IS A RISK-BASED APPROACH APPROPRIATE WHEN REGULATING MATTERS AFFECTING OUR NATIONAL SECURITY?

Dariel De Sousa*

Tuesday, 11 September 2001 is a day that all of us will remember. Indeed, it is a day that is hard to forget. In eastern USA, it was a clear, cloudless morning. Millions of men and women made their way to work, including to the World Trade Centre's Twin Towers in New York City and to the Pentagon in Virginia. Unfortunately, for many of the workers at the World Trade Centre and at the Pentagon, it would be their last day on earth.

At the beginning of 2001, US counterterrorism officials were receiving frequent but fragmentary reports about threats to national security,[1] including troubling information about a number of those responsible for the 9/11 attacks. By spring, the level of reporting terrorist threats and planned attacks increased dramatically[2] and continued to escalate through the summer months to unprecedented levels.[3] These reports led to repeated advisory notices from US intelligence officials warning of impending al Qaeda attacks. The system was 'blinking red'.[4] However, the individual threats posed by those who were responsible for the attacks were not prioritised, allowing the assailants to navigate airport passport control and security checkpoints without obstruction on that fateful day.[5]

More recently and closer to home, on 15 December 2014, in a café in Martin Place, Sydney, Man Horan Monis – a convicted felon – took café patrons hostage. The siege finally ended after Monis took the lives of two hostages. Monis also lost his life in the cross-fire.[6] At the time of the siege, the general terrorism threat had been ranked as high in Australia – that is, it was assessed that a terrorism threat was likely.[7] Nevertheless, investigations conducted by the Australian Security Intelligence Organisation (**ASIO**), the Australian Federal Police (**AFP**) and the NSW Police Force over a number of years prior to the Martin Place siege did not lead to the conclusion that Monis was a threat to national security.[8]

The factual circumstances and associated analyses surrounding both the 9/11 attacks and the Martin Place siege are complex. It would be clearly inappropriate for someone like me who is not a national security expert to draw conclusions about the possible causes of these tragic events or to speculate about whether and, if so, how these events could have been avoided. Nevertheless, it would be fair to say that both cases raise questions about the identification, assessment, evaluation and response to risk posed to national security. In particular, did the regulatory frameworks applicable to managing the national security threats in each of these cases provide for a risk-based approach? If so, was such an approach adopted and effectively implemented in practice? Was a risk-based approach appropriate?

A fundamental assumption of a risk-based approach to regulation is that a regulator will never have sufficient resources to respond to all alleged breaches or monitor all conduct within its regulated sector. The risk-based approach, therefore, requires the regulator to

* Consultant, Maddocks Lawyers. The author would like to thank Kate Lyle (Graduate Lawyer, Maddocks), Xinyu Zhang (Graduate Lawyer, Maddocks), and Billy Gialamas (Lawyer, Maddocks) for their research assistance. The author would also like to thank Bronwyn Weir (Partner, Maddocks) for her contribution and insights.

determine the tolerability of risks – which risks are palatable, which risks need to be mitigated and which risks need to be eradicated altogether. The consequence of this tolerability assessment is that the regulator will not act on every alleged or actual breach. Rather, resources and effort will be directed towards the areas of greatest risks where the risks are deemed to be intolerable.

Necessarily, a risk-based approach implies that some risks are not worthy of regulatory attention in light of the volume and spectrum of risks faced by the regulator. It is possible (albeit unlikely) that matters that the regulator considers to be low risk could lead to catastrophic events, like the 9/11 attacks and the Martin Place siege. This paper considers whether a risk-based approach is appropriate in matters concerning Australia's national security. It also considers whether it is ever appropriate to relegate matters to low risk status when national security could be at stake.

What is a risk-based approach to regulation?

In essence, a risk-based approach to regulation focuses on risks associated with non-compliance with legal rules, rather than the legal rules themselves. More specifically, the regulator identifies and assesses the risk associated with non-compliance by a particular regulated entity and/or with a particular obligation or group of obligations. Based on this risk assessment, the regulator makes decisions regarding a range of regulatory matters, including:

- whether or not a licence or authorisation to undertake a regulated activity should be granted to a particular regulated entity;
- what monitoring and information-gathering mechanisms are needed and when should they be employed for particular regulated entities and/or regulated activities;
- the targets, focus and regularity of audit and inspection programs;
- the nature and intensity of compliance and enforcement activity warranted for non-compliance with particular obligations within the regulatory framework; and
- the targets and contents of public reporting on compliance and enforcement activity to encourage voluntary compliance.

A risk-based approach to regulation enables a regulator to tailor its regulatory responses so that they are commensurate with the relevant risks. It is particularly useful where the regulator has a large number of regulatory obligations and/or regulated entities to oversee, resourcing is limited and, consequently, prioritisation may be difficult.

A risk-based approach to regulation can yield a number of important benefits, including:

- maximise efficiency by allocating resources to areas of highest risk;
- increase compliance by focusing on areas where the compliance risk is greatest;
- enhance consistency in decision-making because the regulator's response will be dictated by the relative level of risk; and
- reduce compliance burden by minimising regulatory intervention where the risks are relatively low.

Risk in the regulatory context is conventionally defined as the product of the likelihood and the impact of non-compliance. In other words, how likely is it that a particular obligation will be breached and, if that obligation is breached, what will be the consequences?

Assessing the likelihood of non-compliance might include consideration of a regulated entity's compliance history, the strength of any incentives to comply or not to comply, and

the practical difficulty to comply. The impact of non-compliance could include consideration of the risk of physical damage, injury or death, the number of people who could be affected by non-compliance and the political repercussions associated with non-compliance.

Considering likelihood or impact on their own will give a distorted assessment of risk. High probability events may be limited in impact. Similarly high impact, catastrophic events, may be highly unlikely. By combining consideration of probability and impact of non-compliance together allows an overall assessment of risk to be undertaken.

There is a range of factors that affect the risk assessment including:

- *Criteria used to assess likelihood and impact*: Ideally, criteria used to assess likelihood and impact of non-compliance should be linked to the regulatory framework which governs compliance.
- *Comprehensiveness and credibility of information to assess probability and impact*: Inadequate information could potentially lead either to an overly high or low assessment of risk, depending upon how the available information is interpreted.
- *Skills, experience and resources available to those undertaking risk assessment*: The accuracy of a risk assessment may be affected by those responsible for undertaking the risk assessment. Inappropriate skills, irrelevant experience and/or inadequate resources could skew the risk assessment results.
- *Risk appetite of the regulator*: The regulator's tolerance for risk will also affect the risk assessment. Different regulators may have different levels of tolerance for risk. Moreover, a particular regulator's risk appetite could change over time – what was once considered to be a low risk could eventually be regarded as a high risk and vice versa.
- *Harm that is not governed by regulatory framework*: There might be some harm that the regulator does not have power to address, which may lead the regulator to ignore the harm and/or downgrade the associated risk assessment.

Are regulators concerned with issues of national security required to apply a risk-based approach?

The Australian Government's red tape reduction agenda calls for a risk-based approach to regulation[9] so as to encourage regulators to respond to regulatory breaches in a consistent, efficient, transparent and proportionate way. The underlying objective of the red tape reduction agenda is for regulators to reduce the burden on individuals and businesses so as to enhance economic efficiency and productivity.

The *Regulator Performance Framework* (**Framework**) is part of the Government's red tape reduction agenda. The main premise underlying the Framework is that poorly administered regulation can impose unnecessary costs on stakeholders that reduce productivity. It seeks to ensure that regulators undertake their functions with minimum impact to achieve regulatory objectives by requiring Commonwealth regulators to meet certain key performance indicators, including that actions undertaken by regulators are proportionate to the risk being managed. In other words, the Framework requires regulators to apply a risk-based approach to regulation.

Not all regulators and regulatory activities are subject to the Framework. In particular, government entities that have no interaction with the public and/or are 'law enforcement agencies' as defined under the *Crimes Act 1914*[10]are not required to comply with the Framework.[11] Moreover, while licensing, monitoring, compliance and enforcement activities are covered by the Framework (assuming they are undertaken by entities that are subject to

the Framework), providing advice and guidance is only covered if the activity is undertaken in conjunction with one of the other covered regulatory activities.[12]

The carve-outs under the Framework mean that many of the agencies involved in protecting Australia's national security are not covered by the Framework and, therefore, are not required to apply a risk-based approach to regulation. Nevertheless, as explained in the next section of this paper, there are a number of such agencies that have opted to do so.

Application of a risk-based approach to matters affecting Australia's national security

There is a broad range of regulated areas that are designed in whole or in part to protect Australia's national security. These areas can be generally categorised as follows:

- regulation of people;
- regulation of goods;
- regulation of information;
- regulation of infrastructure; and
- regulation of transactions.

Examples for each of these areas are discussed below, including an explanation of how the applicable regulatory framework(s) seeks to protect national security and the way in which a risk-based approach to regulation applies under each framework.

Regulation of people

The Department of Immigration and Border Protection (**DIBP**) regulates the movement of people across Australia's borders under a range of regulatory instruments, including the *Migration Act 1958* (Cth) and the *Migration Regulations 1994* (Cth).

An important objective underlying the regulatory framework is to facilitate entry of genuine travellers to Australia, while preventing entry of those who could threaten national security. Ensuring that this objective is achieved is challenging – passenger movements are expected to grow from just over 33 million in 2012-13 to approximately 50 million by 2020.[13]

The visa system is used to screen people that wish to enter Australia. In summary, all non-citizens are required to hold a valid visa to enter and stay in Australia. With some limited exceptions, non-citizens must apply for and be granted a visa before travelling to Australia.

Under section 29 of the *Migration Act 1958*, the Minister may grant a non-citizen a visa to travel to and enter Australia and, in some cases, to remain in Australia. There is a broad range of visas that may be granted by the Minister. In general terms, the class of visa depends upon the purpose of the visit to Australia.[14]

The criteria for assessment of each class of visa are found in in the *Migration Regulations 1994*. For many visa classes, the criteria include 'public interest criteria'. Among the various public interest criteria are:

> The applicant is not assessed by the Australian Security Intelligence Organisation to be directly or indirectly a risk to security, within the meaning of section 4 of the *Australian Security Intelligence Organisation Act 1979*.[15]

A risk-based approach is used by the DIBP to identify and prevent entry into Australia of people who might pose a threat to Australia's national security.[16] In practice, this approach means that risk is used as the basis for determining whether:

- a visa application should be granted;
- more information should be obtained before a determination about whether or not to grant a visa is made; and
- a visa application should be rejected.

The Movement Alert List (**MAL**), which is administered by DIBP, is a tool used to assess visa applicants, including to determine whether or not those applicants pose or may pose a national security risk. MAL is a computer database that contains profiling information for non-citizens who are or may be of concern and information about travel documents that have been reported lost, stolen or fraudulently altered. There are currently over 700,000 identities of interest listed on MAL.[17]

Some salient points about the application of a risk-based approach to protect national security in the context of Australia's visa system are:

- National security risk associated with visa applications is managed at the federal level.
- For many classes of visa, the regulatory framework specifically requires that national security risk be considered and assessed.
- The assessment of national security risk is used to help determine whether or not a visa application should be granted.
- The risk assessment is primarily focused on the national security risk posed by the applicant for a visa.
- DIBP has an established database (MAL), which is used to record on an ongoing basis risk information about visa applicants and relevant travel documents.

Regulation of goods

Depending upon their use, certain chemicals have the capacity to pose significant threats to Australia's national security. Indeed, of the approximately 40,000 chemicals approved for use in Australia, 96 were identified by the Council of Australian Governments (**COAG**) as requiring attention because of their potential for misuse by terrorists. These are known as chemicals of security concern.[18]

The *Agreement on Australia's National Arrangements for the Management of Security Risks Associated with Chemicals* (**Agreement on Chemical Security Risk**) is an inter-governmental agreement, which seeks to enhance the security of these chemicals. The Agreement establishes a framework to ensure a structured process for the development and implementation of measures to enhance the security of chemicals on an ongoing basis that are proportionate to the assessed risk. The measures are intended to assist security and law enforcement agencies in preventing terrorist acts involving chemicals, while not impeding the legitimate use of chemicals. Under the Agreement on Chemical Security Risk, the Australian Government agrees to work with State and Territory Governments to develop a risk assessment methodology, conduct assessments of risks posed by chemicals, and ensure the adequacy of or implement control measures to address these risks.

The only chemical of security concern that is currently regulated is Security Sensitive Ammonium Nitrate (**SSAN**).[19] It is regulated by States and Territories, in accordance with a 2004 COAG agreement to a national set of principles for regulating SSAN.[20] Ammonium nitrate was considered a priority chemical of concern when this agreement was established because of the ease with which it could previously be obtained and used as an explosive.[21]

A licensing regime applies in the States and Territories for the use, manufacture, storage, transport, supply, import and export of SSAN in the various jurisdictions.[22] The primary aim of these licensing regimes is to ensure that SSAN is only accessible to persons who have demonstrated a legitimate need for the product, are not of security concern and will store and handle the product safely and securely. Applicants for a licence need to undergo background checks by ASIO and the local police before an application can be granted.

The regulatory framework applicable to SSAN is complemented by a non-binding *National Code of Practice for Chemicals of Security Concern* (**Code on Chemicals of Security Concern**). The Code on Chemicals of Security Concern, which was launched in July 2013, encourages businesses to prevent potentially dangerous chemicals finding their way into the hands of terrorists. It applies to 11 chemicals that have been assessed as being particularly high risk.[23]

In summary, the objectives of the Code on Chemicals of Security Concern are to promote effective chemical security management practices throughout the chemical supply chain, and in particular to:

- Protect against the diversion of chemicals for terrorist or criminal purposes.
- Encourage cooperation between businesses and organisations that handle chemicals and law enforcement agencies on chemical security matters.
- Educate and train staff to be alert to warning signs and report suspicious behaviours. To achieve these objectives, the Code on Chemicals of Security Concern provides guidance and information on a range of practical security measures that businesses and individuals can take.[24]

Key points about the application of a risk-based approach to protect national security in the context of the use of dangerous chemicals in Australia are:

- National security risk associated with certain chemical use (ie SSAN) is managed at the State/Territory level. However, businesses are encouraged to manage the national security risk associated with other chemicals under a national code, which is non-binding.
- The regulatory arrangements for the management of chemicals of security concern do not require a risk assessment to be undertaken of chemicals of concern because a risk assessment has already been done of a broad range of chemicals by the Commonwealth in collaboration with the States and Territories.
- Nevertheless, the regulatory framework applicable to SSAN seeks to ensure that risks associated with users and use are appropriately managed through the licensing regime.
- ASIO and local law enforcement bodies assist with the assessment of risk associated with applicants for a SSAN licence through background checks.

Regulation of information

The Internet has become an integral, indispensable part of modern society. Nevertheless, given the ease and speed with which information can be accessed and transmitted around the globe, the Internet also poses important national security challenges.

In November 2009, the Australian Government launched its *Cyber Security Strategy*.[25] As explained in the Strategy, the advent of cyber espionage[26] and, potentially, cyber warfare[27] means that this is an important national security issue.[28] Indeed, in the 2008 National

Security Statement to Parliament, the then Prime Minister Kevin Rudd acknowledged that online threats are among Australia's national security priorities.[29]

The Australian Government defines cyber security as:

> Measures relating to the confidentially, availability and integrity of information that is processed, stored and communicated by electronic or similar means.[30]

Australia's cyber security regulatory framework includes the *Criminal Code Act 1995* (Cth) (as amended by the *Cybercrime Act 2001*), *Telecommunications (Interception and Access) Act 1979* (Cth) and the *Spam Act 2003* (Cth). In summary, under the regulatory framework, unsolicited commercial messages are prohibited. Australia's law enforcement and intelligence agencies are empowered to compel carriers to preserve communication records of persons suspected of cyber-based crimes. In addition, cybercrime offences are identified and include:

- computer intrusions (for example, malicious hacking);
- unauthorised modification of data, including destruction of data;
- denial-of-service (DoS) attacks;
- distributed denial of service (DDoS) attacks using botnets;[31] and
- the creation and distribution of malicious software (for example, viruses,[32] worms,[33] trojans[34]).

The *Cyber Security Strategy* emphasises that, in administering the regulatory framework, Australia must 'apply a risk-based approach to assessing, prioritising and resourcing cyber security activities'.[35] The Australian Government Information Security Manual, which helps to implement this imperative, is used for the risk-based application of information security to information and systems.[36] The Manual explains that 'agencies should use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention as opposed to detection of cyber security incidents'.[37] The Manual also requires that cyber security incidents be registered 'to highlight the nature and frequency of the cyber security incidents so that corrective action can be taken. This information can subsequently be used as input into future security risk assessments '.[38]

The Australian Cyber Security Centre (**ACSC**), which brings together cyber security capabilities across the Department of Defence, the Attorney-General's Department, ASIO, AFP and the Australian Crime Commission, plays an important role in assessing cyber security incidents. The main functions of the ACSC are to:

- raise awareness of cyber security;
- report on the nature and extent of cyber threats;
- encourage reporting of cyber security incidents;
- analyse and investigate cyber threats;
- coordinate national cyber security operations and capability; and
- lead the Government's operational response to cyber incidents.[39]

Important points to note about the application of a risk-based approach to protect national security in the context of cyber security are:

- National security risk associated with the use of the Internet is managed at the federal level under a range of regulatory instruments.
- The requirement to adopt a risk-based approach in relation to cyber security is not embedded in the regulatory framework. However, it is referred to in relevant policy

and procedural documents.

- While there is limited public information available regarding how the risk-based approach is applied in practice, it appears that the risk assessment is focused on the nature and consequences of a cyber security incident, more than the profile of the actual or possible perpetrators of cyber crime.
- ACSC plays an important role in assessing the risk associated with cyber security incidents.

Regulation of infrastructure

Critical infrastructure has been defined by the Australian, State and Territory Governments as the back-bone of the country's economy and includes:

> those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.[40]

The spectrum of critical infrastructure includes energy, water, health, communication and banking infrastructure, including the physical facilities, supply chains and the IT networks.[41] Australia's Critical Infrastructure Resilience Strategy notes that '[t]errorism remains an enduring threat to Australia's national security, and violent extremists continue to seek to target critical infrastructure sectors in Australia and abroad'.[42]

Under the current *Critical Infrastructure Resilience Strategy*, the Australian Government takes a non-regulatory approach to critical infrastructure resilience. The approach assumes that owners and operators of critical infrastructure are usually best placed to assess risks and determine how to respond.[43]

In contrast, in Victoria, a new regulatory framework to ensure the protection of critical infrastructure from national security risks came into effect on 1 July 2015. The framework, which was incorporated into the *Emergency Management Act 2013* (Vic),[44] requires certain 'responsible entities' for the State's most critical infrastructure to demonstrate their assets are resilient to risks, including national security risks.[45]

The framework requires the relevant Minister to assess infrastructure for which that Minister is responsible using the criticality assessment methodology[46] to determine whether that infrastructure is:

- *Significant critical infrastructure*: This category applies to the lowest criticality level of infrastructure. If disrupted, this category of infrastructure would affect the supply of an essential service to, or the economic or social well-being of, a region of Victoria.
- *Major critical infrastructure*: This category applies to the middle criticality level of infrastructure. If disrupted, this category of infrastructure would affect the supply of an essential service to, or the economic or social well-being of, more than one region of Victoria.
- *Vital critical infrastructure*: This category applies to the highest criticality level of infrastructure. If disrupted, this category of infrastructure would affect the supply of an essential service to, or the economic or social well-being of, the whole of Victoria.

The 'Victorian Critical Infrastructure Register' is established under the framework and lists all significant, major and vital critical infrastructure.

Only 'responsible entities' have obligations under the new regime. A 'responsible entity' is defined as the person designated by the Governor as the responsible entity in respect of vital critical infrastructure specified in a Council by Order. Each responsible entity must complete an annual 'Resilience Improvement Cycle' comprising:

- *Statement of Assurance*: This must be completed in accordance with the regulations and guidelines and include:
    - an identification of the emergency risks to the relevant critical infrastructure;
    - specify the emergency risk management actions or activities that the responsible entity proposes to take to address the identified emergency risks; and
    - an attestation that the responsible entity has complied with the new obligations imposed by the Act.
- *Emergency Risk Management Plan:* This must be completed in accordance with the regulations and guidelines and must prepare the vital critical infrastructure for an emergency.
- *Exercises:* The responsible entity must develop, conduct and evaluate an exercise each year to test their capability to plan, prepare for, prevent, respond to or recover from an emergency. The exercise must be developed in consultation with the relevant Minister(s).
- *Audit:* The responsible entity must conduct an independent audit of their emergency risk management processes each year to evaluate the efficiency, effectiveness and appropriateness of the management of risks by the responsible authority. A certificate must be provided to the Minister confirming that the audit has been completed, specifying the outcome of the audit and whether any required actions have been identified.

Some of the main features of the application of a risk-based approach to protect national security in the context of the use of Australia's critical infrastructure are:

- National security risk associated with the use of Australia's critical infrastructure is not regulated at the federal level. However, a regulatory framework has been established in one of Australia's States (ie Victoria).
- A risk-based approach is embedded in Victoria's regulatory framework. The framework requires a 'criticality assessment' to be undertaken for key infrastructure involved in the supply of essential services. An Emergency Risk Management Plan must be implemented by infrastructure owners and operators to ensure resilience to risks, including national security risks.
- While relevant ministers have primary responsibility for assessing the criticality of the infrastructure within their portfolio, the final recommendation considers input from owners and operators of critical infrastructure, and an assessment from the relevant department.[47]

Regulation of transactions

As its title suggests, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) is aimed at combatting money laundering and the financing of terrorism, which could threaten Australia's national security. A person is considered to finance terrorism when they intentionally collect or provide money and are reckless about whether the funds will be used to facilitate or engage in a terrorist act.[48]

In summary, the regulatory framework established under the AML/CTF Act regulates a range of sectors that could be susceptible to money laundering and illicit financing – namely, the financial, gambling, remittance[49] and bullion[50] sectors. The framework applies to the supply

by these sectors of designated services listed in the Act, which include services involving account and deposit-taking, payroll, life insurance, loans, securities and derivatives, betting and gaming.[51] The Australian Transaction Reports and Analysis Centre (**AUSTRAC**) is Australia's AML/CTF regulator and is also the government's specialist financial intelligence unit.

Under the AML/CTF Act regulated entities must meet minimum obligations contained in the Act, including enrolment on AUSTRAC's Reporting Entities Roll.[52] Among other things, reporting entities must submit an annual report which provides AUSTRAC with information about compliance with the AML/CTF Act and associated regulations.[53]

The compliance obligations borne by reporting entities include the obligation to conduct a 'ML/TF' risk assessment.[54] This obligation requires reporting entities to put in place a framework to identify, prioritise, treat, control and monitor ML/TF risk – that is, the risk that the reporting entity or its products or services may be used to facilitate money laundering or terrorism financing. A reporting entity must consider the risk posed by the following factors:

- customer types;
- types of designated services provided;
- how the entity provides its designated services (for examples over-the-counter or online); and
- the foreign jurisdictions within which it operates or conducts business.

Reporting entities must ensure that they know their customers and understand their financial activities.[55] Among other things, reporting entities must have risk-based customer due diligence (**CDD**) procedures in place, which must consider risk associated with each of the following factors:

- customer types;
- customers' sources of funds and wealth;
- nature and purpose of the business relationship;
- control structure of non-individual customers;
- types of designated services the reporting entity provides;
- how the entity provides its designated services (for examples over-the-counter or online); and
- the foreign jurisdictions within which it operates or conducts business.

Most CDD obligations must be completed before the provision of a designated service to a customer, regardless of whether it involves a one-off transaction or involves an ongoing business relationship (eg establishing an account or a loan).

The main aspects regarding the application of a risk-based approach to protect national security in the context of money laundering and the financing of terrorism are:

- National security risk associated with money laundering and the financing of terrorism is managed at the federal level.
- Reporting entities that provide designated services must undertake a risk assessment of their customers as well as the supply of services where money laundering or terrorism financing may be involved.
- The regulatory framework sets out the risk factors that must be considered by reporting entities when undertaking risk assessments.
- AUSTRAC can use the risk assessments provided by reporting entities as an input to its financial intelligence.

Comparison of the application of a risk-based approach to regulation in the national security context

In this paper, I analysed an example from each of the main regulated areas that are designed in whole or in part to protect Australia's national security. A risk-based approach has been adopted in the case of each example, although there are some important differences between the examples considered, namely:

- *Level at which risk regulated*: In some cases, national security risk is regulated at the federal level, whereas in others, it is regulated at the State/Territory level.
- *Body responsible for risk assessment*: In a number of cases, the private sector is required to undertake the risk assessment. However, there were also other cases where the relevant government agency undertakes the risk assessment.
- *Information used for risk assessment*: In many cases, specialist intelligence agencies provide or assess information used for the risk assessment, such as ASIO, AUSTRAC and ACSC.
- *Focus of risk assessment*: In a number of cases, the risk assessment focused on the person involved in a regulated activity. Nevertheless, there were other cases where the risk assessment was focused on a thing (eg infrastructure) or activity (eg financial transactions).
- *Guidance for risk assessment*: In some cases the regulatory framework provided guidance regarding the factors to be considered in undertaking the risk assessment. However, in other cases, the guidance was limited.

Assessment of the appropriateness of applying a risk-based approach to regulation in the national security context

The question of whether a risk-based approach to regulation is appropriate in the national security context needs to be answered by considering the alternative. In particular, what would be a regulator's approach if a risk-based approach is not adopted?

The answer is likely to be that the regulator – confronted with an overwhelming spectrum and volume of national security risks at any given time – must address all risks that come to light, applying the same degree of effort and resources for each one. Under such an approach, some risks will be allocated more resources and effort than warranted, whereas others will be allocated fewer resources and effort than required. The response to the former risks is likely to involve undue regulatory intervention and associated burden for regulated entities while the response to the latter risks could lead to major national security events because the response is not commensurate with the true, underlying risk.

This does not necessarily imply that a risk-based approach will yield perfect results, where responses to national security concerns are always commensurate with the underlying risks. Nevertheless, a risk-based approach has the potential to ensure that resources and effort are dedicated to the areas of highest risk, thereby minimising the likelihood of these types of tragic events. A risk-based approach can also help to entrench consistency, efficiency and fairness in decision-making processes by the regulator. Indeed, a risk-based approach is appropriate - if not critical – in the national security context.

Nevertheless, the ability of a risk-based approach to deliver the touted benefits comes down to design and implementation. A well-designed risk framework, which is supported by expert staff, comprehensive information and effective, sophisticated infrastructure (most particularly, IT systems), will help to ensure that a risk-based approach is capable of delivering.

Effective mechanisms to treat low risk issues will be particularly important in the national security context. As previously mentioned in this paper, a risk-based approach will mean that some low risk issues are tolerated by the regulator. It will be important for national security regulators to be clear and conscious about where the threshold between low and higher risks lie. It is possible that the tolerance for risk among national security regulators is much lower than for other regulators because of the possibility that catastrophic events could eventuate in the national security context.

Assuming that national security regulators have a relatively low tolerance for risk, this may mean that resource requirements are higher than if the tolerance for risk were higher. The need for sophisticated tools to identify and assess low risk issues becomes more pressing so that patterns in low risk issues can be detected and risk escalation can occur, when necessary. The absence of such tools may mean that low risk issues are treated as 'noise' and the ability to detect more systemic risks that might be at play is seriously compromised. The 9/11 attacks and the Martin Place siege are cases in point.

Endnotes

1 National Commission on Terrorist Attacks, *The 9/11 Commission Report*, 2005, 254.
2 Ibid 255.
3 Ibid 256 - 262.
4 Ibid Chapter 8.
5 Ibid 1 - 14.
6 Australian Government, Department of the Prime Minister and Cabinet, *Martin Place Siege, Joint Commonwealth – New South Wales review*, January 2015, Executive Summary, iv.
7 Ibid iv.
8 Ibid v.
9 The *Coalition's Policy to Boost Proactivity and Reduce Regulation*, July 2013; Productivity Commission, *Regulator Audit Framework*, March 2014; *Regulator Performance Framework*, October 2014.
10 Under the *Crimes Act 1914*, 'law enforcement agency' is defined under sections 15GC and 15K to include the Australian Federal Police, the police force of a State or Territory, Customs, the Australian Crime Commission and the Australian Commission for Law Enforcement Integrity, the Australian Tax Office and any other Commonwealth agency set out in the Regulations (presently, there are no such regulations).
11 Australian Government, *Regulator Performance Framework Guidance – Coverage*, 2015.
12 Id.
13 http://www.border.gov.au/about/corporate/information/fact-sheets/70border.
14 For example, visa classes include permanent entry visa, work visa, temporary entry visa, visitor visa and business visa.
15 This criterion is public interest criterion '4002' and is defined in Schedule 4 ('Public interest criteria and related provisions') of the *Migration Regulations 1994*. 'Security' is defined in section 4 of the *Australian Security Intelligence Organisation Act 1974* as: '(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from: (i) espionage; (ii) sabotage; (iii) politically motivated violence; (iv) promotion of communal violence; (v) attacks on Australia's defence system; or (vi) acts of foreign interference; whether directed from, or committed within, Australia or not; and (aa) the protection of Australia's territorial and border integrity from serious threats; and (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa)'.
16 http://www.border.gov.au/about/corporate/information/fact-sheets/70border.
17 http://www.border.gov.au/about/corporate/information/fact-sheets/77mal.
18 https://www.ag.gov.au/NationalSecurity/ChemicalsOfConcern/Pages/default.aspx.
19 Ammonium nitrate can be used to make explosives. Some fertilisers contain high concentrations of ammonium nitrate.
20 http://www.nicnas.gov.au/about-nicnas/regulatory-partners/chemicals-of-security-concern.
21 http://www.nationalsecurity.gov.au/ChemicalSecurity/Pages/default.aspx.
22 See, for example, the Victorian *Dangerous Goods (HCDG) Regulations 2005*.
23 http://www.nationalsecurity.gov.au/ChemicalSecurity/Pages/default.aspx. The 11 high-risk chemicals are: ammonium perchlorate; hydrogen peroxide; nitric acid; nitromethane; potassium chlorate; potassium nitrate; potassium perchlorate; sodium azide; sodium chlorate; sodium nitrate; and sodium perchlorate.
24 Australian Government, *National Code Of Practice For Chemicals Of Security Concern*, 2013, 5.
25 On 27 November 2014, the Prime Minister announced that the Australian Government will undertake a review of Australia's cyber security policies and strategies. The results of the review are due to be delivered in mid-2015.

26 'Cyber espionage' is generally defined as the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organisation.
27 'Cyber warfare' is defined as Internet-based conflict involving politically motivated attacks on information and information systems. Cyberwarfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems.
28 Australian Government, *Cyber Security Strategy: An Overview*, 2009, 5.
29 *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia, the Hon Kevin Rudd MP, 4 December 2008.
30 http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx.
31 A 'botnet' is a network of computers infected with malicious software and controlled as a group without the owners' knowledge.
32 A computer 'virus' enters a computer usually without the knowledge of the operator. While some viruses are mild and only cause messages to appear on the screen, others are destructive and can wipe out the computer's memory.
33 An internet 'worm' is a program that spreads across the internet by replicating itself on computers via their network connections.
34 'Trojans' are malicious programs that perform actions that have not been authorised by the user, including deleting, blocking, modifying or copying data.
35 Australian Government, *Cyber Security Strategy*, 2009, vi.
36 Australian Government, Department of Defence, *Australian Government Information Security Manual – Controls*, 2014, 2.
37 Australian Government, Department of Defence, *Australian Government Information Security Manual – Controls*, 2014, 60.
38 Ibid 63.
39 http://www.asio.gov.au/ASIO-and-National-Security/Partners/The-Australian-Cyber-Security-Centre.html.
40 Australian Government, *Critical Infrastructure Resilience Strategy: Policy Statement*, 2015, 3.
41 http://www.nationalsecurity.gov.au/Informationforbusiness/Pages/TrustedInformationSharingNetwork.aspx.
42 Australian Government, *Critical Infrastructure Resilience Strategy: Policy Statement*, 2015, 2.
43 Ibid. 5.
44 Part 7A of the *Emergency Management Act 2013* deals with 'Critical Infrastructure Resilience'.
45 Victorian Government, Emergency Management Victoria, *Critical Infrastructure Resilience Strategy*, 2015, 4.
46 The *Ministerial Guidelines for Critical Infrastructure Resilience*, 28 May 2015, set out the key principles of the Criticality Assessment Methodology.
47 *Ministerial Guidelines for Critical Infrastructure Resilience*, Critical Assessment Methodology, 28 May 2015, 6.
48 Section 103.1 of the *Criminal Code Act 1995*.
49 Remittance services facilitate the transfer of money or property from a customer in one location and pay an equivalent amount in cash or value to a beneficiary customer in another location, often outside the formal financial and banking system.
50 'Bullion' means gold, silver, platinum or palladium authenticated to a specified fineness in the form of bars, ingots, plates, wafers or other similar mass form; or coins.
51 The designated services are listed in section 6 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.*
52 Part 3A – Reporting Entities Roll, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
53 Part 3 – Reporting obligations, Division 5 – AML/CTF compliance reports, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
54 Chapter 8, Part A of a standard anti-money laundering and counter-terrorism financing (AML/CTF) program, *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)*.
55 http://www.austrac.gov.au/part-b-amlctf-program-customer-due-diligence-procedures.