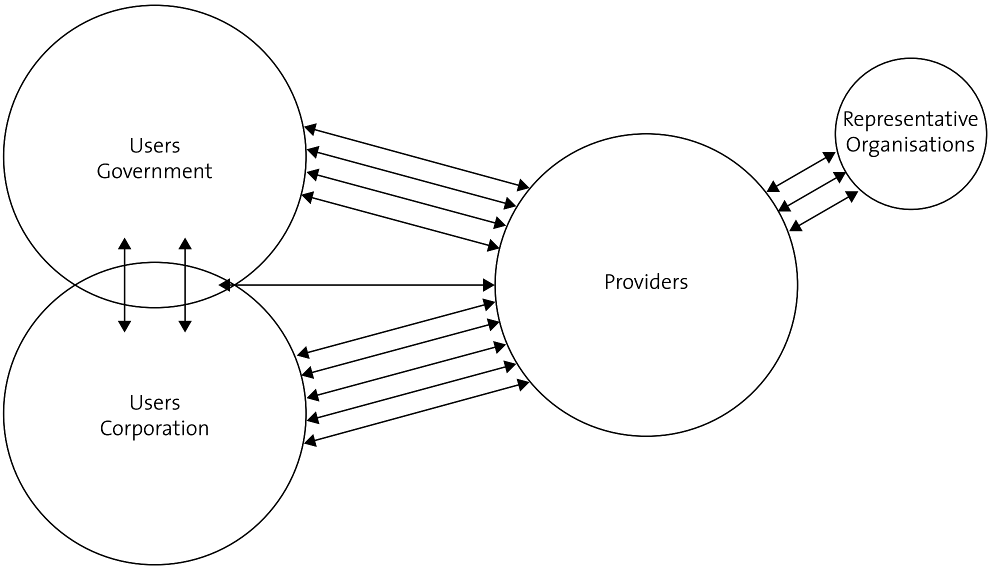
Australian homeland security spending will continue to expand for the foreseeable future driven by risk perceptions of the terrorism threat, the hosting of major

Table 1: ASIAL Security Industry Estimate

Hardware and Electronics	**2007**
Hardware and equipment (alarms, CCTV, access control)	$690,000,000
Installation	$759,000,000
Monitoring	$292,000,000
Other	$343,000,000
Total Hardware and Electronics	**$2,084,000,000**
Total Manpower	**$2,352,000,000**
Including customer service, loss prevention/retail security, concierge/reception desks, corporate risk, investigation services, cash collection, armed escorts, client banking, ATM services, special event security, critical infrastructure protection, passenger screening, mobile patrols, maritime security, crowd control.	
Total Security Industry Estimate	**$4,436,000,000**

Private communication: Bryan de Caires, Chief Executive Officer, ASIAL

Figure 2: User–provider market arrangements



special events, the ongoing need to protect critical infrastructure, the ways in which security is being increasingly integrated into commercial operations, advances in technology, and investor interest in homeland security products that have potential in other commercial markets.

Current challenges

A number of existing public and private structures are involved in managing aspects of homeland security and these are outlined in Annex One of this paper. There are several challenges to achieving better linkages between Australian providers and users in homeland security and developing a more coherent homeland security industry strategy.

Market complexity and fragmentation

Providers need to interface with a vast and complex spectrum of users within the public and private sectors. Their commercial success depends on selling to multiple customers across both sectors. Such widespread interaction is difficult to achieve in an effective manner, especially as it involves operating both with national and state government agencies. It makes the cost of sales and hence of products high and poses problems for small companies with limited marketing resources or access to institutions. Similarly, users may not come to know of solutions best suited to their needs. Hence both providers and users could benefit from better interaction mechanisms.

Figure 2 depicts the existing market arrangements.

Security as a cost

Few organisations wish to spend unnecessarily on security: it indicates that they are vulnerable to loss and are not providing the safest and most secure environment. Security is viewed by most users as a *cost centre*, rather than a *business enhancer.* Often the motivator to spend on security is to comply with legislative, regulatory or insurance requirements or mandated protective limits, such as the Australian Government's *Protective Security Manual* or a perceived need for a reaction to a recent major incident.

The procurement of security products, and in particular consulting services, is often based largely on trust: not surprising given that what's sought is the ability to identify weaknesses in the client's existing security profile and provide reliable solutions. There are also few barriers to those wishing to enter the security market place and users learn to be wary. As a result, the selection of a provider is often based on previous experience and referrals from others, as much as claims of experience, proven performance and suitability. The ability to define and evaluate a security solution is dependent upon the knowledge, experience and commitment of the organisation's security manager (if it has one), and their procurement processes which will focus on the lowest cost bid that complies with their tender specifications. However, how do users determine their specifications or decide trade-offs between competing claims or objectives?

Users often have to decide subjectively between cost or effective capability and coverage. This decision is usually related to the knowledge of the user on what's expected by higher management rather than what's likely to be offered. Unsophisticated users will often select a traditional solution based solely on cost. This may simply be wasted expenditure. There are many examples of catalogue and internet shopping by such buyers. Users are often unfamiliar with the full range or the suitability of what's available. This may lead users to buy ill-chosen solutions or for their greater confidence to buy comprehensive, integrated systems over carefully targeted stand-alone products. The latter favours systems integrators or large entrenched suppliers. Innovative SMEs with good technologies may lose to the larger integrators with broader applications. Similarly providers may offer products and services that are less costly and less suitable, because either they are ill informed and don't fully understand what the user requires or simply to undercut competitors where providers will not be able to properly judge the risks involved.

Just as some users in government and business don't accurately understand the capability of providers, providers don't, in all cases, understand the totality of the users' requirements or the limitations of their products. The result: users and providers in the Australian homeland security sector are now spending considerable time on educating each other on their respective points of view.

Professional indemnity and terrorism

Some Australian professional service providers have raised concerns regarding the allocation of risk between the providers and users, which may expose providers to the cost of losses incurred by acts of terrorism. The Association of Consulting Engineers Australia (ACEA) is the peak industry body representing the business interests of firms providing engineering, technology and management consultancy services. ACEA have expressed concerns that inappropriate risk allocation between users and providers has a deterrent effect, causing providers not to tender or submit non-conforming bids. This occurs where risks are allocated to the supplier that they are unable to control or insure.

'Indemnity' clauses are a feature of professional service contracts and are tools for transferring risk in a contract. ACEA has observed the use of indemnity clauses in some provider contracts to transfer any and all risks of the users loss or damage to the consultant. A key issue here is that a broad indemnity clause it not fault based, raising the prospect that the consultant will be liable for the loss or damage regardless of whether or not the loss/damage was caused by the consultant. Professional indemnity for terrorism is difficult to obtain and very expensive. The use of broad indemnities, because they require the consultant to cover any loss or damage, regardless of negligence, open consultants up to significant liabilities, which are to a great extent uninsurable, including exposure to claims arising from acts of terrorism.[13]

Communication difficulties

There's no obvious portal at the national or state/territory government level or within the corporate sector for those wishing to buy or sell homeland security products and services. Apart from one-on-one meetings, the primary means for providers to present their capabilities to users is at conferences. Regular attendance at such events enables providers to present themselves as reliable and committed participants in the homeland security sector. Security-related conferences often have associated trade shows and some permit presentations of papers from providers. The cost of establishing a trade stand and manning, however, is high for many smaller companies. There's no general homeland security trade show, other than those organised by bodies such as ASIAL[14], the *Security in Government* Conference trade display sponsored by the Protective Security Coordination Centre (PSCC) or the *Safeguarding Australia* conference series.[15]

Providers aren't involved in the Australian Government's Trusted Information Sharing Network (TISN), as they don't fall within the definition of critical infrastructure or the purpose of the Network. Indeed many TISN participants insist on excluding providers from the TISN. Usually government agencies and businesses separately develop their own security requirements. This can result in duplication of effort, expense by users and multiple approaches and costs for providers.[16]

Often the first providers know of a user requirement is when a tender or similar purchase document is released. The security capability is usually drafted in isolation of the providers. The required products and services may not reflect best practice or knowledge of the market's capability, nor be applied with benefit of continuous improvement based on experience. Smaller companies are sometimes disqualified because they don't have sufficient track record or commercial weight; partnering then becomes critical. The release of a procurement document without provider input or specialist expertise suggest the issue is defined in terms of a problem, rather than a solution.

Whilst recognising that each user has specific operating, business, funding and often regulatory, security and safety requirements, generally the key needs for securing the assets and functions of any organisation are fundamentally common. Increased communication between users will assist in developing common capability requirements, consolidated user specifications and standards.[17]

Lack of coordinated capability statements

The lack of a mechanism for providing commercially-neutral guidance from government as to what is required or may be expected is a key issue for providers developing a security related product or service and trying to promote it to the market. Similarly, the lack of a useful non-commercial touchstone with providers inhibits and restricts user analysis of capability needs and possible solutions.

Australia currently lacks a process whereby the capability requirements of homeland security missions are determined and responsibility for developing and maintaining those capabilities is allocated in a verifiable and enforceable manner. This is in spite of some useful work undertaken by the

Defence and industry

Defence spends in excess of $8 billion each year on acquiring, maintaining and supporting military capability.

Defence's capability development process is based on a systematic analysis of the strategic imperative (why), leading to a statement of required capability (what), and then to the delivery of the capability (how). In recent years, the process has undergone significant refinement following the 2003 *Defence Procurement Review*. Key changes include the closer involvement of the government in acquisition approval as well as comprehensive technical risk assessments by the *Defence Science and Technology Organisation* (DSTO).

Defence maintains a close relationship with the industry sectors that provide it with products and services. So much so, that defence industry is now referred to by Defence as its 'fourth arm' and there is a dedicated division within the Defence Materiel Organisation (DMO) to manage the relationship.

Critical to the relationship is transparency of Defence's future purchasing plans. In the case of major capital investment this takes the form of a decade-long *Defence Capability Plan* that articulates capability requirements and gives guidance to industry on timelines for delivery and expected budgets. More generally, Defence routinely gives forward notice of smaller purchases and significant service contracts. On the supply side, a number of Defence industry networks have been established to provide focal points for discussion of issues and requirements: these include the *Australian Industry & Defence Network* (AIDN) that represents defence SMEs, the *Australian Industry Group Defence Council* (AIGDC) that represents larger prime contractors and the broadly based *Australian Business Limited Defence Industry Unit* (ABLDIU).

Defence has an established system for suppliers to offer innovative solutions to Defence requirements, whether stated or not, through the *Defence Unsolicited Proposals Gateway* (DUPG). There's also a *Defence Capability Advisory Forum* (DCAF) where industry can put forward views early in the capability development process and a *Capability Technology Demonstrator Program* (CTD) that helps firms demonstrate the utility of innovative capability solutions. Defence has also recently established the *Rapid Prototyping, Evaluation and Development Program* (RPED), a virtual think tank of defence, industry and research participants to resolve difficult 'bite-sized' problems on a payment for services basis. The RPED group is not engaged on homeland security issues. Each year Defence convenes the *Defence and Industry Conference* (DIC) that brings Defence officials together with more than 1800 delegates to discuss planned Defence spending for equipment and services.

This year the *Defence Future Capability Technology Centre* (DFCTC) will establish a collaborative partnership between universities, science agencies and the defence industry. The DFCTC Program will provide funding of approximately $30 million over seven years to develop technologies to address the future capability needs of the Australian Defence Force.

Capability Steering Group of the National Counter-Terrorism Committee (NCTC).[18]

Some national agencies such as Australian Federal Police (AFP) and Customs have capability development processes, others have informal ones, but most don't have any. At the state level most agencies focus on their own needs: whole-of-state capability mechanisms don't exist.[19] Unlike the Australian Department of Defence (Defence), there aren't formal conduits for industry to put forward its views early in the capability development process.

In response and recovery capabilities, for example, there are significant variations among jurisdictions and the private sector.[20] Statements of capabilities required should include requirements for outcome based system solutions rather than just the delivery of product or a one-off service.[21] At the 2007 *Security in Government Conference*, the Federal Attorney-General underlined this point by noting that while significant technological advances are being made in the area of national security, 'we need to evaluate whether adequate and timely consideration is being given to adopting these technologies. In particular, adopting them in a manner that is in accordance with nationally consistent protocols and practices'.[22]

Some users argue that their security needs must be protected by security classifications. This is true in some instances. In most cases, however, the general requirement is obvious and well known, as are the types of technologies and services that can meet the need. It's usually the detailed application of the products that could be protected. Users stating their capability needs enable providers to concentrate their efforts in development, research and sourcing appropriate solutions. Applying unnecessary barriers to communication between the parties inhibits the ability to identify solutions that may come from non-traditional providers.

Standards and testing

There's a need for standards covering equipment, services, providers, processes, and the security knowledge of users. There are numerous security-related standards. The *National Centre for Security Standards* (NCSS) is developing more.[23] Some corporate users have established in-house standards to augment Australian and other standards or where appropriate standards don't exist.[24]

There's generally a lack of knowledge, by both users and providers, of what Australian standards exist and what other applicable standards could be used.[25] For example, there are international standards and guidelines that could be applicable to Australian public sector site security.[26]

There is a concern by some users that standards may be applied as inflexible minimum measures, restricting the ability to exceed the stated requirement or requiring unnecessary application of resources when not appropriate. Some industry users, for example, have a view that only Australian Security Intelligence Organisation (ASIO) T4[27] approved *Security Construction and Equipment Committee* (SCEC) endorsed consultants could provide security advice to national agencies, even if that advice wasn't about SCEC related matters.[28] Security solely based on a compliance culture can lead to adopting the minimum that's required, rather than measures that will protect all the assets and functions in the most cost-effective way.

Individuals and companies involved in the homeland security market have the opportunity to join relevant professional organisations which have standards for membership, as well as enforceable codes of conduct.

Appropriate standards in equipment, procedures, training and capability enable interoperability across borders and sectors. The Emergency Management Australia (EMA) supported common approach to emergency management is one example of seeking cross-jurisdictional commonality. The inability for a guard to use a security licence in multiple jurisdictions is an example of a barrier to effective homeland security capability.[29]

The establishment in Victoria of a research facility to address major online threats faced by the finance sector and consumers[30] and the Australian Standard *Lexicon of Key Terms used in Security - Creating a Common Language for Security*, currently in draft form, are examples of developing capability standards.

Testing of equipment against national and appropriate overseas standards and combined user requirements is needed so users can understand the effectiveness against agreed metrics and determine the applicability and limitations in their own operating environments. The testing of some equipment on behalf of SCEC doesn't meet this requirement, due to the time taken to test items and the limited range of products of interest to SCEC. Detailed test results aren't published and the requirements of the federal security and construction criteria don't match those of other users.

The National Security Science and Technology Unit (NSST) coordinates scientific research against identified deficiencies in counter-terrorist capabilities. However, this research doesn't include the ability to assess existing technologies. Nor do the capability deficiencies in counter-terrorism necessarily relate to the broader homeland security field.

Next steps

The challenge is to provide a framework that allows users, public and private, access to a wider spectrum of advanced capability than they could otherwise do through the current multiple one-to-one market arrangements. Any approach must be sufficiently flexible to leverage leading edge thinking from industry and the research community. Australian government leadership is the key: it drives the national strategic direction by providing leadership by example and the legislative and regulatory framework to which the market responds.

Produce capability statements

There's a need for clear and concise statements of capability to provide guidance as to the requirements, expectations and desired level of security. Such statements will provide guidance to users and providers.[31] The capability requirements should be drawn from a strategic analysis of what's needed for adequate safety and security: this will pose some challenges in managing the potential classification issues and sensitivities around exposing what might be capability gaps. Given the quick rate of environmental and market change, such statements of capability would need to be very strategic in focus to ensure their continued relevance and usefulness. The challenge at each level would be to bring together common themes and patterns in capabilities and requirements, while identifying and addressing the potentially differing needs of specific users.[32]

Capability statements are required at three levels.

- The national homeland security capability statement should be developed by the *Office of National Security* (ONS).[33]
- At the state/territory level, Premiers' and Chief Ministers' departments could guide departments and agencies, local government, the corporate sector and providers.
- And at the corporate sector level, probably by individual organisations, but possibly

through industry groups, should guide itself, providers and the government as to the corporate sector's expectations for security.

These capability statements should encourage the homeland security sector to invest its resources into long-term Australian projects and provide certainty based on common principles. They would assist in delivering a more competitive and innovative Australian homeland security industry.

Develop capability metrics and testing arrangements

Governments, in conjunction with corporate users and the providers, should develop metrics for security requirements and capabilities against fundamental security and recovery principles for the guidance of security managers in the public and private sectors and also for providers.

Metrics could include: compliance of products and services against standards as well as determining the reasonableness of capability statements against existing or proposed technologies and capabilities.[34] TISN is ideally placed to develop technical standards for security on a non-competitive basis.

Governments should facilitate impartial testing arrangements for emerging technologies relevant to homeland security. They should also oversee and assess the uptake of such technologies. The selection of technologies for testing should be aligned with the stated capability requirements and the results made available to all users.[35]

Establish focal points for users and providers

A key component to improved homeland security across the nation is to reduce the complexity of multiple bilateral arrangements in the market, to enhance communication between users and providers and to allow the maximum number of users access to all those potentially providing relevant technologies and services. This can be achieved by establishing focal points in the user and provider communities.

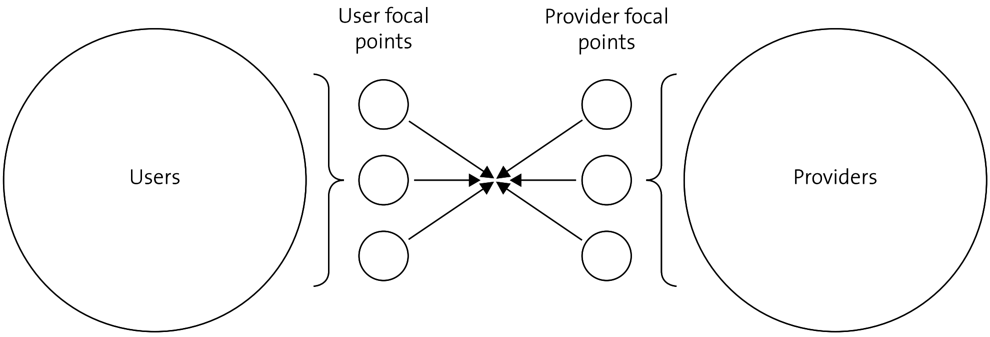
At the national level, a users group should be established that would bring together key Australian government agencies to develop and discuss broad capability requirements, serviced by a relatively small group, and be able to interact with a homeland security providers peak body.[36] Such a group could also consider how to better leverage international engagement to assist Australian companies bidding for contracts in the US market and our region.[37]

In some jurisdictions there is a single public sector user's group that integrates and links homeland security capabilities across state agencies that are involved with protective security, counter-terrorism and emergency response. State homeland security user committees that include relevant departments, counter-terrorism bodies, police and emergency services would help provide a foundation to coordinate, integrate and develop common homeland security capability requirements.

Government user groups must be willing to engage the providers during their deliberations. Private sector users could come together to discuss and promote best practices and to define where there may be areas of common need. The simplest way to achieve this would be through the establishment of a private sector capability group operating within the established TISN framework hosted within the Critical Infrastructure Protection Branch (CIP) of the Attorney-General's Department.[38]

At the state level, users and providers could be assisted in business matching by the *Industry Capability Network Limited (ICNL),* that assists

Figure 3: Preferred user–provider engagement



businesses to maximise opportunities that arise from purchasing requirements from both the government and private sectors. The ICNL should, where appropriate, review the homeland security sector in their jurisdictions with a view to promoting the sector as a major industry.

Private sector providers should form an authoritative voice to represent those involved in the provider community that would have national branches. The AIDN or the AIGDC might be useful models. The industry group could draw from existing industry peak bodies. Similarly universities involved in the federally-funded RNSA and other research institutes could provide an additional reference group.[39]

Such a provider peak body would assist in business matching, provide expert advice to government, market information to providers and discuss long-term user needs. It would be a dedicated channel to allow government to communicate with providers and experts to be a source of advice and direct access to the best capability and technology. It would work on capability gaps and assist government in strengthening its research and development road map for homeland security.

A provider focal point could be the authoritative voice for the homeland security providers community and facilitate effective and efficient communications between providers and public agencies on capabilities, research, services and technologies. It would represent the homeland security industry perspective in the processes of national security capability development. Initial seed funding or secretariat support may be required from government to form such a group. This would also facilitate providing assurance of ethical conduct that does not unfairly advantage or disadvantage any corporation in contravention of the Trade Practices Act and similar legislation.

The primary benefit of identified focal points in both the user and provider communities would be a more resilient Australia, through the ability to more quickly identify and communicate problem solving technologies and to develop and direct research and development priorities against stated capability requirements.

Figure 3 illustrates the suggested approach.

Taken as a package, these suggestions would, if implemented, better integrate users and providers in our homeland security market and enhance the ability of Australia to protect itself at all levels from all hazards.

Annex One

Government and security industry players

Australian Government

The current counter-terrorism framework is based on leadership from the centre: the *National Security Committee of Cabinet* (NSC), and the *Secretaries Committee on National Security* (SCNS).[40]

The *National Counter-Terrorism Committee* (NCTC) is responsible for inter-jurisdictional coordination arrangements. The NCTC has a *Capability Steering Committee* (CSC) that guides the development of Australia's ability to prevent and respond to terrorism.

At the national level, examples of specialist operational *users* include: *Defence* with counter-terrorist response measures (specialist assault, ship-under-way, bomb disposal, and chemical, biological, radiological and nuclear skills); the *Australian Customs Service* (Customs) and *Immigration* with border protection technologies; the *Australian Federal Police* (AFP); *Australian Protective Services* (APS) with physical protection, Air Marshals and Counter-Terrorist First Response at nominated locations; Intelligence agencies; and *Emergency Management Australia* (EMA) responsible for coordinating national responses to incidents and holding the national reserve of emergency equipment.

The *Office of National Security* (ONS) within the Department of the Prime Minister and Cabinet (PM&C) provides central coordinating policy on national security. Located within the ONS is the *National Security Science and Technology Unit* (NSST). It's responsible for providing a national focus on science and technology to enhance Australia's counter-terrorism capabilities. It provides science and technology policy advice for counter-terrorism and divides the capability requirements into three areas: CBRN and explosives; border transport, infrastructure and information security and continuity; and intelligence, surveillance and operations.[41] Companies can register their capabilities with NSST if they believe them to be of interest to the counter-terrorism community. There are opportunities for industry to obtain research funding from the Unit.

The *Protective Security Coordination Centre* (PSCC), within the Attorney-General's Department (AGD), is the central organisation responsible for operational coordination of Australia's counter-terrorism arrangements under the National Counter-Terrorism Plan (NCTP). The PSCC provides policy advice on protective security. It's responsible for technical guidance to the *Agency Security Advisors* in every department and agency primarily through the *Commonwealth Protective Security Manual* (PSM). The PSM provides guidance on protective security, measures mainly related to the protection of government information.[42]

The *Critical Infrastructure Protection (CIP) Branch*, within the Attorney-General's Department, is responsible for the development of Australian government policy relating to the protection of Australia's critical infrastructure and developing and promoting best practice. It provides advice to the owners and operators of defined critical infrastructure on key issues and strategies based on an all-hazards approach: terrorism is only one of the threats against which assets and functions must be protected.

The CIP Branch manages the *Trusted Information Sharing Network* (TISN)[43] which allows the transfer of sensitive information between accredited industry participants. TISN user groups include banking and finance, communications, emergency services, energy, food chain, health, mass gatherings, transport and water services.

A *Critical Infrastructure Advisory Council* (CIAC) provides advice to the Attorney-General on the national approach to protecting critical infrastructure. It consists of representatives from each of the states and territories, the critical infrastructure business sectors, relevant Australian government agencies and the NCTC.

The *Office of Transport Security* (OTS), within the Department of Infrastructure, Transport, Regional Development and Local Government (DITRDLG), provides guidance, mainly to private sector owners and operators of aviation and port transport systems. OTS assesses and enforces compliance against relevant Commonwealth transport security legislation. Surface transport security is administered by the states and territories.

The National Transport Security Working Group (NTSWG) coordinates consistency of security arrangements across all governments in accordance with the COAG Inter-Governmental Agreement on Surface Transport Security.

The *Business-Government Advisory Group on National Security* has met three times to discuss national security, with a focus on the protection of critical infrastructure. Senior leaders across business and government are represented. An Australian Security Intelligence Organisation (ASIO) *Business Liaison Unit* provides a focal point between the private sector and the Australian intelligence community. It produces industry surveys and other general security reporting designed to assist business risk management processes. The unit administers a password access website for business users to disseminate this information to approved private sector participants.

Emergency management

Emergency Management Australia (EMA) is responsible for the coordination of physical emergency and disaster assistance provided by the federal government. The assistance is provided in response to a formal request from the jurisdictions and is coordinated through the *National Emergency Management Coordination Centre* (NEMCC).[44] EMA maintains the *National Disaster Earmark Store* containing a range of emergency and disaster related equipment. The equipment is mainly general stores needed in quantities not normally held by the affected jurisdiction. The age, condition and functionality of the stores are topics that could be addressed under a national capability review.

Security Construction and Equipment Committee

The *Security Construction and Equipment Committee* (SCEC) is a national interdepartmental committee which selects security equipment to meet the physical security needs of the Australian Government. *ASIO (T4)* certifies products as complying with the requirements for protecting Commonwealth assets. T4 trains and endorses, on behalf of SCEC, consultants to certify alarm systems and related hardware.[45]

Industry Capability Network Limited

The *Industry Capability Network Limited* (ICNL) is an Australia and New Zealand wide network that assists businesses to maximise opportunities that arise from purchasing requirements from both the government and private sectors. It assists industry to find new business opportunities by identifying purchasing requirements within the government and private sectors and matches Australian suppliers with buyers, in Australia, New Zealand and overseas. ICNL is independently managed and financially supported by the Commonwealth Department of Resources, Energy and Tourism (DRET). ICNL is part of a network that has twenty-four offices located around Australia and a staff of around eighty technical experts across a number of major industries. ICNL has not addressed, nor at this point is considering addressing, at either national or jurisdictional levels, the homeland security market.[46]

Government panels

Many Australian government agencies have supplier panels or equivalent arrangements for the provision of security products and services. These are let independently of each other and have various, often conflicting, requirements. They are inconsistent in terms of their expectations of security while often having the same providers as panel members. They are expensive and time consuming for providers in terms of response and management. A single panel, or at least a template of stated requirements, would benefit both users and providers. Similar problems exist within the states and territories.

State/territory governments

The bulk of the government sector security and response is at the state level: police negotiators, assault teams, bomb disposal, fire services, ambulance and emergency medical services, state emergency services and the infrastructures to support them. States and territories are also the owners and operators (or the owners of outsourced operation) of major infrastructure: water, power, ports, rail, roads, health services and education.

Each state and territory has a committee, usually chaired by the Premier's or Chief Minister's office, to coordinate counter-terrorist capabilities in accordance with the national CT plan. Each jurisdiction has an emergency management inter-departmental committee structure which coordinates planning, response and seeks national assistance if required and recovery. These committees and their subsidiaries provide similar policy and operational functions as their federal counterparts.[47]

Police forces have crime prevention officers who provide advice on physical security measures related to conventional crime.

Private sector

The majority of critical infrastructure owners are now private. The private sector is both a user of security technologies and services, as well as the main provider. Every private sector body, whether profit making or not, is required to protect its assets and functions. The private sector includes non-government organisations (NGOs), many of which have significant roles in the response and recovery phases of major security incidents. Government owned corporations are generally required to comply with government security processes, as well as private sector practices.

The private sector is focused on achieving the most cost-effective solution, one that provides the required capability over the required time at the minimal acceptable outlay of resources. In some cases, this means that the corporate sector is willing to invest in planning and testing to achieve the best result.

Security managers of thirty-eight of the largest companies in Australia are members of *SecMan*.[48] Membership is by invitation and is limited to senior security professionals in large, national corporations. *SecMan* provides a forum for members to discuss security and related issues in a protected environment.

Security Standards Committee

There are many Australian and international standards, as well as best practice models related to security.[49] In February 2004 *Standards Australia*, a non-government body, launched the *National Centre for Security Standards* (NCSS) to assist Australian businesses meet the challenges posed by a global climate that require organisations to be more vigilant about security.[50] The NCSS is addressing a wide range of security related issues, including those related to protection, risk management, emergency management and recovery.[51]

Representative organisations

There are a wide range of professional and industry organisations that represent homeland security providers such as: *Australian Security Industry Association (ASIAL), ASIS-International*, the *International Association of Emergency Managers* (IAEM) and the *Risk Management Institute of Australia* (RMIA). There are over fifteen organisations representing the professional security consulting sector. The number of representative bodies complicates the challenge of bringing homeland security users and providers together.

Many of these organisations communicate between themselves to share ideas. However, there's no simple way in which they can deal with the Australian Government: there isn't an obvious portal. At the state/territory level some organisations are nominated in legislation as authorised security organisations. These don't, however, represent the entire continuum of homeland security providers.

Some representational bodies are viewed by government users as not much more than political lobby groups, seeking regulatory changes to assist members, rather than representing technology capabilities.

Within the corporate and government sectors (especially in transport) there are examples of precinct-based groups of security and emergency managers. These groups often have established relationships with local police, crime prevention and crime intelligence officers and share information and capabilities, such as overlapping CCTV coverage.

There are some representational groupings within government such as the TISN and the *Security in Government Conference*, sponsored by the PSCC, which bring together Agency Security Advisors (ASAs). Some states have industry consultative bodies, such as the Victorian Security and Continuity Network sector groups. Within Defence, there are networks of Facility Security Officers, responsible to Defence for compliance with Defence security requirements.

Annex Two

US Department of Homeland Security and industry engagement

In 2003, the US created a new security apparatus from scratch. The Department of Homeland Security (DHS) was an amalgamation of twenty-two different agencies, offices and bureaus. The key agencies involved were those with responsibilities for customs and border security, coast guard duties, transport security, immigration and emergency services.

Each agency has responsibility for administering its own finance, personnel, IT, procurement, legal and corporate affairs functions. At the same time, however, a new layer was superimposed which aimed to coordinate those functions across the various agencies. A key function which this new layer sought to coordinate was relations with the private sector.

Individual agencies' day-to-day commercial dealings with the private sector suppliers have continued virtually unchanged since 2003: they are managed on an agency-by-agency basis. The DHS has, however, developed a number of ways of co-ordinating its across-the-board relations with industry:

- the *Office of Policy* facilitates communication between DHS and the private sector, assesses the impact of DHS policies on the private sector and promotes cooperative development of security solutions. Within this Office is the *Business Outreach Group* that presents the private sector's opinions and concerns to the Department and supports outreach efforts of the Department's components.
- the *Directorate of National Protection & Programs* coordinates threat prevention and response regarding the nation's critical infrastructure and key resources between different levels of government and business. The emphasis is on cooperative protection and information sharing, rather than on development of security solutions.
- the *Directorate for Science and Technology* is a dedicated research and development arm which engages the private sector.
- the *Open For Business* website, maintained by DHS, centralises information for the private sector on doing business with DHS. It provides links to contracts, grants, small business opportunities, research and development and contacts.
- the *Office of Small and Disadvantaged Business Utilization* coordinates small business initiatives. These include facilitating information-sharing between federal agencies with the goal of maximising use of small businesses in prime and subcontracts and running small business conferences in different locations.
- the *Mentor-Protégé Program* encourages large business prime contractors firms to provide mutually beneficial developmental assistance to small business. The program is designed to improve the performance of DHS contracts and subcontracts, foster the establishment of long-term business relationships between DHS large prime contractors and small business subcontractors and strengthen subcontracting opportunities and accomplishments at DHS. The stated benefits to DHS include moving from the traditional prime-contractor/subcontractor model to a mentor-protégé relationship model based on mutual agreement, trust, and meaningful business development and an assurance that a

protégé subcontractor will be able to perform.

Congress believes that procurement, among a number of other functions, such as systems engineering and program management, should be carried out at the higher departmental level, that is at the level of the DHS, and it has issued a number of reports and recommendations to that end.

According to a 2006 report by the *Civitas Group,* the homeland security market was once an ill-defined and somewhat unknown sector to many US companies and investors. The report found, however, that the parameters of the US market were now substantially clearer and its potential payoffs more readily determined. It concluded that US government policy priorities are more transparent and that system performance needs have been clarified. The US market had seen less volatility and an increase in long-term investment in and by established and earlier-stage companies. The huge scale of the US market provides its home companies with a strong competitive edge in the global homeland security market.

On its side, the private sector has also sought to achieve stronger coordination. The major suppliers to the Department of Homeland Security have established the *Homeland Security and Defense Business Council* (HSDBC) in Washington DC, a non-profit association of leading companies focused on the homeland security market. The mission of the Council is to advance the agenda of DHS by creating a forum for senior executives among the DHS leading suppliers to engage in open dialogue with senior government officials on homeland security objectives and challenges.

The *US Chamber of Commerce* (CoC) has a Homeland Security Policy Team, which seeks to develop an ongoing, multifaceted program of advocacy, partnership and influence with DHS to create policies that boost the economy, while increasing safety.

The US is home to the world's first incubator focused on security; the *Chesapeake Innovation Center* in Maryland, which aims to create a bridge between buyers and small companies at the forefront of innovation.

Endnotes

1 Similar problems have been identified in the UK and the US homeland security markets. On the UK see Sandra Bell, 'The UK's Risk Management Approach to National Security', *RUSI Journal*, vol 152, no. 3 (June 2007), p.21. For the US see Civitas Group LLC *Homeland Security Market Essential Dynamics and Trends* November 2006, p.7. See Annex Two of this report for an outline of the US approach.

2 An example of what could be provided is the 2006 Council of Australian Governments (COAG) developed National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism. A copy of the code is available at http://www.coag.gov.au/meetings/140706

3 Technologies are most effective when fully integrated into the client's operating environment: therefore development of technologies should relate to the physical, managerial and legal environments in which they will be used. Development of security technologies requires commitment beyond the first generation, as research costs are recovered and on-going development improves the capabilities provided. See Paul Murphy 'Lessons from Lab to Deployment for Security Technology' paper to Research Network for a Secure Australia Conference, University of Melbourne, 28 September 2007.

4 The provision of health security services (human, animal and plant) aren't addressed: they have a different set of providers, markets and means of communicating.

5 The user and supplier divisions are used to differentiate market sectors but there are overlaps. A security guard may be considered a product or a service but uses security equipment and relies on the policies and procedures created by other security providers. Some users are providers: the Australian Government has in-house R&D, consulting and guarding capabilities. Companies that provide security may buy skills and products to protect their business.

6 The definition in the *Draft Australian Lexicon of Key Terms used in Security* is as follows: Resilience is the capacity for complex systems to survive, adapt, evolve and grow in the face of turbulent change. The resilient [nation/organisational] (business) is risk intelligent, flexible and agile.

7 As one industry executive noted to the authors: 'We provide the capabilities that allow the users to provide security'.

8 This brings together four federal agencies: the Commonweatlh Scientific and Industrial Research Organisation (CSIRO), Defence Science and Technology Organisation (DSTO), Australian Nuclear Science and Technology Organisation (ANSTO) and Geoscience Australia, to further their work on counter-terrorism related projects.

9 It should of course be noted that security is an increasingly international issue: the Australian market is related to global economic settings. But the majority of overseas equipment is provided through Australian agents. The manpower and related markets are all domestic in scope and resources, if not ownership. It's the relationship between the local users and providers which dictates the domestic market.

10 The *Information Security Guideline Collection* is issued by the *Defence Signals Directorate* (DSD) and is the basis for communications and related security. It includes the Australian Communications – Electronic Security Instruction 33 (ACSI 33).

11 http://www.asial.com.au/default.asp?page=%2Fnational+and+local+news%2Fmedia+centre%2Fenvironmental+scan+of+the+security+industry. The ASIAL report doesn't include IT security, health security, research, emergency management, response/recovery or some areas of consulting.

12 Civitas Group LLC *Homeland Security Market: Essential Dynamics and Trends,* November 2006, pp. 21 – 24.

13 It should be noted, however, that it's not the Australian Government's intention for risk to be allocated in this way. ACEA has recommended that the consultant's liability be limited to matters within their control and which are insurable. It's not possible of course that providers will be granted some kind of general exemption of responsibility by law from a professional duty for competent advice in regard to terrorism. Liability should involve a demonstrated neglect or failure contrary to reasonable standards of normal professional competency, rather than a simple omission. Experienced providers in the counter-terrorism area usually include disclaimers that clients need to determine their own needs for their own circumstances and restrict their advice to areas of their recognised expertise. It would be incumbent on providers offering services to public sector users to declare the terrorism exclusion on their policies, especially where these services include anti-terrorism services. Users can then be aware of the potential for their own exposure to damages arising from acts of terrorism. It would be wrong for users to assume that their risks are managed if they have contractually passed the terrorism risk to the provider.

14 Security providers don't often present at non-security industry conferences, although this is where many of the potential clients gather. The major Defence and Industry conference each year doesn't include any discussions of the homeland security sector. Whilst the technologies may be applicable across a wide range of user sectors, providers have to decide which sectors they want to target and commit funds to presenting to those users.

15 This conference series is sponsored by the Australian Homeland Security Research Centre (AHSRC) and the RNSA.

16 A clear example emerged in discussions with businesses in preparing this paper. Four large private organisations had independently undertaken a review of CCTV systems within the last two years. Most criteria would appear to be common, with some specific requirements to reflect various operating environments. There should be a common recognition that CCTV/IPTV and recording systems have changed over the last few years and that central trials, based on user and provider input and nationally recognised standards for independent evaluation and publication of results, would have provided a sound basis for the four organisations and many others. There is already a COAG National Code for CCTV Systems for the Mass Passenger Transport Sector for Counter-Terrorism, 2006.

17 An example where there appears to have been no central statement of security requirements and capabilities is the recent construction of buildings specifically for national use such as: Centrelink offices, the National Portrait Gallery, Prime Minister & Cabinet building, Attorney-General's building, Joint Operational Command, AFP Headquarters, and the Australian Crime Commission building. While each of these projects may have different operating requirements there are a number of common security, emergency management, business recovery and related considerations that could have benefited from common

guidance. While the Security Construction and Equipment Committee (SCEC) provides guidance on some physical measures it doesn't address related areas of procedural security, safety, and recovery. Australia does not have a central document along the lines of the US *Site Security Design Guide*. http://www.oca.gsa.gov/perimeter/pdfs/SiteSecurityDesignGuide.pdf

18 The NCTC capability development program incorporates capability fora, workshops, training courses, research and development, exercises and evaluation programs as well as acquisition.

19 That's not to suggest that both formal and informal information sharing doesn't take place amongst state agencies or between jurisdictions.

20 Examples of national level capability statements could include: Australian Government expectations of what minimum security standards should be applied to all organisations in Australia; the purpose and nature of the Emergency Management Australia (EMA) national reserve of emergency stores; the government's intention to replace existing capabilities within the next few years (e.g. secure communications over public phone lines); the development of common visitor accreditation standards for government departments and agencies; assessment of current CCTV/IPTV and related technologies and associated storage, image-search and recovery processes and procedures; the next generation capabilities for identification and access control in both the physical and electronic workplaces; the implications of a return to government-wide, transportable security clearances and the means by which this could be achieved; business continuity standards and technologies for all business and government entities.

21 A system being the integration of the product or service with training, documentation, procedures, maintenance, support and the development of a longer-term relationship than the more traditional buyer/seller exchange.

22 Speech opening SIG Conference, 7 December 2007, Canberra, Attorney-General Robert McClelland.

23 See Annex C of Australian Standards Handbook 167: 2006 Security Risk Management. There are a number of constraints on Standards Australia as a not-for-profit organisation. While there has been agreement on the priorities for new security standards these shouldn't emerge without assistance and resourcing from both business and government in both steering and accelerating the development of standards.

24 ASIAL has contributed to the development of standards, including CCTV and alarms. ASIAL operates a nationally recognised certification program for Certified Monitoring Centres and Manpower. This body is working with Standards Australia to review the Manpower standard to include critical infrastructure protection.

25 For example, the US National Institute of Justice standards for equipment or the ASIS - International *Guidelines for Chief Security Officers*.

26 An example can be found at: http://www.oca.gsa.gov/perimeter/pdfs/SiteSecurityDesignGuide.pdf

27 ASIO T4 certifies products as complying with the requirements for protecting Commonwealth assets.

28 SCEC is a national interdepartmental committee which selects security equipment to meet the physical security needs of the Australian Government. ASIO endorses SCEC consultants who can provide advice on specific equipment topics.

29 The security industry has for the past decade advocated the need to harmonise regulation across the country.

30 Victoria has established a $3.7 million research facility to address major online threats faced by the finance sector and consumers. The Internet Commerce Security Lab is an alliance between the Victorian Government, the University of Ballarat, Westpac and IBM.

31 For some areas in counter-terrorism it may be inappropriate to publish openly capability statements.

32 Each user should be able and willing to inform the market (or selected parts of it) what they intend to achieve in the way of protecting a particular asset capability. Capability requirements will be flexible and evolutionary, but they are better defined and met in conjunction with providers.

33 Follow-on and regular workshops between the peak user/provider bodies would be needed to discuss and understand the issues underlying the broad capability requirements.

34 Metrics will always be easier to develop in some areas than others. Even the COAG sponsored CCTV code of practice, which took significant resource and time to produce, covering just one sector of the security market which was apparently amenable to standardisation, has fairly broad definitions and deliberately leaves a number of issues open to the local decision maker. High standards imply high implementation costs and a code of conduct or standard would need to be mindful of the range of implementation environments which might be required.

35 It should be noted that a technology can be tested against its specification, but that doesn't always tell the user that it will achieve its mission when implemented in their organisation and integrated into the other systems and technologies. For example, a biometric system may appear to work properly in isolation, but unless it's implemented and integrated appropriately it may be ineffective. There's a difference, therefore, between 'Test and Evaluation' (T&E) and 'Operational T&E'. A lot of the current T&E undertaken is sponsored by a particular user agency with their integrated environment as the target. As fitness for purpose testing would need to be performed more or less on individual basis, care would be needed to ensure that the volume of published standards did not become too difficult for suppliers to negotiate.

36 The actual implementation of this proposal would require striking a balance between broad commonalities in government capability requirements and particular, sometimes niche security needs of specific bodies and agencies. A review on the merits of a separate Homeland Security Department is to be concluded by midyear. If such a single agency were created then it would be appropriate that a users group at the national level be serviced from this department.

37 AUSTRADE has of course this as one of their core roles but government can also assist by establishing cooperation agreements with other nations. Australia's 2006 agreement with the US Department of Homeland Security (DHS) on science and technology for homeland security is one example.

The agreement established a formal arrangement to facilitate scientific and technological exchange and interaction on counter-terrorism.

38 As noted earlier, the TISN sector represents the corporate owners of infrastructure and not industry providers.

39 In March 2007 a *Security and Resilience Suppliers Council* was formed in the UK. This initiative owes a great deal to the work of Dr Sandra Bell. See Bell, endnote 1.

40 The structure is outlined in *Protecting Australia Against Terrorism 2006*, Commonwealth of Australia 2006 and the *National Counter-Terrorism Plan* (unclassified version). Both are available on the government's national security website. http://www.nationalsecurity.gov.au

41 There's also a national chemical, biological and radiological improvement program which is jointly administered with EMA and the NSST Unit. It aims to improve Australia's national ability to prevent, prepare and respond to CBR incidents through directed research and development.

42 The PSM contains limited guidance on the protection of staff, physical assets or functionality other than where they relate to government information. The Defence Signals Directorate (DSD) provides guidance on IT and communications security.

43 http://www.tisn.gov.au

44 The EMA NEMCC, PSCC Watch Office and National Security Hotline recently amalgamated their incident notification and government communication functions into the new Attorney-General's Department Coordination Centre (AGDCC). EMA continues to coordinate the Commonwealth response to disasters and emergencies through it's Incident Management Facility (IMF) located at its headquarters in Canberra.

45 http://www.asio.gov.au/Work/Content/EquipmentTesting.aspx

46 http://www.innovation.gov.au/Programsandservices/SupplierAccesstoMajorProjectsSAMP/Pages/IndustryCapabilityNetworkLimited.aspx

47 Descriptions of each state and territory security and emergency management structure may be found at: http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/FA31914A1B115C12CA256FAB001AF573?OpenDocument

48 http://www.secman.com.au

49 A list of security related Standards can be found at Annex C of *Australian Standards Handbook* 167: 2006 Security Risk Management.

50 http://www.standards.org.au/cat.asp?catid=62&ContentId=426&News=1

51 In 2005 NSST signed an agreement with the American National Standards Institute's Homeland Security Standards Panel to assist with transfer of information on common issues.

Acronyms and abbreviations

ABLDIU	Australian Business Limited Defence Industry Unit
ACEA	Association of Consulting Engineers Australia
ADF	Australian Defence Force
AFP	Australian Federal Police
AGD	Attorney-General's Department
AIDN	Australian Industry & Defence Network
AIGDC	Australian industry Group Defence Council
ANSTO	Australian Nuclear Science and Technology Organisation
APS	Australian Protective Services
ASA	Agency Security Advisors
ASIAL	Australian Security Industry Association Ltd
ASIO	Australian Security Intelligence Organisation
BGAGNS	Business–Government Advisory Group on National Security
CBRN	chemical, biological, radiological and nuclear
CIAC	Critical Infrastructure Advisory Council
CIP	Critical Infrastructure Protection Branch, Attorney-General's Dept
COAG	Council of Australian Governments
CoC	US Chamber of Commerce
CSC	Capability Steering Committee, NCTC
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CTD	Capability Technology Demonstrator Program
Customs	Australian Customs Services
DCAF	Defence Capability Advisory Forum
Defence	Australian Department of Defence
DFCTC	Defence Future Capability Technology Centre
DHS	US Department of Homeland Security
DITRDLG	Department of Infrastructure, Transport, Regional Development and Local Government
DMO	Defence Materiel Organisation
DRET	Department of Resources, Energy and Tourism
DSD	Defence Signals Directorate
DSTO	Defence Science and Technology Organisation
DUPG	Defence Unsolicited Proposals Gateway
EMA	Emergency Management Australia
HSDBC	Homeland Security and Defense Business Council
IAEM	International Association of Emergency Managers
ICNL	Industry Capability Network Limited
NCSS	National Centre for Security Standards
NCTC	National Counter-Terrorism Committee
NCTP	National Counter-Terrorism Plan
NEMCC	National Emergency Management Coordination Centre
NGOs	non-government organisations
NSC	National Security Committee of Cabinet
NSST	National Security Science and Technology Unit
NTSWG	National Transport Security Working Group
ONS	Office of National Security
OTS	Office of Transport Security
PM&C	Department of Prime Minister and Cabinet
PPRR	planning, prevention, response and recovery
PSCC	Protective Security Coordination Centre
PSM	Protective Security Manual
RMIA	Risk Management Institute of Australia
RNSA	Research Network for a Secure Australia
RPED	Rapid Prototyping Evaluation and Development Program
SCEC	Security Construction and Equipment Committee
SCNS	Secretaries Committee on National Security
SMEs	small and medium enterprises
T&E	test and evaluation
TISN	Trusted Information Sharing Network

About the Authors

Anthony Bergin is the Director of Research Programs for ASPI. He is responsible for the Institute's research and publications programs on defence and international security issues. Dr Bergin's training is in law and political science. He was most recently an Associate Professor at the University of NSW, Australian Defence Force Academy (ADFA). From 1991–2003 he was the Director of the Australian Defence Studies Centre. Whilst at ADFA, he introduced the first Australian graduate course on Australian homeland security. He has written extensively on a wide range of national security issues and is a regular contributor to the media.

John Azarias is a Senior Partner with Deloitte, specialising in government affairs. He served on the 2006 Defence Management Review, which reviewed the effectiveness and efficiency of the Defence organisation. In 2002 he was commissioned by the Minister for Trade to review Australia's trade and investment links with the European Union. He is a board member of several Chambers of Commerce and holds a Masters qualification in taxation law from the University of Sydney. Mr Azarias is an Associate Member of the Institute of Chartered Accountants.

Don Williams is a Certified Protection Professional and provided professional security consulting services for over twenty years. He holds qualifications in security risk management and project management and is widely published on these subjects. Mr Williams is a member of ASIS International, the Institute of Security Executives and the Institute of Explosives Engineers. He is the Australian chapter director of the International Association of Bomb Technicians and Investigators and an allied member of the Venue Managers' Association.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

About Special Reports

Generally written by ASPI experts, Special Reports are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations. In some instances, material of a more technical nature may appear in this series, where it adds to the understanding of the issue at hand. Special Reports reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au

ASPI gratefully acknowledges the support of Deloitte in the preparation of this *Special Report*.

Deloitte.

TELL A FRIEND ABOUT ASPI

Join Australia's liveliest minds writing today on defence and strategic issues. Each year the Australian Strategic Policy Institute (ASPI) will produce up to ten issues of ***Strategy***, ten shorter ***Strategic Insights*** and a number of ***Special Reports*** on issues of critical importance to Australia and the Asia–Pacific.

Thoughtful, ground-breaking and often controversial, ASPI leads the public debate on defence and security issues.

JOIN ASPI

Name

Position

Company/Organisation

□ **Government** □ **Non-Government**

Address

City **State** **Postcode**

Country

Telephone

Email

SELECT 3 FREE PUBLICATIONS

□ Your Defence Dollar: the 2006–2007 Defence Budget
□ Riding the Wave: the rise of China and options for Australian policy
□ A Big Deal: Australia's future air combat capability
□ Alliance Unleashed: Australia and the US in a new strategic age
□ Future Unknown: The terrorist threat to Australian maritime security
□ Strengthening Our Neighbour: Australia and the Future of PNG
□ Our Failing Neighbour: Australia and the Future of Solomon Islands
□ Living with Giants: Finding Australia's place in a more complex world

INDIVIDUAL	□ 1 year *$199*	□ 2 years *$378*	□ 3 years *$537*
STUDENT*	□ 1 year *$99*	□ 2 years *$188*	□ 3 years *$263*
CORPORATE (Oct 06+)	□ 1 year *$649*	□ 2 years *$1233*	□ 3 years *$1752*

* (STUDENT ID ______________________________)

To join
1) Subscribe online www.aspi.org.au
2) Mail to Level 2, Arts House, 40 Macquarie St, Barton ACT 2600, or
3) Phone (02) 6270 5100 or fax (02) 6273 9566

□ **Cheque** □ **Money Order** □ **Visa** □ **MasterCard** □ **AMEX** □ **Diners**

Payable to Australian Strategic Policy Institute ABN 77 097 369 045

Name on card

Card no.

Expiry Date / **Total Amount $**

Signature

This will be a **TAX INVOICE** for GST purposes when fully completed and payment is made.
Please note specialist publications are not included.