THE UNIVERSITY OF
NEWCASTLE
AUSTRALIA

Professor Mark G Stewart
Professor of Civil Engineering

Director, Centre for Infrastructure Performance and Reliability
School of Engineering
The University of Newcastle
Callaghan, NSW, 2308, Australia

11 February 2009

Aviation Green Paper
Department of Infrastructure, Transport, Regional Development and Local Government
GPO Box 594
Canberra ACT 2601

Dear Sir/Madam,

Re: Comments on Aviation Green Paper - 'Risk-Based' Approaches to Aviation Security

The Aviation Green Paper states that Australia's aviation security should be 'risk based'. I fully endorse such a philosophy. However, the green paper fails to state what it means by 'risk based' and how such approaches can be implemented in practice for decision-making purposes.

I have significant international expertise in the field of risk assessment for low probability - high consequence events, including recent experience of assessing risks, costs and benefits of Australian and U.S. air marshal programs and hardening of cockpit doors[1]. This work found that hardening of cockpit doors is a very cost-effective security measure, whereas air marshal programs are likely not to be cost-effective.

The definition of 'risk' varies from person to person, but for decision-making a definition often used is the combination of probability of occurrence and consequences (ie. expected losses). A cost-benefit analysis can then be used to assess if the benefits of a new or enhanced aviation security measure (measured in lives saved, damage costs averted) exceed the cost of the security measure. The 'benefits' will depend on:

- threat probability
  - how likely is it that the threat will actually happen?
- consequences
  - how many fatalities? what will be the physical damages, loss of business confidence, etc. as a result of a terrorist attack?
- risk reduction
  - how will a security measure reduce the chance of terrorist attack or reduce its consequences?

This is a probabilistic approach to risk assessment. The Australian Government Office of Best Practice Regulation has recommended the use of cost-benefit assessment for all proposed federal regulations and states that 'the Australian Government is committed to the use of cost-

[1] Mark G. Stewart and John Mueller, A Cost-Benefit and Risk Assessment of Australian Aviation Security Measures, *Security Challenges*, 2008, 4(3): 45-61. Stewart, M.G. and Mueller, J, A Risk and Cost-Benefit and Assessment of U.S. Aviation Security Measures, *Journal of Transportation Security*, 2008, 1(3):143-159.

benefit analysis to assess regulatory proposals to encourage better decision making'[2]. To assist regulatory agencies, the Department of Finance and Administration has published several guides to cost-benefit analysis[3], however, these provide little direct guidance for the assessment of counter-terrorism measures. There is a need for more guidance for assessing the costs and benefits of preventative security measures. The Australian Strategic Policy Institute report '*Risky Business: Measuring the Costs and Benefits of Counter-Terrorism Spending'* (Special Report - Issue 18, November 2008) contains a good overview of some of the key issues.

Much of the Aviation Green Paper devoted to aviation security focuses on the vulnerabilities. There is clearly a need for such thinking as part of any risk assessment. However, it is not helpful to base decisions primarily on intuition, speculation and 'what if' scenarios about what could go wrong. This type of 'worst case' thinking can lead to significant risk averse behaviour and overly alarmist predictions of 'risk' – whereas in reality they are predictions of vulnerability where taken to the extreme 'everything can go wrong'. For example, design of buildings is not based on the worst imaginable cyclone, but a cyclone that is predicted to occur once every one thousand years. This is an example of 'probabilistic thinking' that is the basis for risk-based decision-making for much of our infrastructure, which is particularly relevant for low probability - high consequence events such as terrorism.

The sub-heading on page 76 should be 'identifying and prioritising *risks'*, not 'identifying and prioritising vulnerabilities'. Again, this is indicative of the misplaced emphasis on vulnerabilities.

Instead of dwelling on vulnerabilities, the resilience of citizens and institutions to terrorist threats should also be discussed (as well as threat probability, consequences and risk reduction). Resilience is defined as the ability to adapt to changing circumstances - in this case, to thwart potential terrorist attacks or to recover quickly after an attack. Experience has shown time and time again that citizens and institutions show remarkable resilience to terrorist attack - ie. there is no panic and many services soon return to normal. The concept of resilience reduces the costly and damaging 'flow-on' effects of terrorism considerably.

The Aviation Green Paper states on page 76 that 'The preferred approach is to focus preventative security resources on areas of greatest risk of attack, based on an assessment of this risk...'. It would be beneficial if more explicit guidance about the definition of 'risk' was provided, and that this be defined as incorporating threat probability, consequences, costs and risk reduction in an attempt to compare costs and benefits. If there are 'perceived anomalies in the current security regime' (page 83), then a formal cost-benefit assessment would help ascertain the risk that these anomalies pose, and in identifying which anomalies need (or do not need) preventative security resources.

The need to consider mass casualty attacks at airports (page 84) is important. However, it should be kept in mind that mass casualty attacks can occur in many places, such as sporting events, shopping centres, theatres, etc. The statistics also show that bomb and gunmen attacks at airport terminals are very low - the probability of terrorist attack on an individual airport terminal in South-East Asia is less than 0.002 (one chance in 500) per year.[4] The number of fatalities in these

[2] *Best Practice Regulation Handbook*, Office of Best Practice Regulation, Australian Government, Canberra, August 2007, p. 115.

[3] *Handbook of Cost-Benefit Analysis*, Department of Finance and Administration, Australian Government, Canberra, January 2006. *Introduction to Cost-Benefit Analysis and Alternative Evaluation Methodologies*, Department of Finance and Administration, Australian Government, Canberra, January 2006.

[4] Calculation based on Terrorist Incident Database, Memorial Institute for the Prevention of Terrorism, 1998-2007.

attacks was limited to 24. So while airports may be vulnerable to mass casualty attacks (as are many items of infrastructure), the probability of an attack is low, there is little evidence of mass casualties in the past and so the risk is likely to be low. There may well be specific threat information that would change (increase) the threat probability, but a baseline level of risk is still needed as a basis for any such increase. If the risk is low, then it may be that the cost of providing extra protective measures for terminal security should be deferred, and perhaps directed to other preventative security measures where the 'benefits' of such expenditure are higher. These are considerations needed for a risk-based approach.

Summary

Any approach to aviation security should consider not only vulnerabilities, but resilience as a key factor mitigating the likelihood and consequences of terrorist attack. An assessment of costs and benefits needs to consider threat probability, consequences, costs and risk reduction. A rational approach is based on 'probabilistic thinking', and not on alarmist predictions of 'worst case' threats, vulnerabilities and consequences.

Thank you for this opportunity to comment on the Aviation Green Paper. More information about this submission can be provided if required.

Yours sincerely

Professor Mark G Stewart
Director, Centre for Infrastructure Performance and Reliability

T +61 2 4921 6027
F +61 2 4921 6991
Mark.Stewart@newcastle.edu.au