8

Other Issues

National Information Infrastructure

8.1 The broad issues of e-security are dealt with by the E-Security Co-ordination Group (ESCG), chaired by the NOIE. The ESCG has also established a government E-Security Working Group, jointly chaired by the DSD and NOIE.[1]

8.2 The task of the ESCG[2] is the coordination of policy on e-security and achieving:

> … the strategic goal of creating a trusted and secure electronic operating environment for both the private and public sectors, including through:
>
> a) defining and protecting the National Information Infrastructure, including identifying potential incidents of a critical nature;
>
> b) maintaining and enhancing law enforcement, national security, regulatory and revenue protection capabilities in the electronic environment; and

---

1 MAC, Report No. 2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, p. 13.

2 The Group has a broad membership, including: NOIE, Attorney-General's Department, Department of Defence, DSD, Australian Federal Police, ASIO, Department of the Prime Minister and Cabinet, Department of Foreign Affairs and Trade, Department of Transport and Regional Services, Department of Industry Science and Resources, Australian Transactions Reports and Analysis Centre, Australian Securities and Investments Commission, Department of the Treasury, Centrelink and the Australian Bureau of Statistics. NOIE, *E-Security National Agenda*, http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm, 27 October 2003, p. 2.

c) pursuing these goals on an international basis.[3]

8.3 In November 2000, the Secretaries Committee on National Security recommended the establishment of a strategic policy working group, to identify and provide advice on the protection of Australia's National Information Infrastructure. The result was the formation, in September 2001, of the Information Infrastructure Protection Group – then called the Critical Infrastructure Protection Group – as a sub-committee of the ESCG.[4]

8.4 This group, chaired by the Attorney General's Department, is tasked with providing advice to Cabinet on critical issues affecting the National Information Infrastructure. It reports through the Secretaries' Committee on National Security, on serious actual and potential information security incidents affecting the Commonwealth and critical industry sectors.[5] The submission to this inquiry by the Attorney General's Department, outlined the circumstances in which the Information Infrastructure Protection Group would be called upon:

> A critical incident may be defined as an attack or system failure on some part of the National Information Infrastructure which supports or underlies systems or the delivery of services whose loss for more than a short period would:
>
> - be nationally significant, i.e. the loss would be felt nationally;
> - damage the economic well-being of the nation;
> - seriously damage public confidence in the information infrastructure;
> - threaten life, public health or public order; or
> - impair national defence or national security.[6]

8.5 The aim of the group is to improve '… the reliability of the information infrastructure upon which the Commonwealth and the wider community depend' and to '… help to assure the integrity of electronic information in the Commonwealth'.[7]

---

3 NOIE, *E-Security National Agenda*, http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm, 27 October 2003, p. 2.

4 MAC, Report No. 2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, p. 13.

5 MAC, Report No. 2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, p. 13; Attorney-General's Department, *Submission No. 24*, pp. 3-4.

6 Attorney-General's Department, *Submission No. 24*, pp. 3-4.

7 Attorney-General's Department, *Submission No. 24*, p. 4.

8.6 In November 2001, the Government also announced the formation of a Business-Government Task Force on Critical Infrastructure. Following the recommendations of this Task Force, the Government then announced, in November 2002, the formation of a Trusted Information Sharing Network for Critical Infrastructure Protection (TISN). The Network has a much wider brief than the IT sector alone but will discuss and share information on issues vital to that sector, such as: business continuity, information system attacks and vulnerabilities, e-crime and the protection of key sites from attack or sabotage.[8]

8.7 As part of the TISN, a Critical Infrastructure Advisory Council was formed to oversee the various sector advisory groups and '… to advise the Attorney-General on the national approach to protecting critical infrastructure.'[9]

8.8 It is intended that the Critical Infrastructure Advisory Council will concern itself with the preventive side of critical infrastructure protection and not with responses to security incidents.[10]

Committee Comment

8.9 The establishment of the National Information Infrastructure reflects the growing importance of the management of electronic information in Commonwealth agencies. As public expectations about the availability of government services online increase, so does the importance of the role played by that infrastructure.

8.10 The Committee considers that each agency needs to be fully aware of the National Information Infrastructure and the importance of creating a trusted and secure electronic operating environment. It is particularly important that the Chief Information Officer, or equivalent, in each agency should be familiar with its operations and be prepared to contribute when needed.

8.11 The Critical Infrastructure Advisory Council has an important role to play in helping agencies anticipate threats to IT networks.

8.12 The Committee notes as per the recommendations arising out of chapter 2 of this report that elements of Critical Infrastructure Protection remain inadequate and thus require further attention.

---

8 Trusted Information Sharing Network for Critical Infrastructure Protection, *Fact Sheet*, 6 June 2003, p. 1.

9 TISN, *Fact Sheet*, p. 2.

10 TISN, *Fact Sheet*, p. 2.

Report by Management Advisory Committee

8.13 In 2002, the MAC released a report on the *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework.*[11]

8.14 The report highlighted the increasing use of electronic and on-line information by government agencies and the consequent need for changes in business processes. It reasoned that there should be a whole-of-government approach to Information and Communication Technology (ICT) investment and governance:

> Increasingly, information and communication technology … plays an important role in determining the quality and accessibility of services. The development of effective whole-of-government approaches to ICT is critical to achieving further significant gains in the delivery of government services.[12]

Whole-of-Government Approach

8.15 While recognising that a 'one size fits all' approach is unworkable, the report noted that:

> There is an increasing demand for government to provide more integrated and interactive information and services. To provide a seamless and consistent service across government, agencies must work together to ensure that their individual systems are compatible and can be linked.[13]

8.16 The report said that at present, decisions on ICT investment and governance are made by individual agencies. There is no overall co-ordination arrangement which would contribute to the report's aim of achieving an investment regime directed towards '… increased collaboration on ICT procurement and re-use of valuable intellectual property across the Federal government.'[14]

8.17 The report added that chief executives are required by the FMA Act to manage the affairs of an agency in a way that promotes proper use of the

---

11 The role and composition of the MAC is set out in Chapter 3, Footnote 25.

12 MAC, Report No. 2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework,* Australian Public Service Commission, 2002, p. 2.

13 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework,* Australian Public Service Commission, 2002, p. 2.

14 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework,* Australian Public Service Commission, 2002, p. 2.

Commonwealth resources. The result is decisions about resources based on internal agency considerations and to meet an individual agency's requirements. However, the outcome may not be the best one from a whole-of–government perspective.[15]

8.18 To begin the task of moving to a more co-ordinated approach, the report recommended a review of the government sector's ICT arrangements. It proposed that the priorities for the review should be: ICT standards, interoperability, investment, governance of shared infrastructure, IT management skills and contract management.[16]

8.19 The importance of the task can be gauged by the fact that the report recorded that '… the Commonwealth Government spends about $3.5 billion annually on ICT (an estimated $2.1 billion recurrent and up to $1.4 billion capital)'.[17]

8.20 The MAC reached the conclusion that growth in the ICT sector is being driven by public demand for faster and more accessible service delivery. The Government sector itself has the complementary incentive of projected efficiency gains through the extended use of ICT. [18]

8.21 The MAC acknowledged the importance of security in 'Promoting public confidence in these services, including the need to authenticate users of government services …'[19]

Data Sharing Between Agencies

8.22 One area where increasing public expectations cause particular problems, is the task of achieving balance between service efficiencies, individual privacy and the security of the information held by an agency.

8.23 The MAC report commented that clients would rely more and more on '... government remembering services already provided and the information already gathered'. At the same time, the public is growing in awareness of the potential for government to aggregate the electronic data collected by

15 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, p. 11.

16 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, p. 2.

17 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, p. 2.

18 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, p. 6.

19 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, p. 22.

all of its agencies. This awareness is accompanied by increasing sensitivity to any 'unwarranted intrusion' on individual privacy.[20]

8.24 Information sharing and aggregation can both improve the efficiency of government services and streamline service delivery but public acceptance of large scale aggregation would depend on the strength and effectiveness of privacy and security arrangements. There will be a need to balance requirements between clients who expect the agency to know about previous contacts and transactions; those who ascribe to the 'enter once, use many times' principle; and those who are highly sensitive to government management and use of their private details.[21]

Proposals and Conclusions

8.25 The MAC report proposed a series of basic principles for ICT governance, as a means of optimising the outcomes across the range of government agencies. The proposals do not seek to dilute the responsibility of each agency for its own policies, but to take advantage of opportunities where a multi-agency approach could be utilised. In summary, the recommended principles are as follows:

- agencies should continue managing their own ICT strategy, development, implementation and support;
- improved information and knowledge sharing across agencies would enhance management;
- business returns to government from ICT investment can be optimised through guidelines and shared processes;
- new ICT systems should take account of the likelihood of sharing information with other agencies;
- security and privacy is essential to ICT supported business processes;
- all Commonwealth ICT should have a strategic focus on business outcomes and efficiency gains;
- investment and funding models should accommodate shared approaches to system development and Intellectual Property; and

20 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, pp. 13-14.

21 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, pp. 13-14.

- an agreed Quality Assurance process should protect shared architecture and systems.[22]

8.26 The report concluded that the process of change in the ICT area is being powered by a number of business drivers:

- acceleration of the pace of change to improve efficiency and effectiveness; achieving a more flexible and dynamic approach to policy and program delivery;
- ICT enables the same information infrastructure to service a variety of channels for program delivery;
- shared standards, infrastructure, and security, collaboration in procurement and exploitation of government Intellectual Property can deliver better value for money;
- the balance between security and privacy is a key consideration – heightened by increased security awareness following terrorist attacks and the influence of the Privacy Act on individual privacy issues;
- information sharing can improve the efficiency of business processes and streamline service delivery – but subject to appropriate privacy and security safeguards; and
- effective government application of ICT both learns from and influences, private sector development. This process in turn gives impetus to the development of the Australian information economy.[23]

Committee Comment

8.27 The Committee agrees with the MAC that a coordinated approach to the application of ICT to the operations of Commonwealth agencies is needed. It also recognises, however, that there are limits to the standardisation that can be achieved, because of the variety of agencies involved and the need for IT operations to be, to a certain extent, tailor made to suit each agency's needs.

8.28 The Committee believes that the issues raised in the MAC report would provide a sound basis for achieving a balance between coordination and the individual needs of agencies. The Committee expects any whole-of-government initiatives to give a high priority to systems and network security – both electronic and physical – across the Commonwealth, particularly in these times of heightened security risk.

---

22 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, p. 12.

23 MAC, Report No.2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, Australian Public Service Commission, 2002, pp. 12-14.

Closed vs Open Source Software

8.29 The protection of computer systems from attacks from outside is a vital part of the terms of reference for this inquiry. There is a strong body of opinion that the Commonwealth's ability to protect its computer networks would be enhanced if open source software were in general used by Commonwealth agencies.

8.30 The Committee was presented with a considerable body of opinion on the relative security capabilities of closed source software on the one hand and open source software on the other.

8.31 The evidence given on this issue quickly divided itself into the two camps, with little common ground. Supporters of closed source software claimed that the security features of closed source products were subjected to a more rigorous production and testing regime and were superior to comparable open source programs.

8.32 Similarly, open source supporters claimed that the transparency of the source code of these products allowed them to be extensively tested by a wide range of independent users – the so-called 'many eyes' theory. This process, they claimed, has resulted in many vulnerabilities being found and repaired before a major problem could occur.

The Differences

8.33 The AUUG explained the difference between the development processes for the two types of software programs.

8.34 It explained that software is generally written in a high level programming language (such as C, Java or COBOL). The result is source-code with an English-like appearance that can be read and understood by a human. The source code is then passed through a 'compiler' program which produces a binary code translation of the source code. The binary program can be read and executed by any suitably equipped computer, but is very difficult for a human to understand. To change a program or fix a problem, the source code is changed and once more run through the compiler. Changes via the binary code are generally impractical.[24]

8.35 Closed source software is sold in binary only packs and the source code is kept secret by the vendor.[25]

---

24 AUUG, *Submission No. 13*, p. 10.

25 AUUG, *Submission No. 13*, p. 11.

8.36 In the case of open source software, the package going to the user has both the binary code and the source code. Users are therefore able to access the source code and, within the bounds of their licensing agreement, alter it to suit their own needs. [26]

The Arguments

8.37 AUUG was a strong supporter of the case for open source software. It explained that it is Australia's peak open source and open systems user group.[27]

8.38 In its submission AUUG argued that there are two very important considerations in the argument between closed and open source systems. Firstly, the interoperability of software and hardware products and secondly, independence from reliance on a product vendor.[28]

Interoperability

8.39 AUUG commented that the use of standard, open protocols across a network allows a wide range of software, hardware and communications products to interact successfully. If reliance is placed on one proprietary, closed source application, such as Microsoft Word, then all other users are committed to using that same product if they wish to have access to the data. In summary, AUUG said:

> Using standards avoids problems with data stored in proprietary formats being inaccessible due to patents, trade secrets, or just lack of good documentation. … Similar standards should also apply to communication protocols.[29]

Vendor Independence

8.40 AUUG also said that independence from a particular vendor is an advantage: 'Software vendors may go out of business, may increase prices to an unacceptable level, or may decide that it is no longer in their business plan to support the software.'[30] In the long term this could lead to data becoming inaccessible.[31]

8.41 The remedy, AUUG reasoned, is to use standard, open formats:

---

26 AUUG, *Submission No. 13,* p. 11.
27 AUUG, *Submission No. 13,* p. 1.
28 AUUG, *Submission No. 13,* p. 10.
29 AUUG, *Submission No. 13,* p. 10.
30 AUUG, *Submission No. 13,* p. 10.
31 Mr Paddon, *Transcript,* 2 April 2003, p. 167.

> If the software has used standard formats for the data, it should be possible to find another vendor who can access that data. At the worst, custom software could be developed to read the existing data. Using proprietary formats, the vendor achieves a lock-in – only that vendor can access the data without considerable effort.[32]

8.42 In response Microsoft claims that data stored in their closed format will still be accessible in 100 years time. It said that it is in the company's best interests to make sure that compatibility is maintained so that customers see value in upgrading to a new version and are confident that they will have the ability to bring forward their documentation.[33]

8.43 The Committee notes the concern, expressed by NAA, that the use of proprietary software incurs the on-going payment of licence fees.[34]

Security

8.44 Referring to claims that in a recent period, there were more than one thousand viruses and worms targeting Microsoft products compared with less than twenty against Linux and Unix combined, Microsoft said:

> Microsoft operating systems and Microsoft platforms are very popular ... If I were a hacker or a virus writer, the trend would be to write something that does the most damage. The most damage is done by writing it to a Microsoft platform.[35]

8.45 Advocates of open source software argue that it is more secure than closed source software because, as AUUG stated '… access to source means that an enormous amount of peer review goes on.' It continued:

> … the fact that it is available means that it is looked at by a very broad number of people from different educational and cultural backgrounds, and that diversity leads to a lot of out-of-the-box thinking ; therefore a lot of problems are found proactively and are fixed.[36]

8.46 Microsoft countered this argument by saying that security requires highly qualified security experts to actually examine, fix and test code. It claimed that simply making source code available to volunteer programmers is not

32 AUUG, *Submission No. 13,* p. 10.
33 Mr Russell, *Transcript,* 16 June 2003, pp. 280-1.
34 Mr Stuckey, *Transcript*, 1 April 2003, p. 98.
35 Mr Russell, *Transcript,* 16 June 2003, p. 281.
36 Mr Paddon, *Transcript,* 2 April 2003, p. 164.

enough, and widespread source code availability itself can introduce security risks.[37]

8.47 Microsoft argued that the strength of commercial software is in its development processes and claimed that security is being given a very high priority in the products it currently has under development. It claimed that its new security technology for the Microsoft Windows platform is being developed in consultation with the community, to give technology users additional security and privacy protection.[38]

8.48 On the other hand, AUUG argued that market pressures ensure that security is not a high priority in commercial software :

> … it is clear that the large proprietary operating system vendors do not make money by making their products more secure. It is not that they do not want to or there is anything wrong with them; they are very good at what they do. However, it is not necessarily good business to spend a lot of money on security. For example, how many people would go out and spend another $500 on a new version of Windows just because it was a bit more secure? I would put it to you that that would be a fairly small niche market.[39]

Committee Comment

8.49 The debate between the proponents of closed and open source software seems likely to continue with no decisive advantage to either side. It seems to Committee members that there are strong arguments for both sides of the debate. In general terms, the Committee feels that the idea behind a summary comment by AUUG is worth consideration:

> [AUUG] …would hope that the government would make the best technology choice at every juncture. Sometimes the best technology choice may indeed be a proprietary system. It may provide features, capabilities or some functionality that is only available with that system. However, AUUG feels that the government should seriously consider using open systems, particularly where equivalent functionality is available at a much lower cost and with all the benefits of open source software.[40]

8.50 The Committee believes that agencies should consider the benefits or otherwise of using open or closed source software, as a normal part of

37 Microsoft Australia, *Exhibit No. 17*, p. 1.

38 Mr Russell, *Transcript*, 16 June 2003, p. 278.

39 Mr Paddon, *Transcript*, 2 April 2003, p. 164.

40 Mr Paddon, *Transcript*, 2 April 2003, p. 170.

their IT risk management processes and their cost / benefit analysis of new resources.

Mr Bob Charles MP

Chairman

March 2004