Submission No 118

Inquiry into potential reforms of National Security Legislation

Organisation: Department of Broadband, Communications and the Digital Economy

Australian Government

Department of Broadband,
Communications and the Digital Economy

Public Submission to the

Parliamentary Joint Committee on Intelligence and Security

Inquiry into potential reforms of National Security Legislation

August 2012

Department of Broadband, Communications and the Digital Economy 38 Sydney Avenue, Forrest, Canberra ACT 2603 Australia website http://www.dbcde.gov.au

The Department of Broadband, Communications and the Digital Economy (DBCDE) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's inquiry into potential reforms of national security legislation. The department supports the aims of the inquiry in recognition of the growing importance of telecommunications infrastructure and security to the digital economy. The department wishes to provide brief comments on the proposed amendments to the *Telecommunications Act 1997* (see Terms of Reference, paragraph 16) to address security and resilience risks posed to the telecommunications sector.

The department does not propose to comment on the security aspects of the proposals per se, as these are best dealt with by other agencies. However, the department is generally supportive of balanced efforts to lift the security review and management capabilities of agencies and carriers alike; and to update relevant legislation including that which is the responsibility of the Minister for Broadband, Communications and the Digital Economy.

Australia's future economic prosperity and well-being is closely tied to its ability to maximise the benefits of the digital economy. The rollout of the National Broadband Network (NBN) is expected to bring substantial economic and social benefits. Improved access to health and aged care, education, online government service delivery and greater commercial opportunities will make life simpler, save time and drive economic growth.

Communications technologies are raising the quality of services delivered by the economy and lowering their cost. In 2012, IBIS World found that enhancements in information technology through high-speed ubiquitous broadband can return Australia to its long-term average productivity growth of 1.7 per cent by 2020. In 2011 Deloitte Access Economics estimated that the direct contribution of the internet to the Australian economy was approximately $50 billion a year, projected to grow to over $70 billion a year by 2016. In 2012, KPMG estimated that cloud computing would increase the size of the Australian economy by $3.32 billion a year after ten years.

A key aspect of realising these benefits is ensuring the confidentiality, availability and integrity of the telecommunications networks that underpin Australia's digital economy. Government, business and consumers reasonably expect that their communications and information are secure and protected, and that threats to our telecommunications infrastructure are taken seriously. Failure to manage security risks and threats can have far reaching consequences for consumer, business, government and the whole economy.

Australia's telecommunications industry has a long history of working cooperatively with security and law enforcement agencies to ensure our telecommunications infrastructure remains secure and protected. Government and industry regularly consult on emerging security issues through industry forums and dialogue. Experience has demonstrated that early engagement is critical in effectively managing security concerns while minimising the impacts and cost of mitigation for industry.

While these informal arrangements have worked well in the past, they are straining to keep up with the changing security environment. The economy's reliance on telecommunications has significantly increased the security risks and threats. Security agencies are reporting that cyber espionage is being "used against Australia on a massive scale to extract confidential information from Governments, the private sector and ordinary individuals"[1]. The Defence Signals Directorate has publically reported that "more than 65 per cent of intrusions (it is seeing) in Australia are economically motivated."[2] Similarly cybercrime is a significant and growing problem. The Australian Federal Police estimate that Australian losses are in excess of $1 billion a year.[3]

The structural changes in the market and the move to internet technologies are also challenging the effectiveness of the current informal arrangements. The Government has introduced, for good policy reasons, an open and competitive framework that is encouraging a high degree of service innovation and competitiveness. Ease of entry is encouraging many new players to enter the market. The telecommunications industry is delivering services in new and innovative ways. For example, 27 per cent of Australian organisations have outsourced hosting of their data centre infrastructure to third-party service providers and 43 per cent of Australian enterprises use some form of cloud computing. The competitive framework encourages faster speeds to market for new services.[4] However, new players may be less aware of security risks, Australian Government perspectives or the informal arrangements for engaging with security agencies. This raises the risk that they may engage with security agencies late in the decision making process. A more formal approach would assist industry to be more aware of its obligations and ensure it has the necessary information to address security concerns during development of products and services. Incentives to support this and ensure it is a common cost amongst equivalent entities would be an important element in an otherwise highly commercial environment.

Given the changing security environment and the evolving telecommunications market, it is appropriate that Government strengthens and formalises the cooperation arrangements through a legislative framework. Such a framework would provide benefits to both industry and security agencies by setting clear expectations for network security and structured engagement. The framework would also strengthen the basis for information sharing between industry and agencies on security matters.

The department notes, however, that there is a need to balance the impact and costs to industry of such a regulatory approach with security outcomes. Telecommunications and related converging services are a high-growth and often essential input into Australian businesses. The NBN investment by the Government is intended to give Australian business a global competitive advantage in moving service delivery online. All other things being equal, the least cost approach to enhanced security arrangements is most likely to match the aspiration behind the regulatory structure in the future telecommunications and converging markets. This would include – indeed,

[1] Security in Government Conference 2011 Senior Executive Breakfast, Tuesday 5 July Presentation - Director-General of Security, Australian Security Intelligence Organisation
[2] DSD, http://www.dsd.gov.au/speeches/20120416_ddcis_old_crows_assn.htm
[3] Australian Federal Police, 2010, Referenced in Cyber White Paper – Discussion Paper
[4] ACMA Communications Report, 2010-11, Ch 5

may perhaps be most important in – light touch involvement in the key differentiating factors between vendors, for example network design.

The conceptual approach most likely to work, and which as far as possible DBCDE expects to see in the final new structure, is one which emphasises effective security outcomes rather than imposes technical judgements, in a market where information asymmetry tends to see regulators struggle with fast-changing technology.