



[www.ddsi.org](http://www.ddsi.org)

## National Dependability Policy Environments

### AUSTRALIA

Report Version: Final  
Report Preparation Date: 1 November 2002  
Classification: Public  
Preparation led by: RAND Europe (NL)

Contract Start Date: 1 June 2001      Duration: 18 months  
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);  
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);  
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community  
under the "Information Society Technology"  
Programme (1998-2002)

**Table of Contents**

Overview of the Country’s Information Infrastructure ..... 3

Main ICT Regulatory and Legal Developments ..... 5

Assessment of Phenomena Undermining Dependability ..... 10

Government Initiatives Aimed at Tackling Cyber-Security ..... 11

Industry and Other Non-Government Activities Related to Dependability ..... 14

Public-Private Partnerships ..... 14

Research and Development ..... 16

### ***Overview of the Country's Information Infrastructure***

Australia has developed software niches in the IT services areas. The Customer Relationship Management (CRM) software and Knowledge Management (KM) software markets are growing in excess of 40 percent annually. In 1998, the CRM sector was valued at US\$20 million (EUR 22,988,506) and in 1999 at US\$38 million (EUR 43,678,160). Observers predict that there will be approximately 44 percent compound growth over the next five years, given that most companies have yet to implement a CRM solution.<sup>1</sup>

Production of information technology and telecommunications (IT and T) equipment has fallen by 27 percent over the past three years, from A\$4.8 billion (EUR 2.807 billion) worth of products in 1995-96 to A\$3.5 billion (EUR 2.047 billion) in 1998-99. Over the same period, imports of IT and T equipment have shot upward by 21 percent, from A\$8.9 billion (EUR 5.204 billion) in 1995-96 to A\$10.7 billion (EUR 6.257 billion) in 1998-99. For the year 1999, the Australian hardware market showed limited growth. In the local market, about 2 million PCs are exported annually, of which 500,000 are destined for the consumer desktop sector. At the retail level, the market for Personal Digital Assistants (PDAs), or Hand Held Devices, is growing strongly, especially for those devices that connect to the Internet. Australia has abundant local and regional manufacturers of wireless hardware and equipments to meet this demand. In the year 2000, the total size of the hardware market was US\$5.97 billion (EUR 6.86 billion), total local production was US\$1.98 billion (EUR 2.27 billion), total exports amounted to US\$1.35 billion (EUR 1.55 billion), and imports amounted to US\$5.35 billion (EUR 6.14 billion).

In comparison to the local hardware market, which is dominated by large multinational firms with industry-standardised products, the software market is relatively insignificant mainly due to the lack of indigenous sources of venture capital.

There has been a great emphasis on IT outsourcing in Australia, with both government and private companies engaging in large contracts. Revenue from the Australian outsourcing market was A\$1.3 billion (EUR 0.76 billion) in 1997, and projections for 2004 push the amount up to A\$5.3 billion (EUR 3.1 billion), or an average growth rate of 16 percent. This growth has been boosted by large outsourcing contracts from both government and private companies, which had a kick-start in 1998 when revenue from outsourcing rose dramatically by 70 percent, to A\$2.2 billion (EUR 1.28 billion). In 2000, the total size of the software market was US\$4 billion (EUR 4.6 billion), total local production was US\$2.3 billion (EUR 2.64 billion), total exports amounted to US\$300 million (EUR 344,827,586), and imports amounted to US\$2 billion (EUR 2.3 billion).

Data collected by the Australian Bureau of Statistics (ABS) indicate that Australia's performance and growth in terms of uptake of Internet technology and Internet infrastructure is strong and poised to continue in years to come. In 2000, there were 264 ISPs and approximately 7.77 million Internet users.<sup>2</sup> Forty-six percent of the population in 2001 had Internet access at home via a PC; forty percent of households had access to the Internet via a PC. Sixty-five percent of Australians over the age of 16 had access to the Internet, while 68 percent of Australian households had a mobile phone.

---

<sup>1</sup> Software market report: [www.acs.org.au/news/oz150501.htm](http://www.acs.org.au/news/oz150501.htm)

<sup>2</sup> Management of Global Information Technology (MOGIT): Information Technology Landscape in Nations – Australia. American University: [www.american.edu/carmel/dp2143a/australia.htm](http://www.american.edu/carmel/dp2143a/australia.htm) (visited on 21 May 2002)

The 2001 "NOIE Current State of Play" report, published by the National Office of the Information Economy (NOIE), showed that 56 percent of Australian businesses and 50 percent of Australian households were connected to the Internet in June 2001.<sup>3</sup>

Adults are intensive users of the Internet from home or work. Of the adults accessing the Internet from home, an estimated 85 percent did so once a week or more (30 percent daily, 26 percent 2-6 times a week, and 25 percent once a week). Of the adults accessing the Internet from work, nearly 80 percent did so once a week or more (47 percent daily, 21 percent 2-6 times a week, and 12 percent once a week).

By June 2000, an estimated 56 percent of employing businesses were connected to the Internet (an increase of 93 percent since June 1998). Very small businesses (employing 1-4 persons) had the highest proportional increase, an estimated 108 percent (from 24 to 50 percent). Between June 1998 and June 2000, the number of businesses going on-line that employed 5-19 people increased from 32 percent to 65 percent. Those businesses that employed 20-99 people and also going on-line rose from 56 to 83 percent.

At the end of December 2000, there were 696 ISPs operating in Australia, providing access to 3.92 million subscribers. Eighty-seven percent of these subscribers were households and 97 percent of subscribers were using dial-up access. In addition, there were some 2,394 Points of Presence (POPs) and 515,740 Internet access lines giving a ratio of 7.6 subscribers per access line. There are currently 718 ISPs active in Australia, with 2,244 POPs, 521,645 access lines, and 3.849 million subscribers.

The telecommunications sector is one of the fastest-growing and dynamic areas of the economy.<sup>4</sup> The transmission infrastructure includes five major fibre-optic cables that provide most of the bandwidth; and five satellite systems that have coverage footprints over Australia and neighbouring Asian and South Pacific countries. The annual revenue is in the order of A\$36 billion (EUR 21 billion), which represents 5.5 percent of Australia's Gross Domestic Product. Annual investment in telecommunications infrastructure is approximately A\$5 billion (EUR 2.92 billion). Industry growth is approximately 13 percent *per annum*. In the year 2000, there were 71 licensed carriers, 47 major information service providers, and six major operators of carrier infrastructure.

There were 10.7 million main line telephones in use in 2000. Telstra, the former monopoly operator, owns over 1,300 local exchanges, 3.1 million km worth of fibre-optic cabling. There were over 80,000 pay telephones and over nine million mobile telephones in 2000. There were over 9,000 mobile telephone base stations and over one million ISDN lines in service. Nine-hundred thousand people were connected to cable television services in 2000.<sup>5</sup>

A NOIE study into the economic impact of e-commerce to the year 2016 concluded that Australia's economy and those of all States are projected to have a higher level of output of between 0.8 to 3.6 percent by the year 2010 and 30 out of the 57 regions can expect an increase in regional output and employment as a result of e-commerce. M-commerce (transactions via mobile devices), is also under way in Australia. Mobile phone providers offer WAP-based text communications to their subscribers and currently estimate that nine-ten percent of mobile owners use data services.

---

<sup>3</sup> [www.noie.gov.au/projects/information\\_economy/researchandanalysis/ie\\_stats/CSOP\\_June2001/index.htm](http://www.noie.gov.au/projects/information_economy/researchandanalysis/ie_stats/CSOP_June2001/index.htm) (visited on 21 May 2002)

<sup>4</sup> 2001 Report Card Telecommunications: [www.infrastructurereportcard.org.au/2001/index.htm](http://www.infrastructurereportcard.org.au/2001/index.htm)

<sup>5</sup> Sources: Australian Telecommunications User Group: [www.atug.com.au](http://www.atug.com.au) (visited on 28 January 2002)

### ***Main ICT Regulatory and Legal Developments***

Telecommunications access in Australia's regional and rural areas has been an issue for some time,<sup>6</sup> and is one of several currently being addressed by the Federal Government. Such problems require subsidisation of carriers for the provision of reasonable bandwidth, access to the internet, and satisfactory mobile telephone coverage. According to a survey conducted by the Australian Bureau of Statistics, 71 percent of schools reported that they had a student-to-computer ratio of 15:1 or less, with 40 percent having ten or fewer students per computer.

An appraisal conducted by the Australian Information Industry Association (AIIA) predicts that the 2001 demand for skilled IT workers will be an increase of 29,700; between 2002-2003, a further increase of 58,000; and between 2004-2005, an additional rise of 81,800. The total predicted increase for the next five years is 50 percent greater than the total of all Australian university graduates for last year. There is also a constant debate as to whether Australia is facing a net gain or loss of IT professionals.<sup>7</sup>

The Australian Computer Society (ACS) released a report by Professor John W. Houghton at the Centre for Strategic Economic Studies (CSES) in May 2001 (Houghton, 2001). This report talks about the IT landscape of Australia. Houghton attempts to quantify the impact of the Information, Computers, and Telecommunications (ICT) industry in Australia, showing that up to 680,000 Australians work in ICT and related jobs. Industry income is around A\$100 billion (EUR 58.48 billion) a year, increasing at more than 17 percent per year. Australians are amongst the most intensive users of ICTs in the world (4th in the OECD for ICT to GDP), though ICT-producing industries make a smaller contribution in Australia than in other developed countries.

Other sources of government investment funds include *Building on Information Technology Strength* (BITS), a program propelled by the Federal government.<sup>8</sup> In total, there are six incubators in the country. The size of investment is from A\$50,000 (EUR 29,240) to A\$450,000 (EUR 263,158).

The Internet Access Fund is intended to stimulate Internet service delivery in regional and rural Australia in a manner that will enhance the commercial, competitive roll-out of these services. The major priority for projects supported under this fund will be the provision of untimed local call Internet access, or at least the equivalent where traditional dial-up access is not feasible, at reasonable price and bandwidth. Another project is NOIE's Information Technology On-line (ITOL) project, a Commonwealth Government grants program administered by NOIE, which is designed to accelerate the national adoption of business-to-business e-commerce solutions, especially by small-to-medium-enterprises (SMEs), across a broad range of industry sectors and geographic regions. The goal of the ITOL program is to accelerate the national adoption of business-to-business electronic commerce solutions, especially by communities of small and medium enterprises. ITOL have provided funding for projects in the health and pharmaceutical, building and construction, automotive industry, and primary industries.

In terms of education, the number of people trained in technology is very low. In January 2000, an Ernst & Young survey reported that Australians' greatest concern related to the Internet was credit-card security.

---

<sup>6</sup> "Time Running Out: Shaping Regional Australia's Future: The Inquiry into Infrastructure and the Development of Australia's Regional Areas" – House of Representatives Standing Committee on Primary Industries and Regional Services (May 2001)

<sup>7</sup> [www.state.gov/www/about\\_state/business/com\\_guides/2001/eap/australia\\_ccg2001.pdf](http://www.state.gov/www/about_state/business/com_guides/2001/eap/australia_ccg2001.pdf) (IT labour market in Australia) (visited on 21 May 2002)

<sup>8</sup> [www.tcn.net.au/funding\\_options.htm](http://www.tcn.net.au/funding_options.htm) (IT funding in Australia)

More than 40 percent of Australian consumers listed security as a barrier to e-commerce adoption compared with a mere 25 percent in Europe. In the US, security ranks fifth among consumer concerns. High-speed access is being rolled out slowly (particularly in rural areas) and needs to be quickened. Government intervention on audio and video streaming hinders the development of broadband communication.<sup>9</sup>

With regards to legislation, the Australian government has one of the most comprehensive legislative structures in the world as far as e-business and e-commerce are concerned. *The Electronic Transactions Act* (1999), which came into force in March 2000, provides a liberal regulatory regime for the use of electronic communications for legal and government transactions, even though this legislation has been criticised for a lack of coverage of consumer protection issues. In addition, the *On-line Services Act* (1999) provided legislation covering censorship issues, designed specifically so as not to stifle legitimate business development with 'overzealous' laws.<sup>10</sup>

The telecommunication industry operates within a regulatory framework with the intent that there is a large degree of self-regulation to enable and promote competition. The Australian Communications Industry Forum (ACIF) was established by the industry to develop voluntary codes and standards within this framework. The federal authorities exercise a degree of regulation through several government agencies, most notably the Australian Communications Authority (ACA) and the Australian Competition and Consumer Commission (ACCC).

The telecommunications sector is dominated by Telstra, the former government-owned monopoly. Telstra also owns a large proportion of Australia's telecommunications infrastructure. The major regulatory issues faced in the sector are the prices, terms, and conditions of access by telecommunications providers to Telstra's infrastructure. The ACCC is in charge of administering access and approving access prices. The access regime is designed to encourage competition in the industry without duplicating infrastructure in an uneconomic way.

Network access pricing for incumbents has been embroiled in disputes from the outset. The time taken to reach decisions because of this legal process has been criticised as benefiting few in the industry, with all stakeholders facing regulatory uncertainty. The Productivity Commission is currently investigating the Telecommunications Access Regime (TAR) and competitive safeguards, while the Minister for Telecommunications is also currently showing great interest in reforming access rules, possibly before the Productivity Commission reports.

The digitisation of Telstra's Hybrid Fibre Co-ax network, commonly known as Foxtel, is an example of how access regulation impacts on telecommunications industry investment in infrastructure. Telstra has deferred its investment in the digitisation of the network at an estimated cost of over A\$1 billion (EUR 585 million), because of uncertainty over the terms and conditions that future access seekers will be granted by regulators to the upgraded network. The unbundling of this network is still proceeding at an unacceptably slow pace.

---

<sup>9</sup> Key IT issues in Australia: [www.e-businessforum.com/index.asp?layout=rich\\_storyanddoc\\_id=1168andcountry\\_id=AUandcountry=Australiaandchannelid=6andcategoryid=21](http://www.e-businessforum.com/index.asp?layout=rich_storyanddoc_id=1168andcountry_id=AUandcountry=Australiaandchannelid=6andcategoryid=21) (visited on 21 May 2002)

<sup>10</sup> [www.e-businessforum.com/index.asp](http://www.e-businessforum.com/index.asp)

Non-public telecommunications systems infrastructure remains the responsibility of both State and Federal governments. This has led to a proliferation of standards and incompatibility between systems. In areas such as emergency services, where co-ordination is essential - often across State borders and between agencies - this is a real problem.

The provision of services in regional and rural areas is generally subsidised by the federal government through community service obligations. Current government funding is A\$670 million (EUR 392 million). Dual rollout of network systems because of competition and lack of network access by various carriers has resulted in many cases to competitors' cables following parallel routes. The telecommunications industry is predominantly privately funded, with the 50 percent government ownership of Telstra being the major exception, which in any case is a net contributor to the public purse. The half-privatised nature of Telstra means that there is great potential for direct government interference in the telecommunications industry, despite the largely light-handed approach to regulation seen in telecommunications.

Co-operation between carriers in the deployment and sharing of infrastructure is particularly relevant in non-urban areas where it may not be economical to roll out several mobile telephone networks. The carriers have formed a Mobile Carrier Forum (MCF) with the primary aim of improving the co-location of mobile telephone facilities.

The Commonwealth has allocated A\$3 million (EUR 1.75 million) to a national promotional campaign aimed at increasing public awareness of the benefits, opportunities, and importance of being on-line. Up to 30 'On-line Australia' regional summits are being held, to allow regional communities to explore the opportunities and benefits to be gained from the Internet and the emerging on-line economy. All governments were involved in On-line Australia Day 1998.<sup>11</sup> The Education Network Australia (EdNA) initiative is a prime example of national co-operation and collaboration between all levels of Australian government and all sectors of Australia's education and training community, designed to maximise the benefits of information and communications technology for Australian education and training.<sup>12</sup>

As a result of government initiatives, Australians are becoming more aware of on-line choices and the information economy's opportunities, and have the confidence and understanding they need to participate. Data from the ABS indicate that 2.8 million Australian adults regularly access the Internet from home in 2000.<sup>13</sup>

This includes the establishment of a Ministerial Council to develop a National Information and On-line Services Strategy. The government aims to provide a relatively non-interventionist, yet pragmatic, framework for supporting and encouraging private sector-led development of the information economy. In order to avoid legislation, the government also avoids taxes on electronic commerce. To ensure international interoperability of regulatory frameworks between different countries, the Government emphasises self-regulation.

---

<sup>11</sup> National Office for the Information Economy (NOIE): [www.noie.gov.au/projects/information\\_economy/strategic\\_framework/dec98\\_strategy.htm](http://www.noie.gov.au/projects/information_economy/strategic_framework/dec98_strategy.htm) (visited on 21 May 2002)

<sup>12</sup> Ibid.

<sup>13</sup> Strategic Framework for the Information Economy - Action Plans: [www.noie.gov.au/projects/information\\_economy/strategic\\_framework/May2000\\_update.htm](http://www.noie.gov.au/projects/information_economy/strategic_framework/May2000_update.htm) (visited on 21 May 2002).

The government is providing leadership in information economy by adopting on-line technologies to better services and improve its own business practices. These includes delivering Commonwealth services electronically on the internet, establishing electronic payment as a normal means for Commonwealth payments, developing infrastructure for government-wide intranet for secure on-line communication, etc. National authorities are also playing a very important role in educating and training Australians to create a workforce with requisite skills to compete in the information economy, through the Ministerial Council of Education, Employment and Training, and Youth Affairs. Furthermore, the government also implements many funding programmes to enhance access for remote areas and people with disabilities. To foster the development of the information industries, the Government has initiated the Information Industries Action Agenda.

NOIE, in conjunction with the Government On-line Department, is responsible for the development of e-government. The aim is to bring all appropriate government services on-line by 2001.<sup>14</sup> A July 2000 Andersen Consulting report on e-Government Leadership grouped Australia, the US, Singapore, and Canada as top-tier 'early leaders' in e-government.

Australia recently declared that: "the Government realises the opportunities the on-line environment provides to give all Australians improved and expanding access to Government services and to assist streamlining business operations for Government and business". Several programmes have been initiated in order to achieve effective e-government. The E-Procurement Strategy will help foster the growth of e-commerce by letting all simple procurement suppliers who wish to deal electronically with the Commonwealth do so by the end of 2001. The Trials in Innovative Government Electronic Regional Services (TIGERS) project is piloting innovative means of delivering government services, with an emphasis on regional and remote areas. The Government Electronic Resources Network (GOVERNET) aims to provide seamless, cross-jurisdictional access to government information and services, whilst the Australian Government Locator Service (AGLS) has been developed to help in the inter-agency co-ordination of information and services.<sup>15</sup>

Australia has identified ten priority areas towards which it must direct its efforts. These include maximising opportunities for all Australians to benefit from the information economy, delivering the education and skills necessary to do so, and advancing the growth of a world-class infrastructure for the information economy. The overall aim is to achieve a significant increase in the use of electronic commerce by Australian businesses.

The National Office for the Information Economy (NOIE), established in 1997, is considered to be one of the most effective government bureaux in the world for dealing with e-business and building the digital future. More recently, the Australian government invested A\$78 million (EUR 45.6 million) into developing business infrastructures, and has begun initiatives to aid small businesses to prepare for a future of e-commerce. Finally, the Australian government has set up Business Entry Point (BEP), which is intended to provide a quick and easy on-line access point for new and existing businesses to deal with government agencies.<sup>16</sup>

---

<sup>14</sup> Government On-line: [www.ogo.gov.au](http://www.ogo.gov.au) (visited on 21 May 2002).

<sup>15</sup> "Government On-line Out In Front" (7 June 2000) DCITA: [www.dcita.gov.au/nsapi-graphics/?Mival=dca\\_dispdocandID=5051](http://www.dcita.gov.au/nsapi-graphics/?Mival=dca_dispdocandID=5051) (visited on 21 May 2002)

<sup>16</sup> Business Entry Pont – About Us: [www.business.gov.au/documents/dir62/doc504362.html](http://www.business.gov.au/documents/dir62/doc504362.html) (visited on 21 May 2002).

The Department for Information Technology, Communications, and the Arts (DITCA) in Australia is responsible for policy, programmes, and initiatives to support and promote Australia's information technology sector.<sup>17</sup> NOIE is responsible for many areas of e-policy, in particular (in conjunction with the Government On-line Department) that relating to e-government initiatives to promote e-commerce and B2B, the development of the information economy, government on-line services, and the Internet.<sup>18</sup>

In its January 1998 report *A Strategic Framework for the Information Economy*, NOIE stressed the role that Australia would play in the international scene. The desire to lead the world in the development of policy and to influence the development of internationally-based regulatory frameworks was stressed throughout. NOIE's priorities tellingly included the desire to influence the emerging international rules and conventions for electronic commerce, and to implement a world-class model, which would be imitated by other nations.<sup>19</sup>

In a world-wide survey conducted by Business Software Alliance (BSA) this year, Australia was found to have a very low piracy rate (33 percent), in contrast to some of the highest piracy rates seen in the region. Australia is a member of the World Intellectual Property Organisation (WIPO) and most multilateral IPR agreements.

The 1999 *Electronic Transactions Act* creates a regulatory regime for using electronic communications in transactions. The Act facilitates electronic commerce in Australia by removing existing legal impediments that may prevent a person using electronic communications to satisfy legal obligations under Commonwealth law. Section 10 of the Act deals with Digital Signatures, allowing a person to satisfy a legal requirement for a manual signature by using an electronic communication that contains a method that identifies the person and indicates their approval of the information communicated. The legislation provides flexibility for people and businesses to determine the signature technology that is appropriate to their particular needs. Such technology must identify that person sufficiently for the purposes of the communication.

There are currently no legislative prohibitions on organisations transferring personal information from Australia to other countries. From 21 December 2001, organisations will have to comply with the NPP 9, which is based on the restrictions set out in the European Directive on Transborder data flows. The EU has begun to assess the new Australian regime to see whether it meets the required standard for EU privacy regulations. Other Commonwealth laws contain privacy provisions relating to information about health insurance claims, data matching, information about old criminal convictions, as well as personal information disclosed by telecommunications companies, video surveillance, telephone interception or 'bugging', and physical intrusion into private spaces.

The Australian Parliament passed a controversial cyber-crime law in September 2001. These included penalties for up to 10 years for computer-related offences. The new laws would also give police new powers to compel suspects to assist in investigations of crimes involving computers and also covers unauthorised use of a computer in other crimes such as murder. Seven new offences were introduced

---

<sup>17</sup> DCITA: [www.dcita.gov.au/graphics\\_welcome.html](http://www.dcita.gov.au/graphics_welcome.html) (visited on 21 May 2002)

<sup>18</sup> Government On-line, [www.ogo.gov.au](http://www.ogo.gov.au); NOIE, [www.noie.gov.au/about/index.htm#NOIE Activities](http://www.noie.gov.au/about/index.htm#NOIE_Activities) (visited on 21 May 2002)

<sup>19</sup> National Office for the Information Economy (NOIE): [www.noie.gov.au/projects/information\\_economy/strategic\\_framework/dec98\\_strategy.htm](http://www.noie.gov.au/projects/information_economy/strategic_framework/dec98_strategy.htm) (visited on 21 May 2002).

which cover many activities, such as hacking, denial-of-service attacks, web-site defacements, and spreading viruses.<sup>20</sup> However, it was criticised as a knee-jerk reaction to computer security problems. The Australian Computer Society (ACS) said that it supported the intentions of the new laws but was concerned by the departure from the recommendations of a model code that had been finalised in January.

Australia has been an interested observer of the development of the sometimes controversial Council of Europe *Convention on Cyber-Crime* and is expected to be one of the first signatories.<sup>21</sup> Australia is also party to many of the workings of the G-8 developments, in particular the work of Interpol in combating trans-national electronic crime.

### ***Assessment of Phenomena Undermining Dependability***

The impact of lack of diversity cable routes (for telcos) was demonstrated recently when all of coastal NSW north of the Hawkesbury River was left without services, following damage to a single cable. Australian authorities recognise that security and privacy worries relating to trust and confidence in the Internet are central to the issue of success of the on-line component of doing business in the information society. The Federal Police, in particular, are also concerned about the increasing sophistication of the average attacker, and the fact that reported cyber-crimes (to the Australian Computer Emergency Response Team, AusCERT) went up four-fold in 2000.

By 2002, according to the 2002 Australian Computer Crime and Security Survey (undertaken jointly by Deloitte Touche Tohmatsu, AusCERT and the New South Wales Police) released in May 2002, more than two thirds of Australia's largest public and private organisations were reported victims of computer crimes, according to the results of a survey released today. In this sense, the level of cyber-crime in Australia has doubled since 1999, with sixty-seven percent of the 300 organisations surveyed reported incidents of crime including fraud, data sabotage, Trojan infection and laptop theft; in addition, more than 35 percent of those organisations were hit with six or more incidents. When compared with the US in 2002, Australia now has a higher rate of cyber-crime, with the majority of threats emanating from externally. This may have interesting results for Australia's private sector: according to the survey, as many as 43 percent of the organisations said they were interested in recruiting ex-hackers to deal with IT security issues – three times more than in the US.

In addition to a key role for NOIE in co-ordinating e-security activities across the Commonwealth, key players are: the Attorney-General's Department, which maintains the primary responsibility for critical infrastructure protection; the Australian Federal Police (AFP); the Australian Security Intelligence Organisation (ASIO); and the Defence Signals Directorate (DSD).

As reliance on information systems has increased in Australia, so, predictably, have instances of attacks. Australia, a regional centre for many worldwide businesses targeted by online activists, has had its share of web-site defacements, virus 'outbreaks' and Denial of Service (DoS) attacks. There have also been many

---

<sup>20</sup> Kate Mackenzie, "Cyber-crime laws passed" (27 September 2001): [australianit.news.com.au/articles/0,7204,2944524\\_percent5E15306\\_percent5E\\_percent5Enbv\\_percent5E,00.html](http://australianit.news.com.au/articles/0,7204,2944524_percent5E15306_percent5E_percent5Enbv_percent5E,00.html) (visited on 21 May 2002)

<sup>21</sup> "Council Of Europe Adopts Global Cyber-Crime Treaty", [Newsbytes](http://Newsbytes.com/news/01/172012.html) (8 November 2001): [www.newsbytes.com/news/01/172012.html](http://www.newsbytes.com/news/01/172012.html) (visited on 21 May 2002)

warnings from the Australian Police about the dangers of online life in the 21<sup>st</sup> century. Some incidents of note include the defacement of Toshiba's regional headquarters web-site, the inclusion of many local government sites in a mass defacement in January 2001 where dozens of web-sites in three different time zones were systematically defaced. Targets in Australia generally centred around local government sites, or those ending with '.gov' as the top level domain.<sup>22</sup> In October 2001, a hacker who caused thousands of litres of raw sewerage to flood parks was jailed for two years. The man was found guilty of hacking into the sewerage computer system of Maroochy Shire Council in March 2000 and purposely releasing effluent. He was jailed for 12 months for wilfully causing environmental harm, and two years for other computer hacking charges.<sup>23</sup>

In August 2001, an investigation was launched into alleged electronic intrusion into a politician's computer. The allegation was that the computer used to access the files was located in a New South Wales government office, which pointed the finger at foul play. Subsequently, a PC was seized belonging to a state member of parliament.<sup>24</sup>

Summer 2001 also saw another large defacement of Australian company web-sites, a phenomenon that is becoming all the more popular. At least 48 sites were attacked in a seven-day period by a group or individual known only as L4m4 ('Lamer'). Sites invaded included those belonging to the cable TV station Sky Channel, Dymocks online book retailer, a city council, and a charity belonging to a healthcare facility in Melbourne. The likely attack vector was Microsoft's Internet Information Server, which all the sites appeared to have been running.<sup>25</sup>

### ***Government Initiatives Aimed at Tackling Cyber-Security***

Australia defines an attack on the national information infrastructure (NII) as "an attack or system failure that would a) be nationally significant – that is, the loss would be felt nationally; b) damage the economic well-being of the nation; c) seriously damage public confidence in the information infrastructure; or d) threaten life or public health and/or public order." An incident critically affecting the NII may be undertaken for a purpose that is prejudicial to national security and/or for a criminal objective. In Australia, the government has witnessed an increasing rate of referrals of computer network attacks (CNAs) to the Australian Federal Police, as well as a four-fold increase in reports of computer incidents to AusCERT during 2000.

Before analysing the Australian approach towards the protection of CIP, it is clear that Australia has not fully exploited the policy experiences gained while dealing with Y2K. Widespread public awareness campaigns have been launched aimed at small and medium enterprises. A specific Y2K Industry programme was put together to encourage Australian businesses to prepare for day-change, as well as devising appropriate contingency strategies. Moreover, a specific Y2K disclosure legislation was approved calling for voluntary disclosure of information on Y2K problems, remediation efforts and compliances. One of most important aspects of this work was the government's strong emphasis in explaining to the

---

<sup>22</sup> See "attrition.org" for an archived list of web-site defacements: [www.attrition.org](http://www.attrition.org) (visited on 21 May 2002)

<sup>23</sup> "Computer Hacker Jailed for two years", *ABC News* (Australia) (31 October 2001): [www.abc.net.au/news/newslink/nat/newsnat-31oct2001-96.htm](http://www.abc.net.au/news/newslink/nat/newsnat-31oct2001-96.htm) (visited on 21 May 2002)

<sup>24</sup> "Australian Govt Computer Seized In Hacking Incident", *Newsbytes* (6 August 2001): [www.infowar.com/hacker/01/hack\\_080601a\\_j.shtml](http://www.infowar.com/hacker/01/hack_080601a_j.shtml) (visited on 21 May 2002)

<sup>25</sup> "Hacker Goes On Defacement Spree In Australia", *Newsbytes* (5 July 2001): [www.infowar.com/hacker/01/hack\\_070501a\\_j.shtml](http://www.infowar.com/hacker/01/hack_070501a_j.shtml) (visited on 28 January 2002)

general public that the Y2K issue was not just an IT problem. It socio-economic and cultural ramifications could be extensive.

However, the government decided to take a fresh approach to information assurance and infrastructure protection; this “E-Security National Agenda” will involve NOIE as the key player in co-ordinating e-security activities across the Commonwealth and a number of other government bodies.

Two central co-ordination bodies have been established to oversee the government’s critical infrastructure protection (CIP) efforts. The first of these is the E-Security Co-ordination Group (ESCG), the government’s core policy development and co-ordination body on e-security matters for both the public and private sectors. ESCG has been developing an incident-reporting and -response capability; advancing work on raising e-security awareness in both the public and private sectors; ensuring that international activities in e-security are properly co-ordinated across Australia; addressing e-security skills issues; and ensuring that the legislative framework is appropriate to deal with current and emerging e-security issues. The E-Security Policy Section provides administrative support to the ESCG. Chaired by NOIE, the Section’s membership is wide-ranging and includes virtually every government department, as well as the Action Group on Law Enforcement Implications of Electronic Commerce (AGLEC).

The Critical Infrastructure Protection Group (CIPG), chaired by the Attorney-General’s Department, is tasked with the responsibility of identifying and providing advice on the protection of Australia’s NII with respect to critical incidents. The CIPG recently began a study on the degree of threat that exists to Australia’s NII from critical incidents – it is expected that this will be the centrepiece of the government’s policy.

Australia has also set up Fedlink, with the aim of providing secure, quick, and easy electronic channels of communication between government departments and agencies.<sup>26</sup> In 2000, as part of its cyber-security budget of A\$1.7 million (EUR 0.994 million), a National Information Infrastructure Secretariat (NIIS) was established. The Secretariat is advised by an industry committee, which has so far met three times, most recently in July 2000.<sup>27</sup>

The Attorney-General’s Department (which includes ASIO and the AFP) co-ordinates government efforts to identify and protect the critical NII. Co-ordination is located within the Information and Security Law Division, responsible for developing policy and providing advice on law relating to national security, privacy, intellectual property rights, and electronic commerce. The Attorney-General supports the CIPG with executive, policy, and secretariat support; ensures that protection of the critical elements of the NII is done in accordance with government priorities and in a structured and measurable way; co-ordinates the development of NII policy, in particular as it interfaces with criminal and information law reform, and law enforcement; carries out CIP project work; works with NOIE to foster relationships with industry; develops crisis management arrangements to deal with attacks on the NII that affect government interests; and co-ordinates international efforts in NII protection at a strategic level, both in bilateral and multilateral arrangements.

The Defence Signals Directorate (DSD) provides a range of information security services and advice to help ensure that government and Australian Defence Force communications and information systems are secure. DSD manages the Australian Information Security Evaluation Programme (AISEP), which

---

<sup>26</sup> Government On-line – Fedlink: [www.ogo.gov.au/projects/wholeofgovon-line/fedlink.htm](http://www.ogo.gov.au/projects/wholeofgovon-line/fedlink.htm) (visited on 21 May 2002)

<sup>27</sup> “Australia - Business in front line against cyber-warfare”, *Australian Financial Review* (28 April 2000).

provides government and industry with an efficient service for the evaluation and certification of information security products and systems. DSD also administers the Gateway Certification Guide and its associated procedures for Internet gateway certification, designed to ensure the security of government agency links to the Internet.

DSD is represented on the ESCG and the CIPG, and works closely with the AFP and ASIO to monitor incidents potentially threatening to the NII, providing technical expertise in the event that such incidents need to be investigated. DSD also advises government agencies on how to implement effective IT security by providing expert assistance to agencies, reviewing agency information security procedures, assessing agency information systems and networks, and developing guidelines and policies on implementing security – such as the Australian Communications-Electronic Security Instruction 33 on protecting information systems. Finally, DSD also runs ISIDRAS, an IT incident reporting scheme for Commonwealth government agencies specifically concerned with high level incidents that could cause damage to government IT infrastructures.

The Directorate has established a computer network vulnerability team (CNVT) to provide a response capability for agencies which require specialist assistance in either securing their sites following an incident or reviewing their general level of security readiness. The CNVT is also responsible for investigating potential vulnerabilities in software and hardware commonly used by Commonwealth bodies. CNVT also has a threat and vulnerability assessment role specifically focused on communications and IT systems used by Commonwealth government departments, authorities, and the armed forces.

ASIO's role is to collect security intelligence and maintain protective security responsibilities. This includes developing a capability to collect and analyse information relating to CIP threats; developing a small investigative capability to work as necessary with other agencies such as DSD and the AFP; contributing to the development of a CIP security programme; and contributing to policy development on NII protection. ASIO has also developed its Protective Security and T4 Programmes. The T4 project is a team of protective security specialists with expertise in various technical and protective security disciplines. These programmes flow into the Security Construction and Equipment Committee.

Finally, the Action Group on Law Enforcement Implications of Electronic Commerce (AGLEC), formed in 1997 as a response to the Heads Of Commonwealth Operational Law Enforcement Agencies' (HOCOLEA) need to research the impact of electronic commerce on law enforcement and revenue agencies' ability to continue to promote a safe community. AGLEC is currently headed by the Director of the Australian Transaction Reports and Analysis Centre (AUSTRAC), who is a member of the ESCG.

In 1999, ASIO was formally granted powers to hack into computers and conduct electronic surveillance. This has been criticised as unnecessary.<sup>28</sup> Australian focus on CIP issues began in 1998, following publicity surrounding attacks on the electricity supply network.<sup>29</sup> Extensive planning for the Sydney Olympics showed the extent of Australia's preparation to defend itself against cyber-attacks. The Australian Federal Police pursues offences against Commonwealth law in both Australia and overseas and has established an NII Incident Analysis and Response position within the National Operations Monitoring Centre

---

<sup>28</sup> "ASIO given computer hacking powers" (26 November 1999): [www.abc.net.au/news/1999/11/ite\\_19991125231757\\_1.htm](http://www.abc.net.au/news/1999/11/ite_19991125231757_1.htm) (visited on 21 May 2002)

<sup>29</sup> Dr A. Cobb, "Thinking about the unthinkable: Australian Vulnerabilities to High-Tech Risks", [www.apf.gov.au/library/pubs/rp/1997-98/98rp18.htm](http://www.apf.gov.au/library/pubs/rp/1997-98/98rp18.htm) (visited on 21 May 2002).

(NATOMC) located at AFP HQ in Canberra. This position provides specialist assessment and advice on electronic crime referrals received by the AFP (either through the NATOMC or Operations Monitoring Centres in AFP State offices) which potentially impact on the NII. This post is also responsible for co-ordinating analysis of such incidents with other agencies responsible for the protection of the NII and providing advice to AFP management on NII issues. The NII Incident Analysis and Response role is supported by Electronic Crime Collection Manager within the AFP's Strategic Intelligence division and the AFP's Electronic Evidence Teams.

In addition, new privacy laws were introduced in December 2001 that require all private companies with a turnover of more than A\$3 million (EUR 1.75 million) to meet National Privacy Principles or a Privacy Code approved by the Privacy Commissioner. Finally, the GATEKEEPER project aims to provide a structure through which government can ensure integrity, security, and authenticity in the transmission of information and transaction of business.

### ***Industry and Other Non-Government Activities Related to Dependability***

AusCERT is the national CERT organisation and comes under the government bureaucratic structure. AusCERT provides a single, trusted point of contact for the Internet community to deal with computer security incidents and their prevention. AusCERT aims to "reduce the probability of successful attack, to reduce the direct costs of security to organisations and lower the risk of consequential damage".<sup>30</sup>

### ***Public-Private Partnerships***

On November 2001 the Prime Minister of Australia announced the government's intention to form a Business-Government Task Force on Critical Information Infrastructures. Its aim is to give business greater input into the assessment of current arrangements to protect key national infrastructure. The membership of the Task Force provides broad representation of the owners of Australia's critical infrastructure. Relevant Commonwealth, State and Territory government agencies are also represented.

The Task Force met in March 2002. The major themes of that meeting can be summarised into the following six recommendations, which are detailed in the following paragraphs in conjunction with detailed explanations.

- 1. The Commonwealth and the States and Territories, in consultation with the private sector, should develop a strategic overview of risks to critical infrastructures and, as a first step, commit to prioritisation of tasks building on the work that has already been done to assess the vulnerabilities in the telecommunications, transport and public utilities sector by 30 September 2002.*

The objective of this recommendation is to ensure that programs for critical infrastructure protection focus on the areas of greatest concern, assessed on a risk management basis. This recognises the need to apply the limited resources available to the areas of the greatest vulnerability and representing the most significant impact on the community in the event of an attack. A programme of future studies will be developed by the Commonwealth governments' Critical Infrastructure Protection Group (CIPG) in consultation with industry and State governments.

2. *The Commonwealth, in cooperation with the private sector and the States and Territories, should build on existing mechanisms, such as the Standing Advisory Committee on Commonwealth-State Cooperation For the Protection Against Violence (SAC-PAV) and arrangements for emergency management, to ensure systems and procedures are in place to adequately protect the critical infrastructure.*

Many of the structures currently in place in Australia for counter-terrorism and emergency management are highly adaptable to address critical infrastructure protection. More importantly, they are ready to react rapidly to major disasters or emergencies based on their long active experience.

3. *The Commonwealth should build a learning network among the key public and private sector organisations to improve systematic, strategic responses to the security of the National Information Infrastructure separate from, but linked to, physical redundancy and linkages to key international resources. Public-private partnerships should also be encouraged, while the AUSCERT should be strengthened. Finally, the Commonwealth, in consultation with the private sector, should examine major threats and interdependencies in telecommunications and banking as example of specific, targeted consideration between the relevant agencies and organisations.*

The Taskforce called for the creation of US Information Sharing and Analysis Centres supported by consultative arrangements at both the operational and policy levels between the public and private sectors.

4. *The Commonwealth, States and Territories should review their legislative frameworks for sharing information so as to facilitate the supply of information by business, ensure its confidentiality and exclude liabilities.*

There is concern among private sector organisations that their obligation in information sharing arrangements would be limited by obligations under Australian law. There are also major concerns that the collective sharing of information and investigation of vulnerabilities in systems by companies of the same sector of the economy could be interpreted as collusion and be prohibited by Australian anti-trust laws. A similar set of concerns existed in the lead up to the Year 2000 date rollover for computer systems. The *Year 2000 Information Disclosure Act 1999* was enacted to give business some protection of voluntarily exchanging information. This could serve as a model for enabling legislation for infrastructure protection.

5. *The Commonwealth should develop models of good critical infrastructure assurance, taking into account relevant standards, in consultation with the private sector and the States and Territories.*

In Australia, infrastructure assurance is a relatively new philosophy combining existing security and risk management practices. The Task Force would like the development of effective critical infrastructure assurance models.

---

<sup>30</sup> AusCERT, [www.auscert.org.au](http://www.auscert.org.au) (visited on 21 May 2002)

6. *The Commonwealth, States and Territories should examine ways to encourage investment in the security and resilience of critical infrastructures.*

The Australian government is well aware of the fact that some industry sectors lack market pressure to deliver a more secure or more robust infrastructure. This is in part due to lack of interest in the market for a so-called “premium service, and in part due to structural factors relating to market regulations. Consequently, the government is strongly invited to foster strong public-private partnerships to define measures calling for determining information assurance as a business priority.

### ***Research and Development***

Various defence research organisations are involved with information security thinking in Australia. These include the Australian Defence Organisation Defence Science and Technology Organisation (DODSTO) and the former Air Power Studies Centre (now the Aerospace Center). In addition, Dr Adam Cobb’s paper reveals the extent of interest in this issue at the Australian National University’s Strategic and Defence Studies Centre. There are a number of technology science parks specifically designed to be conducive to R&D (favourable tax breaks, etc.), including ones located in Brisbane, Adelaide University, Tasmania, and at LaTrobe University.

The University of Wollongong has one of the most technically advanced computer science departments in Australia, with a strong emphasis on cryptography and information security.<sup>31</sup> The Centre for Computer Security Research conducts advanced research into primarily technological security methods, including cryptography and intrusion detection systems. It is widely regarded as the foremost regional centre for research and development in this field and the LOKI197 cryptographic algorithm attracted attention as being twice as strong as DES (Data Encryption Standard), the former US NIST encryption standard. Finally, the University of Newcastle’s Department of Computer Science and Software Engineering also has a research program on IT and e-Commerce which covers data security for e-Commerce systems.<sup>32</sup> Notwithstanding these academic activities, there does not seem to be a strong industry involvement in the this area. TELSTRA, the country’s main telecommunication and information provider, has its own R&D centre with some projects in this area. Nevertheless, it is possible to speculate that the country’s increase interest towards safeguarding the country’s information infrastructures for accidental and malicious attacks and faults may lead to more funding and activities in the field of information security and privacy.

---

<sup>31</sup> University of Wollongong Centre for Computer Security Research: [www.uow.edu.au/research/about/brochure/cyber.html](http://www.uow.edu.au/research/about/brochure/cyber.html)

<sup>32</sup> University of Newcastle, IT / e-Commerce Research: [www.cs.newcastle.edu.au/Research/ITEC/index.html](http://www.cs.newcastle.edu.au/Research/ITEC/index.html) (visited on 28 January 2002).