The Parliament of the Commonwealth of Australia

Report 399

Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

Joint Committee of Public Accounts and Audit

March 2004
Canberra

ISBN 0 642 78452 3

Contents

APPENDICES

Foreword

Report 399 is the outcome of an inquiry by the Joint Committee of Public Accounts and Audit into the management and integrity of electronic information in the Commonwealth. The inquiry had originally focused on the electronic protection of information held by Commonwealth agencies. However, it became apparent that a far more fundamental problem was the physical security of Commonwealth computing assets and the information held on them.

Towards the end of the inquiry, the Committee had been angered to learn about the theft of IT equipment from an Australian Customs Service facility at Sydney airport through the media, rather than from Customs officials – who had appeared before the Committee the previous day.

So concerned was the Committee at the approach by Customs and the nature of the security breach at the airport that Members resolved to extend the inquiry – in part to take further evidence from Customs. The Committee accepts that agencies will make mistakes from time to time and need to improve their procedures. What is totally unacceptable, however, is any lack of openness before the Committee.

The Customs incident also occurred at the same time as a break-in at a Department of Transport and Regional Services computer facility, which the Committee also learnt about via the media. Fortunately that department was more forthcoming with information to the Committee.

In its determination to investigate the scale of the security problem, the Committee wrote to all departments seeking details of their security breaches and thefts of IT equipment. The Committee discovered that between 1998 and 2002 Commonwealth agencies lost almost 950 laptop computers alone. This figure does not include an unknown proportion of the 537 computers of all types lost by the Department of Defence during the period.

All the departmental responses are published on the Committee's website. Members hoped that departments drew lessons from the Customs incident about the need for them to be forthcoming with the Committee. The alacrity with which departments provided additional information to the Committee gives cause for optimism.

Nonetheless, the Committee found that a number of Commonwealth agencies had inadequate levels of the physical security for IT equipment. This was reflected in successful breaches of the security of facilities, in poor record keeping of lost or stolen IT equipment and in a lack of knowledge of appropriate reporting mechanisms in the event of a security breach.

The physical security of IT equipment held by Commonwealth agencies is the first requirement for the integrity of the information held by the

Commonwealth. A second area that is vital to the satisfactory management electronic information by Commonwealth agencies is the need to develop and implement practicable standards for the protection of information against access by unauthorised persons or for unauthorised purposes. The security of information held by providers of tendered services caused the Committee particular concern.

The Committee has recommended that standards for the making and management of contracts between Commonwealth agencies and external service providers be implemented across the whole of government. All new and re-negotiated outsourcing contracts for information technology should pursue best practice and cover three areas that are fundamental to the security of electronic information. First, they should prohibit service providers from entering into sub-contracting arrangements that are not authorised by the Commonwealth. Second, they should establish clear lines of communication between contracting parties by requiring information sharing protocols. Third, they should provide for graduated sanctions that can be implemented when service providers are found to be in breach of contractual arrangements.

The Committee also explored security measures associated with the transmission of data between Commonwealth agencies and between agencies and citizens. Both Commonwealth and private sector agencies complained that the Commonwealth's public key infrastructure system – Gatekeeper – is too complex and too expensive to make agency accreditation practical. The Committee has recommended that the cost effectiveness of Gatekeeper procedures be reviewed in light of other commercially available public key infrastructure technologies.

Finally, the Committee found that Commonwealth agencies need to implement effective data storage practices is in guaranteeing future access to data in the face of rapidly changing technology. To this end, the Committee has recommended that the preservation of Commonwealth electronic records is given equal priority to paper records and that all Commonwealth electronic records are subject to comprehensive and tested business continuity and disaster recovery plans.

On a final note the Committee is aware of the impending replacement of the National Office of Information Economy with two new bodies: the Australian Government Information Management Office (AGIMO) and the Office of Information Economy. Accordingly, recommendations have been redirected to AGIMO, even though the organisation was not in existence at the time that this report was tabled.

Mr Bob Charles MP
Chairman

Membership of the Committee

40th Parliament

Chairman	Mr Bob Charles MP	
Deputy Chair	Ms Tanya Plibersek MP	
Members	Senator Richard Colbeck (until 25/03/03)	Mr Steven Ciobo MP
	Senator Stephen Conroy (from 5/02/03, until 10/09/03)	Mr John Cobb MP
	Senator John Hogg (until 5/02/03, from 10/09/03)	Mr Petro Georgiou MP
	Senator Kate Lundy (from 19/11/02)	Ms Sharon Grierson MP
	Senator Claire Moore (until 19/11/02)	Mr Alan Griffin MP
	Senator Andrew Murray	Ms Catherine King MP
	Senator Nigel Scullion	Mr Peter King MP
	Senator John Watson	The Hon Alex Somlyay MP

Membership of the Sectional Committee

Chairman	Mr Bob Charles MP	
Deputy Chair	Ms Tanya Plibersek MP	
Members	Senator Kate Lundy	Mr Steven Ciobo MP
		Mr John Cobb MP
		Ms Sharon Grierson MP
		Mr Peter King MP

Committee Secretariat

A/g Secretary	Mr James Catchpole
Sectional Committee Secretary	Mr Tas Luttrell (until 05/12/03)
	Dr Glenn Worthington (from 05/12/03)
Research Officer	Dr Marcus Hellyer
	Mr Alex Stock
Administrative Officers	Ms Maria Pappas
	Mr Patrick Pantano
	Ms Sheridan Johnson

Duties of the Committee

The Joint Committee of Public Accounts and Audit is a statutory committee of the Australian Parliament, established by the *Public Accounts and Audit Committee Act 1951*.

Section 8(1) of the Act describes the Committee's duties as being to:

(a) examine the accounts of the receipts and expenditure of the Commonwealth, including the financial statements given to the Auditor-General under subsections 49(1) and 55(2) of the *Financial Management and Accountability Act 1997*;

(b) examine the financial affairs of authorities of the Commonwealth to which this Act applies and of intergovernmental bodies to which this Act applies;

(c) examine all reports of the Auditor-General (including reports of the results of performance audits) that are tabled in each House of the Parliament;

(d) report to both Houses of the Parliament, with any comment it thinks fit, on any items or matters in those accounts, statements and reports, or any circumstances connected with them, that the Committee thinks should be drawn to the attention of the Parliament;

(e) report to both Houses of the Parliament any alteration that the Committee thinks desirable in:

(i) the form of the public accounts or in the method of keeping them; or
(ii) the mode of receipt, control, issue or payment of public moneys;

(f) inquire into any question connected with the public accounts which is referred to the Committee by either House of the Parliament, and to report to that House on that question;

(g) consider:

(i) the operations of the Audit Office;
(ii) the resources of the Audit Office, including funding, staff and information technology;
(iii) reports of the Independent Auditor on operations of the Audit Office;

(h) report to both Houses of the Parliament on any matter arising out of the Committee's consideration of the matters listed in paragraph (g), or on any other matter relating to the Auditor-General's functions and powers, that the Committee considers should be drawn to the attention of the Parliament;

(i) report to both Houses of the Parliament on the performance of the Audit Office at any time;

(j) consider draft estimates for the Audit Office submitted under section 53 of the *Auditor-General Act 1997*;

(k) consider the level of fees determined by the Auditor-General under subsection 14(1) of the *Auditor-General Act 1997*;

(l) make recommendations to both Houses of Parliament, and to the Minister who administers the *Auditor-General Act 1997*, on draft estimates referred to in paragraph (j);

(m) determine the audit priorities of the Parliament and to advise the Auditor-General of those priorities;

(n) determine the audit priorities of the Parliament for audits of the Audit Office and to advise the Independent Auditor of those priorities; and

(o) undertake any other duties given to the Committee by this Act, by any other law or by Joint Standing Orders approved by both Houses of the Parliament.

Terms of reference

The Committee shall inquire into and report on the potential risks concerning the management and integrity of the Commonwealth's electronic information.

The Commonwealth collects, processes and stores a large amount of private and confidential data about Australians. This information is held by various Commonwealth agencies and private bodies acting on behalf of the Commonwealth. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrelink keeps social security, family and health information. The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.

In conducting its inquiry the Committee will consider:

- the privacy, confidentiality and integrity of the Commonwealth's electronic data;
- the management and security of electronic information transmitted by Commonwealth agencies;
- the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks; and
- the adequacy of the current legislative and guidance framework.

List of abbreviations

ABS	Australian Bureau of Statistics
ACA	Australasian Certification Authority
AGIMO	Australian Government Information Management Office
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ANAO	Australian National Audit Office
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
AUUG	Australian UNIX and Open Systems Users Group
CA	Certification Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
CD	Compact Disk
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DEWR	Department of Employment and Workplace Relations
DoFA	Department of Finance and Administration

DoTaRS	Department of Transport and Regional Services
DSD	Defence Signals Directorate
DVD	Digital Versatile Disk
EDS	Electronic Data Services
EPL	Evaluated Product List
ESCG	E-Security Co-ordination Group
FaCS	Department of Family and Community Services
FMA Act	Financial Management and Accountability Act 1997
HIC	Health Insurance Commission
ICT	Information and Communication Technology
IPP	Information Privacy Principle
ISIDRAS	Information Security Incident Detection, Reporting and Analysis Scheme
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
JCPAA	Joint Committee of Public Accounts and Audit
MAC	Management Advisory Committee
NAA	National Archives of Australia
NOIE	National Office for the Information Economy
OECD	Organisation for Economic Cooperation and Development
OGIT	Office of Government Information Technology
PDF	Printable Document Format
PKC	Public Key Cryptography
PKI	Public Key Infrastructure

PM&C	Department of Prime Minister and Cabinet
RA	Registration Authority
ROM	Read Only Memory
SSL	Secure Socket Layer
TES	Telstra Eneterprise Services
TISN	Trusted Information Sharing Network
XML	eXtansible Markup Language

List of recommendations

2 Physical Security

Recommendation 1

The Defence Signals Directorate (DSD) in conjunction with other agencies where appropriate, ensure that Commonwealth agencies institute without delay, physical security plans for each of their information technology systems. Additional plans may be necessary for key information technology centres. DSD to advise the Committee within six months of the tabling of this report, on the status and adequacy of these plans.

Recommendation 2

The Australian Government Information Management Office advise all Commonwealth agencies that new or renegotiated contracts for outsourcing of information technology services need to pursue best practice and include the following:

- clear information sharing protocols that require each party to inform the other when an information technology security incident occurs that, directly or indirectly, affects the security of agency information technology networks;
- prohibition of unauthorised subcontracting of information technology services;
- provision for a graduated hierarchy of sanctions in response to security breaches.

Recommendation 3

The Department of Prime Minister and Cabinet introduce regulations that address the issuing and use of laptop computers and other portable electronic devices by Commonwealth agencies. The regulations should require that:

- such equipment is only issued to officers on a needs basis;
- such equipment is assigned to an individual, rather than to a work area, to ensure clear accountability;
- portable electronic devices are given password protection and, where they hold sensitive information, that data should be suitably encrypted;
- movement logs are made mandatory for valuable equipment taken outside agency premises ('valuable' here includes the significance of the information involved, as well as the monetary value);
- all thefts are reported to the police and to a central reporting body such as the Defence Signals Directorate; and
- regular inventory audits are conducted.

Recommendation 4

The Australian Government Information Management Office (AGIMO) ensure that Commonwealth agencies:

- have up-to-date asset registers of all IT equipment owned by them and used on their premises; and
- undertake a regular audit and reconciliation program of all owned and leased IT equipment.

AGIMO should advise the Committee, in an Executive Minute, of the completeness of the registers and the audit procedures that have been established.

4 Risk Management

Recommendation 5

The Australian Government Information Management Office, in consultation with the Defence Signals Directorate, reiterate to all Commonwealth agencies their responsibility to comply with the reporting requirements of the Information Security Incident Detection, Reporting and Analysis Scheme particularly the mandatory reporting of category 3 and category 4 incidents.

Recommendation 6

The Australian Government Information Management Office (AGIMO) monitor and report on the performance of Commonwealth agencies:

- implementation and maintenance of a flexible and responsive security risk management strategy for IT networks including hardware, software and data protection; and
- maintain an awareness of current and emerging threats to their computer networks and the recommended countermeasures.

AGIMO should advise the Committee in an Executive Minute, of the status and completeness of these arrangements.

5 Data Preservation

Recommendation 7

The Australian Government Information Management Office (AGIMO), with support from the National Archives of Australia (NAA), ensure that Commonwealth agencies implement knowledge management and archival policies such as e-permanance which give equal priority to preserving electronic and paper-based records. AGIMO to advise the Committee, in an Executive Minute, of the status of these arrangements. The NAA to be resourced properly.

Recommendation 8

The Australian Government Information Management Office (AGIMO), in consultation with the Australian National Audit Office, ensure that Commonwealth agencies have in place comprehensive and tested business continuity and disaster recovery plans for their electronic records networks and services. AGIMO to advise the Committee, in an Executive Minute, of progress with the implementation and testing of these plans.

6 Information Security

Recommendation 9

The Department of the Prime Minister and Cabinet should review and report to the Committee on the cost effectiveness of Gatekeeper versus other commercially available public key infrastructure products and systems.

On 10 March the Minister for Communications Information Technology and the Arts announced that the National Office of Information Economy (NOIE) responsibilities would be carried out by two new bodies: the Australian Government Information Management Office (AGIMO) and the Office of Information Economy.

The Committee notes that among the AGIMO's responsibilities is included 'research on e-government issues such as governance, security, authentication and investment.' The Committee originally directed recommendations 2, 4, 5, 6, 7 and 8 of the report to NOIE. These recommendations have been redirected to the AGIMO.

1

Security and Integrity of Electronic Information

Introduction

1.1 The secure storage of information has always been a challenge for Commonwealth agencies. As the use of computers and electronic communication has expanded, this challenge has escalated and taken on new dimensions.

1.2 Computers and electronic communication allow business to be conducted more efficiently. Everyday activities such as information retrieval and processing can be performed with increasing speed and accuracy.

1.3 With the increased efficiency of computers and electronic communication comes different risks. Greater efficiencies in data processing and communication mean that more information is potentially available to a party that has gained unauthorised access to an electronic information system. Easier access to data increases the risk of unauthorised access and theft. Being able to store more data in one place means that more data can be lost in a fire or natural disaster. On the other hand, improvements in information technology (IT) design have provided new opportunities to manage the security of information.

The Setting

1.4 As Commonwealth agencies increasingly rely on the internet to conduct business with the public, they must adopt strategies to protect data transfers from unauthorised access.

1.5 Similarly, the integrity of the Commonwealth's electronic data must be protected from:

- theft and malicious damage;
- electronic attacks, such as viruses and worms;
- negligence and human error; and
- natural disasters, such as fires or earthquakes.

1.6 Rapid advances in computer hardware and software add another challenge. Electronic information may be lost or become inaccessible because of the degradation or obsolescence of the data format or storage medium.

1.7 In addition to its obligation to the Australian people, the Commonwealth has an international obligation to protect the privacy and integrity of electronic information. It has agreed to implement Guidelines adopted in 1980 by the Organisation for Economic Co-operation and Development (OECD) for the Protection of Privacy and Transborder Flows of Personal Data.

1.8 In a recent publication *Guidelines for the Security of Information Systems and Networks*, the OECD outlined the information security problem:

> … As a result of increased interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. For these reasons, these guidelines … suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".[1]

1.9 In a similar vein, the Australian National Audit Office (ANAO) commented:

> The Commonwealth's use of computer software permeates every aspect of daily business from email to accounting and payroll. It is pervasive in the delivery of services by all entities and is rapidly

1 Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris, 2002, p. 7.

> changing the way the public interacts with entities through the ongoing growth of Internet enabled services.[2]

1.10 Reliance on electronic information storage and transmission is growing so quickly that it is essential that the Commonwealth build public and private confidence in the management and use of electronic information by government such as the maintenance of personal records. This can best be accomplished by protecting the privacy, security and integrity of electronic information under Commonwealth control.

1.11 The National Archives of Australia (NAA) addressed this situation in its submission to the inquiry, when it said:

> The Australian community needs to be confident that these records, while in the custody of the agency that collected or created them or with the Archives if they are assessed as being of enduring value, will be secure and retain their integrity.[3]

1.12 The physical security of the information and the equipment it is stored on also cannot be overlooked. The Committee found that more than a thousand laptop computers had been lost by Commonwealth agencies in the last five years. Among the equipment reported lost or stolen were:

- 537 laptops and PCs from the Department of Defence
- 117 laptops and 94 PCs from the Department of Family and Community Services (FaCS).

1.13 These examples are from large agencies and were numerically significant losses. However, the Committee noted that even among smaller agencies, which operate IT resources on a much smaller scale, the loss rate was often still high. Quite apart from the financial aspect of such losses, the danger of information held on the missing equipment being compromised is an issue of significant concern. A more detailed examination of this issue follows in Chapter 2.

1.14 In an effort to encourage a quality of record keeping which protects the privacy, confidentiality and integrity of commonwealth records, the NAA released, in March 2000, the *e-permanence* suite of best-practice recordkeeping standards, manuals and guidelines.[4]

1.15 The standards outlined for recordkeeping call for the institution of:

---

2 ANAO, *Capitalisation of Software*, Audit Report No. 54 2002-2003, p. 13.

3 NAA, *Submission No. 22* (http://naa.gov.au/recordkeeping/, 27 October 2003), p. 3.

4 NAA, *Submission No. 22*, p. 3.

> … policies, procedures and practices that produce records which have the characteristics of:
>
> - authenticity;
> - reliability;
> - integrity; and
> - useability.[5]

1.16 The NAA considers that present agency practices for record keeping do not provide a full, accurate, reliable, accessible and durable record of government activity. NAA said it is a situation '… where the essential evidence of government decisions and transactions is often kept in the hard drives, e-mail in-boxes and shared folders of individual[s] … or work groups.'[6]

1.17 The NAA concluded that the successful adoption of the *e-permanence* regime is essential for the proper management and maintenance of electronic information in the Commonwealth.[7] Support for this conclusion came from the ANAO. In 2002 it carried out an audit of recordkeeping in four Commonwealth agencies and the findings showed that none of the agencies satisfied the audit criteria.[8]

1.18 Electronic records were a particular focus of concern for the ANAO, which found that agencies were not sure that all essential electronic records were being captured. Most agencies were relying on individuals to print the records to paper but ANAO found that '… in practice, there were significant risks relating to capture of e-mail and electronic documents from personal workspace.'[9]

The Committee's Inquiry

1.19 The Joint Committee of Public Accounts and Audit (JCPAA) has a statutory duty to 'examine all reports of the Auditor-General', and the powers to report to Parliament 'on any items or matters' in the Commonwealth's 'accounts, statements and reports, or any circumstances connected with them'.[10]

---

5 NAA, *Submission No. 22*, p. 3.

6 NAA, *DIRKS – A Strategic Approach to Managing Business Information, Part 1 – The DIRKS Methodology : A User's Guide*, NAA, Canberra, September 2001, p. 5.

7 NAA, *Submission No. 22*, p. 4.

8 NAA, *Submission No. 22*, p. 2.

9 ANAO, *Recordkeeping*, Audit Report No.45 2001-2002, pp. 18-19.

10 *Public Accounts and Audit Committee Act 1951*, Sections 8(1) (c) & (d).

1.20 The Committee resolved in October 2002 to review the management and integrity of the Commonwealth's electronic information. This decision arose out of the Committee's review of a number of reports by the Auditor-General that addressed, wholly or in part, the issues of the management and integrity of electronic information held by the Commonwealth. A list of these reports, together with later reports on related issues, is shown in Appendix A.

1.21 The Committee established its own terms of reference, which are listed at page xii. The following paragraphs from the preamble to the terms of reference reflected the Committee's concerns:

> The Committee shall inquire into and report on the potential risks concerning the management and integrity of the Commonwealth's electronic information.
>
> The Commonwealth collects, processes and stores a large amount of private and confidential data about Australians. This information is held by various Commonwealth agencies and private bodies acting on behalf of the Commonwealth. For example, the Australian Taxation Office keeps taxpayer records, the Australian Electoral Commission keeps electoral roll information and Centrelink keeps social security, family and health information.
>
> The Committee is concerned that the Commonwealth's electronic information is kept securely and in a manner that ensures its accuracy.

1.22 Invitations to provide submissions to the inquiry were advertised in the national press on 30 October 2002. In response, 103 submissions have been received – a list can be found at Appendix B. Exhibits are listed at Appendix C.

1.23 The Committee held public hearings in Canberra and Sydney between March and October 2003. A list of witnesses at the hearings can be found at Appendix D.

1.24 In August 2003 the theft of two computer servers from the Australian Customs Service (Customs) facility at Mascot Airport was reported in the media. The Committee became aware of this incident during a public hearing into aviation security[11] but only after Customs had completed its evidence. Customs was recalled to explain why it had failed to advise the Committee of the breach during its evidence.

---

11 *Transcript*, 5 September 2003, pp. 42-46.

1.25 The incident had serious ramifications for the management and integrity of electronic information and the Committee decided to reopen the evidence gathering phase of the inquiry. The Committee had an additional public hearing in October and also wrote to Commonwealth agencies for details of IT thefts and security breaches suffered since July 1998. The data collected from these replies reinforced the Committee's growing concerns about the physical security of IT equipment and the data stored on it.

Report Structure

1.26 In addition to this introductory chapter the report is divided into seven parts:

- Chapter 2, Examines the physical security of IT equipment and the information stored on that equipment.
- Chapter 3, Outsourcing, considers the advantages and problems in outsourcing IT functions.
- Chapter 4, Risk Management, considers the issue of risk management as a response to the threats posed to the security and integrity of the Government's electronic information.
- Chapter 5, Data Preservation, examines the problems of long term storage of information and agencies' plans for business continuity and disaster recovery.
- Chapter 6, Looks at Public Key Cryptography and how it is used to protect Commonwealth information in transit.
- Chapter 7, Evaluation of Products under Australasian Information Security Evaluation Program, is an examination of the process used to evaluate software products for use in Commonwealth systems.
- Chapter 8, Other Issues. This chapter covers three additional topics: the National Information Infrastructure, a Report by the Management Advisory Committee, and the debate on Commercial versus Open Source Software.

Existing Legislation

1.27 There is a body of legislation and supporting material that directly or indirectly covers the integrity of electronic information held by the Commonwealth. This includes:

- The *Financial Management and Accountability Act 1997* (FMA Act), which provides a framework for the proper management of public money and

public property. Section 42 of the Act states that an official or Minister may be held civilly responsible for the loss of any public property, including information, that is in their custody. Each department and agency is responsible for protecting the electronic information that they hold.[12]

- The *Electronic Transactions Act 1999*, which provides a regulatory framework that facilitates the use of electronic transactions and enables business and the community, to use electronic communications in their dealings with government. Division 1 of the Act makes electronic transactions workable by giving them the same legal validity as regular transactions. Division 2 allows a person to use an electronic communication when required to provide information to the Government. Division 3, section 14, defines the time and place of the dispatch and receipt of an electronic communication. The Act also holds the purported sender of an electronic communication responsible for that communication, so long as it was actually sent by them.

- The *Privacy Act 1988*, which protects the privacy of individuals. Division 2 addresses the issue of information privacy, including electronic information. This division provides eleven Information Privacy Principles (IPPs) that set privacy standards for the keeping of personal information by Commonwealth and Australian Capital Territory government agencies. The Privacy Commissioner has responsibilities under the Privacy Act to pursue complaints of privacy breaches.

- The *Privacy Amendment (Private Sector) Act 2000*, which amends the *Privacy Act 1988* to set privacy standards for the collection, holding, use, correction, disclosure and transfer of personal information by private sector organisations. The amendment added ten National Privacy Principles, which provide a framework for the protection of personal information.

- The *Copyright Act 1968*, which relates to copyright of, among other things, electronic information. Sections 10AB, 10AC and 10AD of the Act describe the circumstances in which it is legal to copy electronic information. Sections 44E, 44F and 112DA describe the circumstances in which it is legal to import and sell copies of computer programs and copies of electronic literary or music items. Sections 49, 50, 51, 51AA and 51A describe the circumstances in which it is legal to electronically reproduce and communicate works for various purposes. Division 2A

12 NOIE, *Submission No. 20*, p. 7.

covers circumvention devices and electronic rights management information.

1.28 This body of legislation is supported by a number of Commonwealth Government guidance documents. These include the:

- *Protective Security Manual* issued by the Attorney-General's Department, disseminates Commonwealth protective security policies, principles, standards and procedures, to be followed by all Commonwealth agencies for the protection of official resources. Part C specifically addresses information security;
- *Australian Communications Electronic Security Instruction 33*, developed by the Defence Signals Directorate, provides guidance to Australian Government agencies on protecting their information systems; and
- ANAO Better Practice Guide, *Internet Delivery Decisions: A Government Program Manager's Guide*, identifies key questions and issues for managers to consider when deciding whether and how their agency should use the internet.

1.29 The legislation and the guidance documents will be referred to through the following chapters as appropriate.

2

Physical Security

2.1 The question of the physical security of the Commonwealth's IT equipment, and the data stored on it, sprang into prominence during the course of the inquiry. Evidence taken by the Committee in another inquiry and press reports of the theft of two file servers from Customs underlined the vulnerability of IT equipment and the consequent threat to data security.

2.2 The Committee's concern was increased when evidence came to light of a serious security breach by Telstra Enterprise Services (TES), when backup tapes for several departments disappeared – presumed dumped as rubbish.

Introduction

2.3 The Committee was disturbed about the reports of IT equipment thefts. Although all of the details of the losses were not available, due to ongoing police investigations, there was sufficient information to indicate that lapses in security had occurred.

2.4 To clarify the facts, the Committee held a special public hearing in Canberra on 17 October 2003, taking evidence directly from the departments affected and the agencies involved in the investigation of the thefts.

2.5 In addition, the Committee asked Commonwealth agencies to provide details of all IT equipment, software and related products, lost since July 1998. The agency responses indicated a need to reduce the unacceptably high loss rate of equipment apparent in some departments and agencies. In addition, the difficulties and delays encountered in compiling the

requested data, showed that inventory controls have been neglected in many Commonwealth agencies.

2.6 The data provided by agencies revealed that laptop computers have been by far the most vulnerable equipment to loss or theft – more than 1000 having been lost over the five years surveyed.[1] A list of losses of IT equipment from Commonwealth agencies can be found at Appendix E. What was equally disturbing in the agency responses was the very low rate of recoveries and prosecutions related to these losses.

2.7 The Committee was particularly concerned to receive evidence from the Department of Defence that 'Not all data prior to 2002-03, such as laptops lost or stolen in 2000-01, is available from the asset management database and information prior to 2000 is not available from the investigations database.'[2] The Committee finds it unacceptable that of 64 computers lost or stolen in 2001-02 only 11 of these incidents were reported to federal or state police.[3]

Physical Security of IT Networks

2.8 In examining the evidence before it, the Committee found that the physical security of IT networks has two main aspects:

1) the security of the building itself and measures in place to counter attempts to break-in to secured areas; and

2) the screening process for people seeking access to secured areas and the measures in place to verify their identity and right to be admitted.

2.9 The Committee observed contractual relationships and responsibilities between Commonwealth agencies and IT service providers provide an additional layer of complexity in ensuring the physical security of IT equipment.

Building Security

2.10 One of the difficulties which became apparent during the inquiry, was the problem of maintaining a high level of security in shared office buildings.

---

1 Aggregate figure calculated from responses by Commonwealth Departments and associated agencies to the request made by the JCPAA in mid-October 2003.

2 Minister for Defence, *Submission No. 86,* p. 1.

3 Minister for Defence, *Submission No. 86,* p. 1.

Where Commonwealth agencies do not have full control of a building for security purposes, it is difficult to ensure that an adequate level of security is in place.

2.11 Inadequate building security allowed a break-in at the Department of Transport and Regional Services (DoTaRS) in August 2003, where the thieves used false identification to gain access to the building's public spaces and then physically broke-in to the secured area by smashing glass doors.[4]

2.12 This case shows the need for effective alarm systems in secured areas and for much faster response times from security services. As a result of this incident, DoTaRS is reviewing its security arrangements and, in the meantime, has hired security guards to patrol the area.[5]

2.13 To some extent, attention to physical security has taken second place in agency planning to the high profile task of protecting IT networks from electronic attacks. Electronic Data Services (EDS), an IT contractor to Commonwealth agencies including Customs, commented in its evidence that most of the focus is on stopping attacks on networks and that '… there is an assumption that physical security around key systems is going to be in place.'[6]

2.14 The Committee is concerned that this climate of complacency is addressed very quickly.

Visitor Identification

2.15 It is an essential link in the security chain that staff controlling access to secured areas are completely satisfied about the identity of anyone admitted to that area.

2.16 The Committee emphasises that, as in many aspects of security, the weak point in the system is the human factor. The best system possible cannot protect a site adequately against a security staff member who fails to carry out the correct procedures. This fact stresses the need for careful selection and training of security staff.

2.17 The theft from Customs is an excellent illustration of this principle – the thieves gained access to the building with false identification and then were allowed to enter a secure area unescorted. Neither of these errors

4 Mr Fisher, Mr Yuile, Mr Banham, *Transcript*, 17 October 2003, pp. 351-2.

5 Mr Fisher, *Transcript*, 17 October 2003, p. 364.

6 Mr Smith, *Transcript*, 17 October 2003, p. 321.

would have remained undetected if the prescribed security procedures had been followed.

2.18 When questioned by the Committee about the incident, Customs responded:

> We have a comprehensive set of security practices that are required to be followed – and are generally followed – which, I think, meet the standards that any external agency would set. In essence, what happened was a breakdown in the process in a particular location.
>
> We have taken physical steps to deal with access to the building; security steps in relation to the computer room; and steps in relation to accompanying people when they go on site. … So we are having a comprehensive look at security throughout Customs, with one of the major requirements being security plans which will be site specific – so that each site will need to have a security plan and an obligation that the security plan is complied with.[7]

2.19 EDS agreed with Customs that the security process and policy in place at the site was 'sound and robust' and that the problem was a local practice that negated the system:

> I would say that the approach being taken within Customs, defined by the policy and the processes that were in place, was sound, robust and sufficient to secure the equipment. What occurred was a breakdown in that process.[8]

2.20 The evidence suggests to the Committee that security procedures should be tailored to each location, as intended by Customs. In addition, to ensure that security procedures are followed correctly, regular staff training in security awareness should be conducted.

2.21 Appropriate security procedures provide a necessary condition for the safeguarding of electronic information, but the Committee is of the view that this by itself will not guarantee effective protection. To be fully effective, procedures must be underpinned by a strong security culture among departmental officials.

---

7 Mr Woodward, *Transcript*, 17 October 2003, p. 369.

8 Mr Smith, *Transcript*, 17 October 2003, p. 321.

Recommendation 1

2.22 **The Defence Signals Directorate (DSD) in conjunction with other agencies where appropriate, ensure that Commonwealth agencies institute without delay, physical security plans for each of their information technology systems. Additional plans may be necessary for key information technology centres. DSD to advise the Committee within six months of the tabling of this report, on the status and adequacy of these plans.**

2.23 The security lapses examined by the Committee have revealed that there is a need for clear and active channels of communication between agencies and outsourced service providers. In the context of this inquiry, contracts should place obligations on both parties to inform each other when an IT security incident occurs.

Recommendation 2

2.24 **The Australian Government Information Management Office advise all Commonwealth agencies that new or renegotiated contracts for outsourcing of information technology services need to pursue best practice and include the following:**

- **clear information sharing protocols that require each party to inform the other when an information technology security incident occurs that, directly or indirectly, affects the security of agency information technology networks;**
- **prohibition of unauthorised subcontracting of information technology services;**
- **provision for a graduated hierarchy of sanctions in response to security breaches.**

Survey of Equipment Losses

2.25 The responses from Commonwealth agencies to the Committee's request for details of lost or stolen IT equipment revealed that those losses had reached alarming levels. The value of the lost equipment and the cost of

replacing it, together represent a very substantial cost to the Commonwealth. This could either be in direct replacement costs or increased insurance premiums.

2.26 When the threat to data security is also considered, it becomes obvious that this is an area where all Commonwealth agencies have a need to ensure that their procedures and accountability are brought up to best practice as quickly as possible.

2.27 Even where the equipment is, in fact, owned by a contractor rather than the agency itself, the contract would no doubt have built-in to it an additional cost factor in anticipation of likely losses. It is in the Commonwealth's interest to institute practices which minimise that anticipated cost and hence the contract loading.

2.28 DSD has said that losses of IT equipment rate as Level 3 incidents under the Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) and should all, therefore, be reported to DSD. Agencies seem to be unaware of this assessment and very few cases have, in fact, been reported without prompting from DSD.[9]

2.29 Customs offered the opinion that it is almost impossible to completely eliminate theft – but high quality internal security systems in IT equipment could ensure the protection of the data. In giving evidence Customs said:

> … it is going to be extremely difficult for any agency or private sector organisation to come up with a foolproof mechanism that prevents theft from either buildings or homes. What it does do is put a lot more pressure on those who design systems to enable appropriate protection and a series of layers of security to be built into those computers, and into the software that lies behind them, in the event they are stolen. I just do not believe there will ever be a solution to theft. We do the best we can.[10]

IT Equipment Lost by Agencies

2.30 A summary table of the IT equipment reported lost or stolen from Commonwealth agencies can be found at Appendix E. The following paragraphs, however, look at some of the more serious cases revealed in those reports. The Committee notes that IT assets are in some cases the property of the contracted service provider which can add a level of complexity to lines of responsibility.

9 Mr Burmeister, *Transcript*, 17 October 2003, p. 392.

10 Mr Woodward, *Transcript*, 17 October 2003, p. 370.

2.31 For sheer volume the quantity of equipment lost by the Department of Defence stands out. Although the losses reflect, to some extent, the scale of its operations compared to other departments, the loss of 537 personal computers and laptops in five years is alarming.

2.32 A particularly worrying aspect of the Defence losses is that three of the computers lost contained material classified as secret. Even though these machines were recovered, these incidents represent significant security breaches. In addition, there were more than thirty additional security breaches which did not involve national security level data.

2.33 FaCS also reported large quantities of equipment lost in the five year period. FaCS lost 117 laptops and 94 PCs and when the extremely personal nature of the data handled by this department is considered, these statistics represent a potentially substantial breach of individual privacy. The other aspect to be considered is that over half the laptops and almost three quarters of the personal computers, were lost in the last two years. This indicates that FaCS security position is worsening.[11]

2.34 Within the Treasury portfolio, the Australian Taxation Office (ATO) reported that in the period from 1 July 1999 to 29 September 2003, over one hundred laptops were stolen and twenty-two were lost. Fortunately, in this case Treasury reported that the hard drives of all laptops are encrypted with DSD approved software and would be very difficult to access.[12]

2.35 The Department of Industry, Tourism and Resources portfolio reported the loss of 138 laptops and 42 personal computers, 64 of these items were lost from the Commonwealth Scientific and Industrial Research Organisation (CSIRO) and the rest from the department itself.[13]

2.36 The equipment listed by departments was lost or stolen in a variety of locations. Personal computers were most often stolen from offices; while for laptops, thefts from offices, private homes, vehicles and hotel rooms were common. Laptops were also prone to be left in taxis and lost at airports. Several laptops were lost in the Canberra bushfires in January 2003.

2.37 Losses which were particularly disturbing were a laptop and a printer / facsimile machine stolen in separate incidents, while being

11 FaCS, *Submission No. 87*, p. 1.

12 Treasury, *Submission No. 82,* pp. 3-4.

13 DITR, *Submission No. 78,* pp. 2-4.

transported by courier services and a briefcase containing an encryption modem stolen while in transit in aircraft baggage. [14]

2.38 Although many of the thefts and losses were reported to police, the recovery and prosecution rate is best described as disappointing. The Committee believes Commonwealth agencies should report all thefts of laptops, personal computers and other valuable IT equipment to the police. This strategy will reinforce the significance of IT losses on those responsible for the safekeeping of the equipment.

Telstra Incident

2.39 The case involving TES reinforced the need for staff to adhere closely to security guidelines. In this case, backup tapes holding e-mail traffic for several departments, were routinely stored for a brief time in a wheelie bin, while awaiting movement to a secure storage area. On this occasion there was a changeover in staff and the new staff member presumed that the normal transfer to secure storage had proceeded as usual. Several weeks later it was discovered that the tapes were not in the secure storage area.[15]

2.40 Telstra have been unable to trace the tapes and it is presumed that they were thrown out in the course of the normal rubbish collection – although no-one can be certain of this.[16]

2.41 The Committee has reviewed the comments made by TES on this incident and was dissatisfied with their vagueness. For example, asked where the incident occurred, TES representatives were unable at first to say which city the problem occurred in. They were also unable to definitely state whether or not press reports that Telstra staff had searched rubbish tips for the lost tapes, were accurate or not.[17]

2.42 It was left to the Department of the Prime Minister and Cabinet (PM&C) to explain that, in fact, since the loss was not discovered for some time, no physical search was made because by then, the dumping area would have been covered by several metres of landfill.[18]

---

14 Attorney-General's Department, *Submission No. 75*, pp. 3 and 5 and Treasury, *Submission 82*, p. 6.

15 Dr Ball, *Senate Hansard Transcript*, 4 November 2003, F&PA, pp. 65-6.

16 Mr Scales, *Senate Hansard Transcript*, 3 November 2003, ECITA, p. 41.

17 Mr Scales, *Senate Hansard Transcript*, 3 November 2003, ECITA, p. 42.

18 Dr Ball, *Senate Hansard Transcript*, 4 November 2003, F&PA, p. 66.

Laptop Computers

2.43 Laptop computers have proved to be the most attractive target for thieves and also, because of their small size, easy portability and marketability, the item of equipment most frequently lost. The Committee considered that reducing the loss rate for laptops should be a priority for all agencies – not only because of the monetary value of the equipment, but also because of the value of the information that may be lost or disclosed.

2.44 Each agency will need to make its own assessment of the best ways of achieving this aim. The Committee discussed with a number of witnesses, possible means of achieving tighter control over laptops and thus reducing the loss rate.

2.45 Several departments reported that their laptops were protected by encryption software, approved by DSD, which locked down their hard drives and operating systems to prevent unauthorised access. The Committee believes this policy should be adopted by any agency which has a need to carry classified information on its laptops.

2.46 DSD suggested that, given that the equipment is specifically designed for easy transport from place to place, the focus should be on better asset controls and on making individuals responsible for their safekeeping.[19]

2.47 The Committee considered which agency would be the most appropriate to introduce tighter security requirements for the use of portable electronic devices across government. The agencies considered were:

- the Department for Communications, Information Technology and the Arts and its portfolio agency National Office for the Information Economy (NOIE), which is responsible for promoting 'e-security';
- the Attorney-General's Department because unauthorised access to the information held on lost or stolen equipment could have national security implications;
- the Department of Finance and Administration (DoFA) because the loss of items in such numbers has financial management and asset management implications; and
- PM&C because it administers the *Public Service Act 1999* which outlines standards of behaviour expected of public servants.

2.48 Given the role of the Management Advisory Committee (MAC), the Committee concluded that PM&C is the most appropriate agency, particularly given that the implementation of the recommendation below

19 Mr Merchant, *Transcript*, 17 October 2003, p. 368.

will require the promotion of a broad change in behaviour towards greater security awareness across agencies.

2.49 In framing the recommendation below the Committee recognises the value of laptop computers in enabling flexible working arrangements such as working from home.

Recommendation 3

2.50 **The Department of Prime Minister and Cabinet introduce regulations that address the issuing and use of laptop computers and other portable electronic devices by Commonwealth agencies. The regulations should require that:**

- **such equipment is only issued to officers on a needs basis;**
- **such equipment is assigned to an individual, rather than to a work area, to ensure clear accountability;**
- **portable electronic devices are given password protection and, where they hold sensitive information, that data should be suitably encrypted;**
- **movement logs are made mandatory for valuable equipment taken outside agency premises ('valuable' here includes the significance of the information involved, as well as the monetary value);**
- **all thefts are reported to the police and to a central reporting body such as the Defence Signals Directorate; and**
- **regular inventory audits are conducted.**

Committee Comment

2.51 In relation to the reporting of security incidents, the Committee wishes to remind agencies of their responsibility to advise DSD of level 3 and 4 security breeches, which includes the loss of IT equipment. DSD should not have to chase agencies to obtain a report.

2.52 While acknowledging that complete elimination of theft may be impossible, the Committee expects agencies to reduce the level of theft through improved security procedures and better training.

2.53 Similarly it expects agencies to impress on their staff the responsibility they have to safeguard IT resources. The Committee anticipates that a security awareness program, combined with individuals taking greater responsibility for equipment assigned to them, will help to reduce IT losses. To aid the cultural change, IT security should also be included in all staff induction programs and staff members should be given regular refresher sessions thereafter.

2.54 The Committee has recommended that the theft of any piece of IT related equipment, whether a mobile phone or a laptop computer, should be reported to the police. In addition, IT thefts and security breaches should also be reported to agencies' audit committees to ensure there is 'whole of agency' recognition of the problem and of the impact on agency business.

2.55 Agencies should review back up storage plans including whether they need to encrypt all data in back-up storage, especially data stored off-site with an external provider. The necessity for this step will depend on the agency concerned, but the Committee believes agencies should err on the side of caution.

Asset Registration

2.56 Among other things, the recent incidents have shown that there are serious flaws in the system of asset registration and accounting in a number of agencies.

2.57 In the Customs case, it became apparent to the Committee that control of the asset register maintained by EDS was inadequate. On 28 August 2003 Customs inquired of EDS as to the possible loss of any equipment besides the two file servers that were originally notified as stolen.[20] It was not until 15 October 2003 that EDS confirmed to Customs that two desktop computers and a battery charger had been stolen at the same time as the file servers.[21] In giving evidence, EDS admitted that it was unable to immediately establish just what equipment had been stolen.[22]

2.58 This apparent lack of control of valuable assets (or, at the least, a sad lack of communication), was of concern to the Committee. A considerable amount of time went by after the theft was discovered before Customs

20 Ms Batman, Mr Woodward, *Transcript*, 17 October 2003, pp. 368-72.

21 Mr Woodward, Ms Batman, *Transcript*, 17 October 2003, pp. 374-5.

22 Mr Merchant, *Transcript*, 17 October 2003, p. 351.

and EDS both knew exactly what had been lost.[23] The Committee considers this unacceptable.

2.59 The lack of precision in the assets register was clearly illustrated when Customs said:

> We did not do a reconciliation between the previous asset register with the current one – I think the assumption … is that assets remain where they are forever. These assets are being moved around all the time-
>
> … It is not an unusual situation for PCs … to not be in the place you think they are, in an environment like this.[24]

2.60 Further evidence came from the Department of Defence, when it was unable to provide a detailed breakdown of its equipment losses prior to 2002-03.[25]

2.61 The potential seriousness of the loss of portable IT equipment was demonstrated by an incident in the United Kingdom in December 1990. A Ministry of Defence laptop, which had been left unattended in a private car, was stolen. The laptop contained extremely sensitive military plans on the upcoming Desert Shield campaign in Iraq. The incident also demonstrates the importance of a robust security culture.[26]

2.62 The impression of an overall lack of control and accountability of IT assets is heightened when the lengthy list of lost equipment reported by agencies, is considered. The Committee suggests that this would be a suitable area for review by ANAO in the near future.

23 Mr Woodward, Ms Batman, *Transcript*, 17 October 2003, pp. 352-7.

24 Mr Harrison, *Transcript*, 17 October 2003, p. 359.

25 Minister for Defence, *Submission No. 86*, p. 1.

26 *The Independent*, 31 December 1990.

Recommendation 4

2.63 **The Australian Government Information Management Office (AGIMO) ensure that Commonwealth agencies:**

- **have up-to-date asset registers of all IT equipment owned by them and used on their premises; and**
- **undertake a regular audit and reconciliation program of all owned and leased IT equipment.**

AGIMO should advise the Committee, in an Executive Minute, of the completeness of the registers and the audit procedures that have been established.

2.64 The publicity on the theft of IT equipment that resulted from this Committee's inquiry, particularly the loss of the two servers from the Customs facility at Mascot Airport, has dramatically changed department security procedures. The Chief Executive Officer of Customs stated that:

> We have taken physical steps to deal with access to the building [at Mascot] security steps in relation to the computer room and steps in relation to accompanying people when they go on site … we are having a comprehensive look at security throughout Customs, with one of the major requirements being security plans that will be site specific – so that each site will need to have a security plan and an obligation that the security plan is complied with.[27]

2.65 This incidence of reporting of the breaching of the security of Commonwealth electronic information systems clearly demonstrates the link between transparency and increased accountability of agencies.

27 Mr Woodward, *Transcript*, 17 October 2003, p. 368.

3

Management of Outsourcing Contracts

3.1 In 1997 the Government determined to outsource its IT infrastructure and aggregate services within and across groups of agencies. The initiative aimed at :

(i) complementing modern management practices;

(ii) enhancing access to wider technical skills and technologies; and

(iii) introducing discipline into the use of technology, to achieve economies of scale and reduce overall costs.[1]

3.2 This chapter considers the management implications of outsourcing for the control and security of electronic information held by Commonwealth agencies. Outsourcing requires carefully written contracts to ensure that network control and security remains firmly with the agencies and is not devolved in any way to contractors and sub-contractors.

3.3 Evidence given by witnesses to the inquiry, indicated that there are some management problems presented by the practice of outsourcing IT services including:

- adverse impacts that the security requirements of one agency can have upon the security requirements and cost effectiveness of other agencies when they are inappropriately grouped together under clustered contracts;[2]

---

1 Richard Humphry, *Review of the Whole-of- Government Information Technology Outsourcing Initiative* (Humphry Review), December 2000, p. 4.

2 ANAO, *Submission No. 42*, p. 2.

- failure to specify expected service levels and clear performance indicators in contracts;[3]
- uncertainty of access to Commonwealth data held by outsourced service providers;[4]
- costs and inefficiencies caused by service providers resetting passwords;[5] and
- lack of monitoring of outsourced service providers for compliance with their privacy obligations.[6]

3.4 Agencies need to take these issues into account in outsourcing contracts and build them into agency risk assessment calculations.

3.5 The 'Humphry Review' of the IT outsourcing initiative in 2000 included consideration of possible breaches of privacy, security and confidential undertakings. The review proposed that chief executives or boards of the various Commonwealth agencies and authorities should be given full discretion to determine what functions should be outsourced and how that should be done.[7]

3.6 Among the problems with outsourcing revealed to the Committee by the evidence, was a degree of loss of communication on IT issues between sectors of an agency, when IT functions are outsourced. ANAO commented that '… agencies that had not contracted out … had better communication within the different components of the entity'.[8]

3.7 ANAO also found that this was an important factor in relation to the management of information on-line. It said that where in-house resources were used to manage Commonwealth websites, communication between groups was better than when an outside contractor was used.[9]

3.8 The Committee accepts that the quality of communication between Commonwealth agencies and service providers will depend on the quality of the contract and management of arrangements between these entities. The Committee notes that there appears to be a correlation between maintaining IT functions in-house and security management.

---

3 ANAO, *Submission No. 42*, p. 3.
4 Mr Taylor, *Transcript*, 1 April 2003, p. 110.
5 Mr Wilson, *Transcript*, 2 April 2003, pp. 155-6.
6 ANAO, *Submission No. 42*, p. 3.
7 Humphry Review, p. 6.
8 Dr Nicoll, *Transcript*, 31 March 2003, pp. 6.
9 ANAO, *Submission No. 17*, p. 12.

Accountability Remains with Agency

3.9 Most importantly, contracting functions to an outside body does not reduce an agency's responsibility for IT security. As ANAO commented:

> In the end the agency has to be aware of its own risks in transacting business electronically. You cannot contract that out.[10]

3.10 The Health Insurance Commission (HIC) agreed with that opinion when the Commission noted that:

> In relation to our outsourcing arrangements with IBM GSA, the types of services under that are infrastructure services, so the asset ownership is with IBM GSA, as are the services to operate, run and maintain those infrastructure assets. In terms of security, the HIC retains responsibility for the management of security, and certainly IBM GSA provide some security related services for us under that arrangement.[11]

3.11 In its evidence, the contractor EDS also recognised this point and said that the Commonwealth agency is '… the custodian of the information. It holds the information in trust …'.[12]

3.12 Despite the difficulties involved in IT outsourcing, however, the Department of Employment and Workplace Relations (DEWR) acknowledged that it does have its place and, at times, agencies are left with no other choice than to engage a contractor:

> … where there are specialist niches of technology or where there are bursts of requirement that we cannot sensibly fill, ... then, of course, we are relying on IT contractors.[13]

3.13 There are many problems which can arise if an agency allows its control of security to relax. One example found by ANAO in the course of its audit program, arose when contractors further subcontracted parts of the work, without informing the responsible agency. ANAO commented:

> … the agency should know who is going to work on these projects … if somebody has access to the data on the IT system and they happen to be a subcontractor, you need to be aware … of any conflict of interest.[14]

---

10 Mr Meert, *Transcript*, 31 March 2003, p. 6.
11 Ms O'Connell, *Transcript*, 2 June 2003, p. 234.
12 Ms Whittaker, *Transcript*, 1 April 2003, p. 85.
13 Mr Burston, *Transcript*, 31 March 2003, p. 65.
14 Mr Meert, *Transcript*, 31 March 2003, p. 7.

3.14 The Committee wishes to emphasise, that accountability for the good management and security of agency networks remains with the agency, regardless of whether elements of network activity are outsourced.

When is Outsourcing Appropriate

3.15 In response to a question from the Committee regarding difficulties with some outsourcing contracts, ANAO said that an agency can only control or direct what a service provider does through the terms of the contract. It is essential, therefore, that the parameters are clearly established when negotiating the contract.[15]

3.16 Some agencies have decided not to outsource IT functions or, at least, to limit the functions contracted out to the less sensitive areas. The Australian Bureau of Statistics (ABS), for example, commented:

> We are largely self-reliant; self-servicing. We own and operate our own IT infrastructure and we own the vast bulk of it and operate the vast bulk of it. We were not one of the parties to the outsourcing clusters.[16]

3.17 In response to questions about the continuation of their outsourcing contract with Telstra following a serious security incident, DoTaRS said that it was market testing to find a new provider and would not simply roll over the contract. It said that '… DoTaRS has actually taken steps to find alternative ways of getting its IT needs met.'[17]

3.18 One decision already taken, DoTaRS indicated, was that security management would no longer be part of the outsourcing contract. In its evidence to the Committee, DoTaRS asserted that the security function would, in future, be handled in-house.[18]

3.19 Other agencies have built safeguards into their outsourcing contracts. DEWR, for instance, requires its contract or account managers to regularly undertake monitoring visits to the contractors. A task of major importance in these visits is to ensure that the contractor can show that it has fulfilled its obligations regarding the privacy of personal data.[19]

---

15 ANAO, *Submission No. 42*, Attachment A.

16 Mr Palmer, *Transcript*, 31 March 2003, p. 35.

17 Mr Fisher, *Transcript*, 17 October 2003, p. 362.

18 Mr Banham, *Transcript*, 17 October 2003, p. 365.

19 Mr McMillan, *Transcript*, 31 March 2003, p. 63.

3.20 This course is strongly encouraged by ANAO, which found in its report on the *Implementation of Whole-of-Government Information Technology Infrastructure and Outsourcing Initiative,* that there were considerable differences in the approaches by various agencies. Some gave security aspects a high priority in their preparations for outsourcing; others '… appeared to have been less active, with scope for improvement in the extent, and timing, of attention to the recommended preparatory steps … in tenders'.[20]

3.21 The Committee notes that recommendations 16 to 20 of the ANAO report reflect the importance of security considerations in the outsourcing of Commonwealth IT services. The Committee also notes that the Commonwealth Government agreed with each of these recommendations.

3.22 The ANAO report also recommended that DSD have an active role in consulting agencies on IT outsourcing arrangement (Recommendation 18) and this supports the DSD's suggestion to the Committee that it has considerable value to add to this process and added that it would be happy to work with agencies in the development of their IT outsourcing contracts.[21]

Addressing Security Issues in Outsourcing Contracts

3.23 ANAO recommended that, where appropriate, all agencies should:

> … develop, in consultation with [DSD], an integrated security architecture strategy that addresses operational security issues, identifies the necessary security safeguards and the required timetable for their implementation by the external service provider.[22]

3.24 If such arrangements are implemented correctly, ANAO indicated that there could be '… an improvement over the internal security arrangements previously existing within agencies.'[23]

3.25 ANAO noted that if contracts are properly framed, the problem of unauthorised sub-contracting should never arise. Provisions preventing the main contractor from sub-contracting, without the knowledge and approval of the responsible Commonwealth agency, should be a standard

20 ANAO, *Submission No. 42*, Attachment A.
21 Mr Merchant, *Transcript*, 17 October 2003, p. 394.
22 ANAO, *Submission No. 42*, Attachment A.
23 ANAO, *Submission No. 42*, Attachment A.

part of outsourcing contracts. ANAO found that, in practice, that was generally the case and that sub-contractors are normally required to sign non-disclosure agreements and prohibited from using the equipment for other clients unless specified security requirements are met.[24]

3.26 The MAC report on *Australian Government Use of Information and Communications Technology*, found that the security aspects of outsourcing contracts have not been as prescriptive as they might have been.[25]

3.27 The report noted that the MAC's Chief Information Officer's Committee[26] plans to encourage information exchange between Commonwealth agencies on their experiences in administering outsourcing contracts. It also concluded that Commonwealth agencies have a need to improve contract management skills and suggested that they draw on the work of the ANAO to assist in the task.[27]

3.28 The JCPAA noted that one aspect of outsourcing contracts which is in need of attention is the provision of sanctions for failure to carry out the terms of a contract. When taking evidence on the IT contract held by Customs (see Chapter 2 for greater detail), it became apparent to the Committee that the cancellation of IT contracts as a sanction may be, in practical terms, unenforceable.

3.29 Under some contracts, the contractors own the IT assets used by the Commonwealth agencies. Cancellation of such a contract could place an agency in the impossible short term position of having no IT assets at all. As per Recommendation 2 of this report, the Committee recommends that contracts need to include a graduated and realistic range of sanctions that can be invoked if necessary, rather than just providing the options of cancellation or non-renewal.

---

24 ANAO, *Submission No. 42*, Attachment A.

25 The MAC is a forum of Secretaries and Agency Heads established under the *Public Service Act 1999*. It is chaired by the Secretary of the Department of the Prime Minister and Cabinet with the Public Service Commissioner as executive officer. It is charged with advising the Government on matters relating to the management of the Australian Public Service (APS). While it has no statutory powers or executive functions, it provides a forum for secretaries and heads of major agencies to discuss significant issues of topical and long-term interest to the APS.[25]

26 The Chief Information Officer's (CIO) Committee consists of fourteen members and is drawn from both key central agencies and agencies that are high users of Information and Communication technology.

27 MAC, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, p. 22.

Addressing Privacy Issues in Outsourcing Contracts

3.30 The Privacy Commissioner noted in his Submission that contractors to Commonwealth agencies were not directly covered by the Privacy Act until 21 December 2001. Until that date, it was the contracting agency itself which was required by the Act's IPPs, to take responsibility for the contractor's handling of the information. In particular, IPP 4(b) required:

> A record-keeper who has possession or control of a record that contains personal information shall ensure: … (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.[28]

3.31 The December 2001 amendments to the Privacy Act have assisted in this area by requiring the contracting agencies to include contractual provisions that '… ensure that contractors and sub-contractors are bound to comply with the IPPs'. [29]

3.32 In addition, the amendments to the Act provide that failure to abide by these contractual obligations regarding privacy, constitutes an 'interference with the privacy' of the individuals to whom the records refer. The new provisions allow the Commissioner to investigate such breaches directly with the contractor.[30]

3.33 Nonetheless, outsourcing gives an outside entity, usually from the private sector, access to information, often sensitive information, collected by the Commonwealth. The rapid growth in on-line services makes it important that Commonwealth agencies set a very high standard of integrity and privacy in administering the data they hold. It is equally important that the public is aware of the high standard being applied.

3.34 The onus is on agencies, to not only protect the information they hold for the sake of its value to the Commonwealth, but also to protect the privacy of the individuals whose information is being held.

3.35 The Committee believes that all agencies should co-operate closely with the Privacy Commission to ensure that outsourcing contracts contain adequate protections for privacy. The Committee notes that the Privacy Commission requires adequate resources to fulfil this function.

---

28 Federal Privacy Commissioner, *Submission No. 33*, p. 24.

29 Federal Privacy Commissioner, *Submission No. 33*, p. 25.

30 Federal Privacy Commissioner, *Submission No. 33*, p. 25.

Committee Comment

3.36 Notwithstanding Recommendation 2 of this report, the Committee makes the following additional comments.

3.37 The Committee observed that for agencies electing to outsource their IT functions, it is vital that the contracts are tightly written and well managed. The Committee is concerned that many agencies still face a considerable amount of work to achieve best practice in this area.

3.38 There are any number of government guides at the Commonwealth and State level about contract management. At the Commonwealth level, the ANAO's *Better Practice Guide - Contract Management*, provides detailed advice, as will the ANAO, DoFA and, for IT security, DSD. Agencies should avail themselves of this advice.

3.39 In the context of this inquiry, particular attention should be given to the security and privacy related provisions of contracts. Similarly, agencies should also ensure they have available a range of graduated and realistic sanctions short of contract cancellation that can be applied if necessary.

3.40 The Committee is particularly concerned about the physical security issues raised by outsourcing - an issue discussed in Chapter 2. However, in relation to the terms of outsourcing contracts, the Committee also urges agencies to consult DSD to ensure that the security related provisions included in those contracts are adequate.

4

Risk Management

Introduction

4.1 This chapter examines the security risks involved in the movement of electronic messages and other data, particularly sensitive data, where unsecured public communication networks – such as the Internet – must be used.

4.2 The Internet is an environment of constant, low-level threat. A computer connected to the Internet faces a potential threat from any of the millions of other computers that make up the so-called World Wide Web. A 'cracker'[1] on any one of these computers can attempt illegal access.

4.3 Most threats are easily defended against. Virus scanners can be kept up to date and vulnerabilities can be closed with the latest software patches. EDS indicated that:

> In the case of the Melissa virus, which first manifested itself in North America, we were able to advise our customers here and close the gateways so that the virus did not have an impact on our customers. The Slammer was actually detected by our team in South Australia, who were responsible for not only informing our customers in this country and isolating the servers that could have been impacted but informing the world of the Slammer virus.[2]

---

1 A cracker is a person who breaks the security on a computer system, usually for malicious or destructive purposes.

2 Ms Whittaker, *Transcript*, 1 April 2003, p. 88.

4.4 In rare cases exploitation may occur before countermeasures are available. The Committee heard that the 'I Love You' virus infiltrated DoFA.[3] In such cases, prompt action will be necessary to temporarily protect the system until a more permanent solution is available.

4.5 The ANAO recommends that agencies adopt a structured approach to the management of Internet security, employing a sound risk management model. It also recommends that agencies ensure that appropriate risk assessments are conducted prior to introducing a new IT system or instituting major changes to an existing system[4].

4.6 Commenting on the need for regular risk assessment in its *Guidelines for the Security of Information Systems and Networks*, the OECD encouraged an active program. It said that risk assessment should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications:

> Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected.[5]

Broad Risk Management

4.7 Risk assessment and management must be applied broadly and continuously and must cover all areas of the computer system. This includes not only the computer hardware and software, but everything that comes into contact with the system.[6]

4.8 Effective risk management is an unending project. Threats to computer systems are constantly evolving, with new vulnerabilities discovered and exploited on an almost daily basis.[7] Even a system that has initially been thoroughly secured can quickly become insecure.

---

3 Mr Nicholson, *Transcript*, 2 June 2003, p. 247.

4 ANAO, *Submission 17*, p. 12; ANAO Audit Report No. 13 2001-2002, *Internet Security within Commonwealth Government Agencies*, p. 23.

5 OECD, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Paris, 2002, p. 11.

6 Check Point Software Technologies (Australia) Pty Ltd, *Submission No. 9*, p. 19.

7 Check Point, *Submission No. 9*, p. 16.

4.9 Check Point Security Technologies (Australia) Pty Ltd recommends that risk management for computer systems be applied to all of the following areas:[8]

- Exterior security – fencing, lighting, building location;
- Secured dumpsters – disposal of confidential information;
- Building security – key-locked doors, biometric authentication, physical guards, cameras;
- Departments - logically broken up, kept secure;
- Passwords – elimination of Post-It notes stuck under a keyboard or on the side of the monitor, with user ID and password;
- Computer / Data Centre – environmental controls, fire and cable management, secure consoles;
- Data Classification – confidential, secret, need-to-know;
- Access groups – assigned by user and / or group;
- Human Resources and IT staff coordination;
- Unauthorised modems; and
- Social Engineering – persons pretending to be an employee or maintenance worker to gain unauthorised access.

4.10 The initial parts of this list, dealing with physical security, were examined in Chapter 2. This chapter concerns itself with the prevention of attempts to access the electronic data itself.

Risk Management Lifecycle

4.11 Continuous risk management can be illustrated by a risk management lifecycle, which proceeds through a series of fixed stages. Immediately it completes the last stage, it reverts to the beginning and restarts. System administrators may start a new instance of the lifecycle for each new threat and need not complete the previous one before restarting.

4.12 There are various ways of approaching the task of applying a risk management lifecycle. Submissions from Check Point and EDS set out detailed steps by which an effective program could be established.[9]

4.13 The common elements of those proposals make up a simple risk management lifecycle of three stages: Analysis, Implementation and Testing. Check Point also proposes additional precautions through an initial stage of Perimeter Protection, performed before the first Risk

8 Check Point, *Submission No. 9,* p. 19.

9 Check Point, *Submission No. 9,* pp. 17-21 and EDS, *Submission No. 6,* p. 7.

Assessment is made and an Intrusion Detection System that operates throughout the lifecycle.

Analysis

4.14 Analysis is the process of identifying potential threats to a computer system – what the ANAO described as '… formally identifying risks across the range of organisational activity'.[10]

4.15 In order to carry out an effective analysis, a system administrator must know and understand all of the components of the computer system: what they are, how they work and the current threats to those components. System administrators can also supplement this analysis through penetration testing and review.

4.16 Based on this knowledge administrators will then be in a position to proceed by:

> … evaluating the identified risks based on the likelihood that the event will occur and the potential impact on the entity's activities and functions …[11]

System Components

4.17 If system administrators do not know that a particular component is installed on the computer system, then they will not look for reports of vulnerabilities in that component. In this event, even when vulnerabilities have been discovered and corrected by the vendor, the system will remain at risk because the administrators, being unaware of any weakness, will not have implemented the necessary corrective action.

4.18 Similarly, system administrators must know what each component does. If it has functions that they are unaware of, then the system may be vulnerable in a way that they do not guard against. For example, a software program may interact with the Internet without the user or the system administrators being aware of it.

4.19 In relation to risk management, the DSD offered the general advice that '… wireless devices should not be allowed and wireless networks should not be created … [because of] the inherent insecurity.'[12]

4.20 Hardware and software can often be used 'out of the box', using a default configuration. This means that system administrators could set up a

10 ANAO, *Capitalisation of Software*, Audit Report No.54 2002-2003, p. 35.

11 ANAO, *Capitalisation of Software*, Audit Report No.54 2002-2003, p. 35.

12 Mr Burmeister, *Transcript*, 17 October 2003, pp. 389-90.

system, but still not have detailed knowledge about the software and hardware being installed. Such a system may contain components and have functions that the administrators are unaware of. For this reason, the ANAO recommends that agencies avoid default installations of operating systems and web server software[13].

4.21 Even if a system administrator has detailed knowledge of the system, unless that knowledge is committed to writing, it will be lost if that person leaves and a new administrator takes over. The new system administrator may be able to run the system without their predecessor's detailed knowledge, but may be unaware of some of the installed components and so unable to fully protect the system.

4.22 Agencies should avoid these situations by building and maintaining a database of all hardware and software components installed on their computer systems. This would allow a new system administrator to very quickly know which components are installed and what they do. If a weakness is then advised for a particular component, they would know whether or not the system included this component and needed to be protected.

Threat Awareness

4.23 In order to carry out an effective threat analysis, system administrators must learn of newly discovered vulnerabilities as soon as possible. There are many ways that they can be reported by vendors and other interested parties. System administrators need to keep a close watch on all of these sources.

4.24 A number of web sites publish reports on viruses and other computer security threats. These include the *Symantec Security Response* site[14] and the *McAfee Security* site[15]. Threats are reported on these web sites as soon as they become known. Security reports include an assessment of the threat and suggested countermeasures.

4.25 A number of computer system suppliers maintain web sites that report on security threats to their products. These include Microsoft's *Technet Online* site[16], the *Oracle Technology Network Security* site[17], the Sun Microsystems

13 ANAO, *Submission No. 17*, p. 13; ANAO, *Internet Security within Commonwealth Government Agencies*, Audit Report No. 13 2001-2002, p. 23.

14 Symantec Security Response, http://www.symantec.com/avcenter, 28 October 2003.

15 McAfee Security, http://www.mcafee.com/anti-virus/default.asp, 28 October 2003.

16 Technet Online, http://www.microsoft.com/technet/, 28 October 2003.

17 Oracle Technology Network – Security, http://otn.oracle.com/deploy/security/alerts.htm, 28 October 2003.

Security Information site[18] and the *Netscape Security Center* site[19]. These web sites alert users as threats to their products become known and offer fixes and patches to remove vulnerabilities.

4.26 Other resources include user groups, technical discussion forums, journals and books.

4.27 System administrators must consult all of these resources frequently and systematically, in order to keep up with the latest threats to their computer networks and the recommended countermeasures.

4.28 Unfortunately, not all threat reports are genuine; some are hoaxes.[20] Others may be malicious and following their instructions will create a new vulnerability on the computer system.[21] System administrators therefore need to be wary and only heed threat reports that can be corroborated or come from a reputable source.

Incident Reporting

4.29 DSD maintains an incident reporting scheme called ISIDRAS. This scheme collects and analyses information on security incidents as an aid to the protection of Government computer systems.

4.30 The information collected by ISIDRAS is used to compile Security Advisory reports, which are available to all agencies and members of the public on DSD's *Computer Security Advisories* web page.[22] However, not all agencies are reporting incidents to ISIDRAS. For example, Centrelink told the Committee that it only reports the most serious of incidents[23], while CSIRO does not report to ISIDRAS at all because of the volume of information that it handles.[24]

4.31 DSD classifies incidents into four categories:

- Category 1: events not definitely identified as an attack;
- Category 2: unsuccessful attacks;

---

18 Security Information, http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec, 28 October 2003.

19 Netscape Security Center, http://wp.netscape.com/security/index.html, 28 October 2003.

20 e.g. Symantec Security Response - Jdbgmgr.exe file hoax, http://www.symantec.com/avcenter/venc/data/jdbgmgr.exe.file.hoax.html, 28 October 2003.

21 e.g. Symantec Security Response - SubSeven 2.0 Server, http://www.symantec.com/avcenter/venc/data/sub.seven.20.html, 28 October 2003.

22 Computer Security Advisories, http://www.dsd.gov.au/advisories/advisories.html.

23 Ms Treadwell, *Transcript*, 31 March 2003, p. 30.

24 Mr Morrison, *Transcript, 1 April 2003,* p. 129.

- Category 3: successful attempts to breach security but with only minor effects on system operations; and
- Category 4: Successful attempts with major consequences.

4.32 Of the four Categories, reporting to ISIDRAS is only mandatory for Categories 3 and 4. DSD acknowledges that if all incidents were reported the system would be overwhelmed:

> It is very much the view of the people in our network vulnerability team that if you move to a mandatory reporting regime for all levels of incidents we would be swamped with information which would not really give us any additional insights.[25]

4.33 DSD commented that one of the problems they encountered is that agencies often do not prepare all of the documentation needed to fully explain their network:

> When we work with departments to give advice on how they should set up IT infrastructure, there is a general set of documents that they ought to produce that we would then review. That includes security plans, architectural and network diagrams – things that we can help them develop. … there are certainly a number of documents that we would expect every agency to have so that they completely understand the nature of their networks.[26]

4.34 When asked by the Committee whether agencies, in practice, had that documentation, DSD responded:

> … I think you would probably find that the answer is no.
>
> When we do work with agencies and do security audits with them, our experience is that often the documentation is not complete or is out-of-date.[27]

4.35 In discussing the losses of IT equipment examined by the Committee, DSD commented:

> For the purposes of ISIDRAS, we would consider physical loss of equipment to be probably a level 3 incident. So it really is a mandatory reportable incident – and a number of people have been surprised when we have said that.[28]

4.36 DSD said that the reports that are being received from agencies '… give us an overview of the level of sophistication of attacks that people will

---

25 Mr Merchant, *Transcript, 16 June 2003,* p. *262.*

26 Mr Burmeister, *Transcript*, 17 October 2003, p.393.

27 Mr Burmeister, *Transcript*, 17 October 2003, p.393.

28 Mr Burmeister, *Transcript*, 17 October 2003, p. 392.

experience over the public network.'[29] It added that whereas previously agencies which notified incidents received very little feedback or direct assistance:

> We are now providing a response capability to agencies. If they do have a problem and report it to us, we can help them fix the problem, identify it and make sure it does not happen again for them. So there are now people at the end of the line who will be able to work with them to fix any problems they identify.[30]

4.37 The Committee noted that ISIDRAS is the only scheme for reporting IT security incidents and potential security breaches, which operates throughout Commonwealth agencies. DSD indicated, however, that the system was not widely known, nor were the reporting requirements well understood:

> … I have to say that we do actually have a fairly proactive line with incident reporting. If we hear about something and a department has not told us, we will go and seek a report. Often it turns out that they are not aware of the scheme – which is one of the things we are trying to improve. If they are aware of the scheme they are not necessarily aware of what each of the levels means and which incidents they need to report to us.[31]

Recommendation 5

4.38 **The Australian Government Information Management Office, in consultation with the Defence Signals Directorate, reiterate to all Commonwealth agencies their responsibility to comply with the reporting requirements of the Information Security Incident Detection, Reporting and Analysis Scheme particularly the mandatory reporting of category 3 and category 4 incidents.**

Penetration Testing

4.39 Penetration testing is a controlled attempt to gain unauthorised access to the computer system. If it succeeds, then it has identified a vulnerability in the system. This method is an effective test of the internal and external

29 Mr Burmeister, *Transcript*, 16 June 2003, p. 262.

30 Mr Burmeister, *Transcript*, 16 June 2003, p. 263.

31 Mr Burmeister, *Transcript*, 17 October 2003, p. 392.

security of the computer system.[32] Centrelink carries out penetration testing as an established part of its security measures.[33]

4.40 Penetration testing must be carried out by a person or organisation with no inside knowledge of the computer system. This reflects the circumstances of a cracker trying to gain unauthorised access to the system.[34]

4.41 It is important that penetration tests be carried out in controlled circumstances. In November 2002, a Commonwealth Government agency received an e-mail survey, purportedly from the ABS. Users who responded would have compromised the security of their agency. This e-mail was part of a penetration test performed by a private security company on behalf of another government agency. Neither the ABS, nor the agency being tested, had known that the name of the ABS would be used in the e-mail.[35]

4.42 Any agency conducting a penetration test must be aware of exactly what is to be done, how it is to be done, any possible consequences that may arise and any recovery or response processes which need to be put in place.[36]

Review

4.43 A review involves examining the computer system in detail. It is a long and laborious process, but can be very thorough in locating vulnerabilities. Each component of the system can be examined separately.

4.44 Hardware and software components can be reviewed by their observed behaviour and by examination of the accompanying documentation.

4.45 Open source software allows system administrators to examine source code and determine the behaviour of software components in the greatest detail. The Committee heard that:

---

32 Check Point Software Technologies (Australia) Pty Ltd, *Submission No. 9*, p. 20.

33 Centrelink, *Submission No. 18*, p. 1.

34 Check Point Software Technologies (Australia) Pty Ltd, *Submission No. 9*, p. 20.

35 Defence Signals Directorate (DSD), Information Security Group Computer Security Advisory DA2002-05, Hoax E-mail, November 2002, http://www.dsd.gov.au/_lib/pdf_doc/advisories/da2002-05hoax.pdf, 28 October 2003.

36 DSD, Information Security Group Computer Security Advisory DA2002-05, Hoax E-mail, November 2002, http://www.dsd.gov.au/_lib/pdf_doc/advisories/da2002-05hoax.pdf, 28 October 2003; DSD, Information Security Group Computer Security Advisory DA 2002-06 IT Security Audit Guidance and more on E-mail Hoax Advice (DA 2002 –05), 26 November 2002, http://www.dsd.gov.au/_lib/pdf_doc/advisories/da2002-06moremailhoax.pdf, 28 October 2003.

> The issue of access to source means that an enormous amount of peer review goes on. Certainly, not everyone who uses an open source system looks at the source code, but 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.[37]

4.46 In response to this line of criticism, Microsoft Australia informed the Committee that it had launched a Government Security Program which will give key government security agencies access to the source code on its products. [38] Negotiations on the participation of Commonwealth agencies in this program were completed to the satisfaction of DSD in 2003.

4.47 System processes in a network can be reviewed by examination and analysis and by interviews with the people responsible for carrying them out. The practical experience of the users can be used to reveal flaws that are not readily detectable by other methods.

4.48 ANAO recommends that agencies ensure that applications supporting transactions with users be reviewed regularly for secure coding practices.[39] DSD uses a detailed review of the relevant system as part of its accreditation process.

Implementation

4.49 Implementation is the process of modifying the computer system so that it is no longer vulnerable to the threats identified in the Analysis stage. Methods of implementation include applying a patch which eliminates the weakness, or instituting a temporary arrangement to work around the problem until the solution becomes available (known as a 'work around').

Patches

4.50 The simplest way of addressing a software vulnerability is to apply a patch; that is, a piece of software that modifies the system's existing software.

4.51 When a software provider learns of a problem affecting one of its products, it will usually act quickly to develop a patch that removes the

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

38 Microsoft Australia, *Submission No. 64*, p. 1.

39 ANAO, *Submission. 17*, p. 13; ANAO, *Internet Security within Commonwealth Government Agencies*, Audit Report No. 13 2001-2002, p. 24.

vulnerability. The patch is then made available to users through the company's web site.

4.52 The ATO has built this requirement into its system processes. The measures applied within its system to protect electronic information during transmission, require it to apply the latest patches to software as soon as they are available.[40]

4.53 Microsoft pointed out that unless IT managers regularly patch their systems, vulnerabilities will continue to exist even when they have been recognised and addressed by the original software developer.[41] To suggestions that a disadvantage of closed source systems is that they require continuous security responses Microsoft responded that the high incidence of attacks upon its operating systems and platforms testified to the popularity of these products.[42]

4.54 For serious vulnerabilities, it is critical that the provider release the patch as soon as possible. Until the patch is available, most of their users will be vulnerable. Lately, software providers like Microsoft Australia have improved response times and have been releasing patches in a timely manner, often before any major attack has occurred.[43]

4.55 The Australian UNIX and Open Systems Users Group (AUUG) acknowledged the improved timeliness of the provision of patches by closed source vendors, but stated that patches had not always been made available in adequate time frames and that this may also be the case in the future.[44]

4.56 In some cases, the patch may have been developed very quickly so that it could be released as soon as possible. Because of this, it may not have undergone proper quality control. Consequently, installing a patch may have unintended consequences, including introducing a new vulnerability or causing the computer system to become unstable. System administrators should therefore be cautious when installing patches. Each one should be carefully tested before being applied to a live system.

4.57 ANAO strongly recommends that agencies test and install security patches in a timely manner.[45]

---

40 Australian Taxation Office, *Submission No. 14*, p. 12.

41 Microsoft Australia, *Submission No. 12*, p. 5.

42 Mr Russell, *Transcript*, 16 June 2003, p. 281.

43 Mr Vohra, *Transcript*, 31 March 2003, p. 49; Mr Paddon, *Transcript*, 2 April 2003, p. 165.

44 Mr Paddon, *Transcript*, 2 April 2003, p. 165.

45 ANAO, *Submission 17*, p. 13; ANAO, *Internet Security within Commonwealth Government Agencies*, Audit Report No. 13 2001-2002, p. 23.

Correcting a Vulnerability

4.58 If the system administrators understand enough about their computer system, then they may try to fix the vulnerability themselves.

4.59 Open source software can be fixed by system administrators because the source code is included in the software release. Fixing the problem may involve changing the source code and recompiling the software. Information on how to do this is often included in the report of the vulnerability released by the software provider.

4.60 Source code is often large and complicated and altering it may have unintended consequences. System administrators should be cautious when altering source code and always test any changes before implementing them on a live system.

4.61 Closed source software cannot be fixed by the system administrators. When a vulnerability is found, the administrators must wait for the provider to release a patch. This may limit agencies' control and create additional risk.

4.62 If a vulnerability is discovered in a hardware component, the system administrators may be able to fix it by replacing the component or altering its configuration. If the problem is in a process, the system administrators must alter the existing process or implement a new process that avoids the problem.

4.63 ANAO recommends that risk assessment techniques be applied at the process-level with the aim of enhancing control structures, detection of control weaknesses and prevention of breakdown; all of these improvements leading to increased operational efficiency.[46]

Working Around a Problem

4.64 The situation may arise where a threat requires immediate action, but the necessary patch is not yet available so that the problem cannot be immediately fixed by the system administrators. Alternatively, there may not be time to properly identify the threat and implement a specific solution.

4.65 In these cases, it may be necessary for the system administrators to institute a 'work-around'. This is a temporary change that will avoid the vulnerability until a better solution can be implemented. Once the problem has been overcome, the administrator may remove the work-around.

46 ANAO, *Capitalisation of Software*, Audit Report No.54 2002-2003, p. 35.

4.66 In extreme cases, a work-around may involve shutting down the computer system or disconnecting it from the internet. Measures like these may be necessary to protect the system from a particularly dangerous virus or a Denial of Service (DoS) attack.

4.67 In less serious cases, a work-around may involve blocking some kinds of internet traffic or disabling some of the system's functionality, to prevent it from being compromised.

Testing

4.68 Testing is the process of verifying that the modifications made in the Implementation stage effectively protect the computer system from the threats identified in the Analysis stage. The process may include a controlled simulation of an attack which targets an identified area of vulnerability.

4.69 The testing process must cover the entire system, to ensure that the solution has not introduced any new vulnerability or other unintended consequences.

Committee Comment

4.70 The Committee noted the concerns expressed by various witnesses, regarding the necessity for continual awareness of changing threats to a computer system. It stressed the necessity for administrators to know their system in detail.

4.71 The Committee noted with concern the comments by DSD about the lack of complete and up-to-date documentation on agencies' IT network architecture. The Committee expects Commonwealth agencies to consult with DSD and to complete the necessary documentation without delay.

4.72 The debate between the security advantages associated with closed and open source systems is on-going. The Committee accepts that each of these systems has advantages and disadvantages and agencies should be aware of the opportunities offered by each type of system.[47]

47 Ms Connick, *Transcript*, 16 June 2003, p. 261.

Recommendation 6

4.73 **The Australian Government Information Management Office (AGIMO) monitor and report on the performance of Commonwealth agencies:**

- **implementation and maintenance of a flexible and responsive security risk management strategy for IT networks including hardware, software and data protection; and**
- **maintain an awareness of current and emerging threats to their computer networks and the recommended countermeasures.**

AGIMO should advise the Committee in an Executive Minute, of the status and completeness of these arrangements.

5

Data Preservation

Introduction

5.1 Commonwealth recordkeeping is in the midst of a major shift in focus. For many years recordkeeping in Commonwealth agencies was overwhelmingly paper-based. In recent years, however, the rapid growth in the use of electronic messaging and storage systems has drastically changed the requirements.

> The National Archives of Australia has the task of ensuring that there is a full and accurate record of Government business. The changes flowing from the rise of electronic recordkeeping have presented NAA with the additional task of radically changing the way that government records are maintained.[1]

5.2 In reassessing its role, NAA produced a Green Paper in 2002, to promote discussion among Commonwealth agencies and to make government employees aware of the importance (and difficulty) of the task. The paper said that the rate of change had increased with the widespread introduction of computers into the workplace and had '… dramatically altered the way in which employees work, communicate and share information.' It continued:

> These changes have made recordkeeping both more difficult and more significant. For many years lack of attention to recordkeeping has been mitigated by the existence of long-standing, well known practices for the use of paper records. Paper

---

1 Helen Heslop, Simon Davis and Andrew Wilson, *An Approach to the Preservation of Digital Records*, National Archives of Australia, December 2002, pp. 5-6.

> records also have a robustness that enables them to survive long periods of neglect. In contrast, the sometimes haphazard use of electronic systems for communication and storing recorded information is more fragile.[2]

5.3 Another problem facing those responsible for setting the standards for Commonwealth recordkeeping is that, to date, the preservation of electronic records has not been treated with the same importance as the preservation of paper records. In a survey commissioned by the NAA, the results showed clearly that the bulk of electronic information in Commonwealth agencies was '… being created, managed and possibly disposed of without the benefit of the knowledge and expertise of trained records management staff.'[3]

5.4 The NAA Green Paper described the new challenges presented by the proliferation of electronic information by saying that electronic systems offer many advantages but agencies must ensure that these records are captured, survive as long as they are needed, and can be read and understood. The main example is e-mail messages, which must be captured into corporate recordkeeping systems where they can be preserved securely and found easily.[4]

5.5 In addition, the data must be stored in such a way that it can '… be migrated forward with hardware and software changes so that the records are still accessible.'

> Such records provide evidence that the transaction occurred and essential details about it. Nonexistent or poor quality records will prevent online business being conducted successfully ...[5]

5.6 A significant amount of the Government's electronic information needs to be preserved for very lengthy periods. FaCS stressed the importance of this factor and the need for a concerted approach to the problem.

5.7 FaCS considered that the Commonwealth needed to pay greater attention to the long term preservation of, and access to, its data holdings. It said '… there is no whole of government strategy or resources for identifying data sources across agencies that need to be preserved over long periods of time.' And then it added: 'There is also a need to ensure that such data remain accessible over changes of technology including software.'[6]

---

2 Heslop et al., *Preservation of Digital Records*, p. 5.

3 NAA, *Submission No. 22*, p. 2.

4 Heslop et al., *Preservation of Digital Records*, pp. 5-6.

5 Heslop et al., *Preservation of Digital Records*, pp. 5-6.

6 FaCS, *Submission No. 21*, p. 7.

Archival Integrity

5.8 In addition to the problem of insufficient importance being given to electronic records, there are two additional factors that make the long term preservation of electronic records difficult: media degradation and application obsolescence.

Media Degradation

5.9 The various types of information storage media all degrade over time. Magnetic and optical media, such as floppy disks, tape cartridges, CD ROMs and DVD ROMs, have an archival life of about 20 years.[7] After this time, the information becomes less and less readable and may be lost entirely. The NAA Green Paper commented that these storage media '… decay relatively rapidly compared to other media. They are not designed for long term use and are therefore extremely susceptible to short and medium term decay.'[8]

5.10 Alternatively, data may become unreadable through technological obsolescence, when the hardware no longer exists to read the media used for storage. As an example, data stored on 5¼ inch floppy disks is becoming less and less accessible, because few modern computers are equipped with 5¼ inch disk drives.

5.11 NAA noted that the pace of market driven innovation means that '… without the intervention by archivists to preserve the source and process, the performance cannot be guaranteed.' It also commented, however, that:

> The problems of decay and obsolescence do not make the job of preserving digital material impossible. … As long as the essential parts of the performance can be replicated over time, the source and process can be replaced.[9]

5.12 One solution to media degradation is to store all archival data in live storage. This involves copying the data to a modern storage device, such as a hard drive or storage silo. If the chosen device is regularly maintained to prevent degradation, the data stored on it will remain accessible as long as the device remains in working order. This method requires that, periodically, when the storage device is upgraded, all data must be transferred to the new storage device.

---

7 AUUG Inc., *Submission No. 13*, pp. 7-8.

8 Heslop et al., *Preservation of Digital Records*, p. 11.

9 Heslop et al., *Preservation of Digital Records*, p. 11.

Application Obsolescence

5.13 The pace of computer software development is such that each version of a program, such as a word processor or a spreadsheet, is rapidly replaced by a new version.[10] For users, the problem in this process is that most vendors only support the superseded format for a limited time. This can occur through the policy decisions of software companies or through the failure of the company itself.

5.14 The result of this process of obsolescence is that users need to establish a comprehensive forward plan to prevent the inadvertent loss of valuable data.

5.15 One technique would be to use a long-term storage format; a solution already under consideration by a number of Commonwealth agencies. The format adopted would be selected both for its suitability and the expectation that applications capable of reading its files would still be available in 50 to 100 years. All information to be archived would then be converted into the chosen format as part of the standard archiving procedure.

5.16 An advantage of long-term storage formats is that because their rules are known and freely available, anyone can write an application that can read the files. If no such application existed, then a new one could be written from the specifications.

5.17 The National Archives has chosen XML (eXtensible Markup Language) as its long-term storage format. This format is open and non-proprietary, so many applications exist that can read it, and new applications can be written at any time.[11]

5.18 The Victorian Electronic Records Strategy (VERS) has chosen Adobe's Printable Document Format (PDF) as its long-term storage format.[12] This program was created by a private company but it is an open format, with its standards freely available and widely known. Hence, it has the same sort of advantages as XML. The differences between PDF and XML are easily dealt with because each format can be converted to the other without loss of information.

5.19 All agencies should consult NAA, to ensure that that their plans are compatible with the national archival plans for Commonwealth data. Of

10 Heslop et al., *Preservation of Digital Records*, p. 11.

11 Mr Stuckey, *Transcript*, 1 April 2003, p. 98.

12 Victorian Electronic Records Strategy, *Final Report*, Chapter 3, p. 16, http://www.prov.vic.gov.au/vers/published/final/final3.pdf, 28 October 2003.

necessity, this would include arrangements for the long-term storage of data in a format that:

- will continue to be accessible for the foreseeable future; and
- uses an information storage medium that will:
  - (i) also remain accessible for a long period, and
  - (ii) allow a simple transfer procedure when a new medium becomes necessary.

5.20 The Committee notes the NAA use of open source and notes the reason for using it; namely the expense associated with maintaining a long term licence if the NAA was reliant on proprietary software and accessibility.[13]

Recommendation 7

5.21 **The Australian Government Information Management Office (AGIMO), with support from the National Archives of Australia (NAA), ensure that Commonwealth agencies implement knowledge management and archival policies such as e-permanance which give equal priority to preserving electronic and paper-based records. AGIMO to advise the Committee, in an Executive Minute, of the status of these arrangements. The NAA to be resourced properly.**

Business Continuity and Disaster Recovery

5.22 In addition to preparing defences against attacks on electronic data systems and degradation of records over time, it is also important for each Commonwealth agency to have a program in place to quickly re-establish normal operations after events such as fires or earthquakes.

5.23 In an audit report released in July 2003, the ANAO gave attention to the current state of preparedness in Commonwealth agencies. Its findings indicated that although most agencies were aware of the necessity for such preparations, the actual arrangements are, in most cases, far from complete. The report commented:

> Many of the entities reviewed either have no business continuity plan, or are in the process of developing one … However their ability to recover from a disaster may be limited.[14]

13 Mr Stuckey, *Transcript*, 1 April 2003, p. 98.

5.24 The ANAO report made the assessment that '… only about 30 per cent of the entities reviewed had a business continuity plan, a disaster recovery plan or use high availability equipment to deal with the threat'. In other cases, where plans do exist, ANAO found that:

> … there is insufficient scope or detail in the plans to be able to conclude confidently that they could recover from a disaster. In addition, some … have not tested these plans to ensure that they can recover from a disaster.[15]

5.25 ANAO itself reported that its '… Disaster Recovery Plan was reviewed in February 2002 and incorporated in an updated Business Continuity Plan…' The plans were tested by external consultants at the end of that year and recommendations from that review accepted and put in place. A further check by ANAO's internal auditor, confirmed that the plans were an appropriate way to minimise threats to the data it held.[16]

5.26 At the ANAO, data on the servers is backed up daily and the tapes stored off site. In the event of a disaster, the contractor is required to provide backup facilities at its premises for the restoration of ANAO's operations. This plan restricts the potential loss of data to a maximum of one day.[17]

5.27 Similarly, NOIE advised that its data is backed up and a copy stored offsite by TES.[18] The issue of the security of information stored offsite was addressed in Chapter 2.

5.28 As an example of how Commonwealth departments addressed this issue in response to this inquiry, FaCS told the Committee that it had developed a Business Continuity Framework to manage and recover from major disruptions. The Framework includes a command structure, recovery teams, high level strategies and detailed plans and procedures to cover key risk areas.[19]

5.29 The IT area of FaCS has a disaster recovery plan as part of a Business Continuity Management Project. This plan has been subjected to disaster scenario testing, to identify weaknesses in the system. A number of

---

14 ANAO, *Control Structures as part of the Audit of Financial Statements of Major Commonwealth Entities for the Year Ending 30 June 2003,* Audit Report No. 61 2002-03, 30 June 2003, p. 71.

15 ANAO, *Control Structures as part of the Audit of Financial Statements of Major Commonwealth Entities for the Year Ending 30 June 2003,* Audit Report No. 61 2002-03, 30 June 2003, p. 71.

16 ANAO, *Submission No. 42,* p. 7.

17 ANAO, *Submission No. 42,* p. 7.

18 NOIE, *Submission No. 60,* p. 4.

19 FaCS, *Submission No. 21,* p. 6.

recommendations for improvement arising from these tests will be addressed by the department.[20]

5.30 The evidence before the Committee indicates that, although some agencies have put adequate preparations in place, taken as a whole, Commonwealth agencies are not well prepared to cope with large scale interruptions to, or losses of, their IT capacity.

5.31 The Committee believes that all Commonwealth agencies should assign a high priority to the completion of comprehensive plans for business continuity and disaster recovery. DSD has offered its assistance in preparing such plans and agencies should take advantage of that assistance.

Recommendation 8

5.32 **The Australian Government Information Management Office (AGIMO), in consultation with the Australian National Audit Office, ensure that Commonwealth agencies have in place comprehensive and tested business continuity and disaster recovery plans for their electronic records networks and services. AGIMO to advise the Committee, in an Executive Minute, of progress with the implementation and testing of these plans.**

20 FaCS, *Submission No. 21*, p. 6.

6

Information Security

Introduction

6.1 In recent years Commonwealth agencies have rapidly expanded their use of the Internet as a contact point for their clients. In doing so, the agencies have changed the nature of the challenges to maintain the confidentiality and integrity of information in messages and data bases.

6.2 Despite the changing nature of the risks, however, there are numerous advantages to be gained by the use of electronic transactions: increased speed, increased customer participation and satisfaction, improved data keeping and analysis, increased productivity, improved product quality and better, more up-to-date, information for the public.[1]

6.3 In addition, NOIE considers that the risks can be minimised by a well designed and maintained security regime. Electronic records lend themselves more easily to robust security measures than do paper records. For the storage and transmission of very sensitive data, there are obvious benefits to be gained from an effective security protection regime, even though the initial cost may be considerably heavier than for less secure systems.[2]

6.4 Consideration of the increased risks and the increased ability of 'crackers' to break into seemingly secure computer systems has contributed to the decision by the Commonwealth to adopt a form of encryption known as Public Key Cryptography (PKC).

---

1 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, pp 18-19.

2 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 19.

Public Key Cryptography[3]

6.5 The traditional form of message encryption, known as symmetrical encryption, uses a single secret key to both encrypt and decrypt messages. The weak point is the need for both parties to have the same key. If the key is intercepted and copied while being transmitted from one to the other, the whole system is compromised. Another problem is that a separate key will be needed for each different recipient. If the same key is used, all recipients will be able to read every message, not just the ones directed to them.[4]

6.6 In the PKC system, an asymmetric encryption technique is used. That is, the system uses two different but complementary (mathematically related) keys. One of these is known only to the holder – the private key. The other is a public key that can be known to anyone. A message encrypted with the public key can only be decrypted with the corresponding private key and vice versa. This means that anyone can use the public key to send a message and only the holder of the private key can decrypt it.[5]

6.7 PKC provides the following attributes for the communication of electronic information:

- **integrity**: the contents of the message received must be the same as that which was sent;
- **authentication**: the message can only have been sent by the purported sender; and
- **non-repudiation**: the sender cannot credibly deny that they sent it.[6]

6.8 To authenticate the identity of the sender or to ensure that a message has not been modified, the message can be sent with a digital signature appended. A digital signature is a special piece of data related to both the message being sent and to the sender's private key.

---

3 Public Key Cryptography is explained in more detail in Appendix F.

4 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 7; Mr Clarke, *Message Transmission Security (or 'Cryptography in Plain Text')*, 11 May 1998, http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html , 28 October 2003, p. 3; and Computer Associates, *Submission No. 52*, p. 2.

5 Mr Clarke, *Message Transmission Security*, pp. 3, 10; NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 8; Mr Engelman, *Transcript*, 2 April 2003, p. 153; Computer Associates, *Submission No. 52*, p. 2.

6 Mr Clarke, *Message Transmission Security*, p. 2.

Digital Certificates

6.9 Even when used correctly, PKC does not absolutely establish the identity of the sender – only that the sender had access to a particular private key. This problem can be resolved by using a trusted third party to verify the association between a public key and the identity of the owner of the associated private key.

6.10 Once that association has been verified and published in a digital certificate, other parties can trust that the person identified in the certificate holds the private key which matches the public key also referred to in that certificate. To achieve this, a significant number of infrastructure elements must be in place and functioning securely and effectively.[7]

Public Key Infrastructure

6.11 To implement the large-scale use of PKC requires the establishment of a Public Key Infrastructure (PKI), that is:

> … a set of procedures and technology that … enables users of a basically unsecured public network such as the Internet, to securely exchange information through the use of public and private cryptographic key pairs that are obtained and shared through a trusted evaluated infrastructure.[8]

6.12 Through the PKI, digital certificates are issued to properly identified applicants. The certificates are digitally signed, structured messages and achieve the aim of binding a public key to a verified identity. In doing so, they permit the accurate identification of an organisation or an individual.

6.13 The system consists of several components:

- Certification Authorities (CAs): trusted authorities which create and issue digital certificates. They may also create users' private keys (although, in practice, this is rarely done).
- Registration Authorities (RAs): check identities when new certificates are requested and process requests for renewal or revocation of existing certificates. In rare cases they also perform the CA functions of generating keys and certificates.

7 NOIE, *Online Authentication : A Guide for Government Managers*, July 2002, pp. 8-9.

8 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 8.

- Certificate or Key Holders: the end-user. They are issued with keys and certificates which enable them to digitally sign and encrypt electronic documents.
- Relying Parties: who receive, validate and accept digital signatures from key holders / subscribers.
- Repositories: which store and make available certificates and Certificate Revocation Lists (which are maintained by CAs).[9]

Gatekeeper

6.14 The Commonwealth PKI system is known as the Gatekeeper project. NOIE commented that Gatekeeper is not a product, as many people think, but a framework of standards used to measure the capability of applicants seeking accreditation as service providers.[10]

6.15 In late 1997 a number of agencies were investigating ways to enhance their service delivery by conducting business electronically. PKC was emerging as an accepted means of authenticating users, to ensure the security of electronic transactions. The Government decided to develop a national framework for the authentication of users of electronic online services. The then Office of Government Information Technology (OGIT) was charged with developing a strategy for the Commonwealth Government's use of PKC. OGIT formally established Project Gatekeeper in October 1997, and it was launched in May 1998.[11]

6.16 Application of the Gatekeeper standards is not compulsory for most Commonwealth agencies – each agency must make its own assessment of its need for security. However, if an agency decides that PKI is necessary, application of the Gatekeeper standards becomes compulsory for external use.[12]

6.17 On the other hand, firms or agencies wishing to become service providers must go through a long and comprehensive process to prove that they can meet all of the requirements of the Gatekeeper standards.[13]

---

9 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 29.

10 Ms Elsley, *Transcript*, 19 June 2003, p. 290; Mr Besgrove, *Transcript*, 19 June 2003, p. 293.

11 Gatekeeper Strategy, http://www.noie.gov.au/projects/confidence/Securing/Gatekeeperstrategy.htm, 28 October 2003.

12 NOIE, *Online Authentication:: A Guide for Government Managers*, July 2002, p. 4; Mr Besgrove, Mr Grant, *Transcript*, 19 June 2003, pp. 297.

13 Ms Elsley, *Transcript*, 19 June 2003, pp. 292-3.

Gatekeeper Accreditation

6.18 Firms or agencies seeking accreditation as Gatekeeper service providers – CAs or RAs – must meet stringent requirements which encompass all security enforcing aspects of their business and its operations. Accreditation is applied to the organisation, not their products. To use NOIE's words:

> The purpose of Gatekeeper accreditation is to provide an objective standard against which the competence of an organisation to deliver certification services can be assessed.[14]

6.19 Physical security of the premises is checked thoroughly by the Australian Security Intelligence Organisation (ASIO); the extent of these checks depending on what role is being requested under Gatekeeper. Different standards apply for CAs and RAs but in each case they would need to be assessed as Highly Protected by ASIO for their application to proceed.[15]

6.20 DSD carries out a detailed evaluation of the security of the applicant's IT system. This process includes an evaluation of the software involved.[16]

6.21 Operational evaluation of the applicant is handled by NOIE, which examines the applicant's operations manuals, their disaster recovery and business continuity plans and carries out a legal evaluation. The latter is necessary to establish the required level of trust for clients of the applicant.[17]

6.22 A Certification Practice Statement is developed by each CA/RA covering its operations, the infrastructure and the certificates to be issued. For each different type of certificate to be issued, a separate Certificate Policy is also developed.[18]

6.23 Security vetting of applicants is rigorous. The staff of each applicant must be vetted to the Highly Protected level. This is carried out by the Australian Security Vetting Service and the Australian Protective Service. Under the Gatekeeper arrangements, all service providers must also be on the endorsed supplier list administered by DoFA.[19]

6.24 When all of the requirements have been met to the satisfaction of the Chief Executive Officer of NOIE, a contract is signed on behalf of the

---

14 NOIE, *Submission No. 57,* p. 20.

15 NOIE, *Submission No. 57,* p. 22.

16 Ms Elsley, *Transcript,* 19 June 2003, p. 292; NOIE, S*ubmission No. 57,* p. 23.

17 Ms Elsley, *Transcript,* 19 June 2003, p. 292.

18 NOIE, *Submission No. 57,* p. 25.

19 NOIE, *Submission No. 57,* p. 24; Ms Elsley, *Transcript,* 19 June 2003, p. 292.

Commonwealth. The contract sets out in detail the obligations the service provider must fulfil. Every 12 months thereafter they must undergo a compliance audit to ensure that the Gatekeeper criteria are still being satisfied. The audits are carried out by one of a panel of auditors established and approved by NOIE.[20]

6.25 At the time of the inquiry, NOIE advised that eight organisations had achieved full Gatekeeper accreditation:

- Secure Net Limited as CA;
- Pricewaterhouse Coopers (beTRUSTed) as CA and RA;
- Australia Post as RA;
- Telstra Corporation Limited as CA and RA;
- eSign Australia Limited as CA and RA;
- Health eSignature Authority Pty Ltd as RA;
- Baltimore Certificates Australia Pty Ltd; as CA; and
- the ATO as CA and RA.[21]

6.26 In addition, the ANZ Bank was then undergoing the evaluation process for Gatekeeper accreditation.[22]

Commonwealth Agencies Using Gatekeeper

6.27 Government agencies participate voluntarily in Gatekeeper.[23] To date, very few agencies have chosen to participate. NOIE attributes this, in part, to the slow acceptance of PKC and the slow growth of the PKI market.[24]

6.28 The ATO was the first agency to attain full gatekeeper accreditation for their CA in May 2000. The HIC uses the authentication services of Health eSignature Authority Pty Ltd, which is a Gatekeeper certified RA.[25]

6.29 Some Government agencies have little or no need for certification. The type of business conducted by the ABS does not warrant the Bureau

20 Ms Elsley, *Transcript*, 19 June 2003, pp. 292-3.

21 NOIE, *Submission No. 57*, p. 5.

22 NOIE, *Submission No. 57*, p. 5.

23 Gatekeeper Strategy, http://www.noie.gov.au/projects/confidence/Securing/Gatekeeperstrategy.htm, 28 October 2003.

24 Mr Besgrove, Mr Dale, *Transcript*, 1 April 2003, p. 73.

25 Mr Farr, *Transcript*, 31 March 2003, p. 38; Gatekeeper Accreditation, http://www.noie.gov.au/projects/confidence/Securing/GatekeeperAccreditation.htm, 28 October 2003.

seeking certification. As it commented: 'People tend not to fraudulently lodge statistical returns on behalf of other people'.[26] Similarly, the Attorney-General's Department said that it has not yet found a business use for Gatekeeper.[27]

6.30 Other Government agencies have found that their authentication needs are met by less formal PKC, such as the Secure Socket Layer (SSL) protocol. DEWR said that it currently finds SSL to be sufficient:

> We believe that secure socket layer security is more than adequate for our interacting with the Job Network. … Certainly it is working well at the moment.[28]

Limitations of Gatekeeper

6.31 The Committee heard evidence on the limitations of Gatekeeper, in terms of cost and security.

Cost

6.32 A frequent comment by Government agencies and private companies was that Gatekeeper is too complex and / or expensive.[29] NOIE at first estimated that achieving Gatekeeper accreditation would cost around $300,000, but later commented that depending on circumstances and requirements, the cost has varied, in practice, between $200,000 and $2.2 million.[30] The use of Gatekeeper is not likely to expand until certification costs come down.

6.33 Some Government agencies are using authentication services that are not Gatekeeper accredited. A number of private companies offer their own authentication services in competition with Gatekeeper. These include Computer Associates and Check Point Software Technologies (Australia) Pty Ltd. Agencies outsourced to these companies use their services rather than the services of a Gatekeeper accredited provider.[31]

---

26 Mr Palmer, *Transcript*, 31 March 2003, p. 34.

27 Mr LeRoy, *Transcript*, 1 April 2003, p. 134.

28 Mr Burston, *Transcript*, 31 March 2003, pp. 63-64.

29 Ms Treadwell (Centerlink), *Transcript*, 31 March 2003, p. 30; Mr Besgrove (NOIE), *Transcript*, 1 April 2003, p. 73; Mr Wilson (Computer Associates), *Transcript*, 2 April 2003, p. 148; Ms Reich (SingTel Optus), *Transcript*, 2 April 2003, p. 194.

30 Mr Grant, *Transcript*, 1 April 2003, p. 80.

31 Mr Engelman, *Transcript*, 2 April 2003, p. 147; Mr Ferguson, *Transcript*, 2 April 2003, p. 185.

Security

6.34 PKIs such as Gatekeeper are '… not a foolproof solution to identity management'.[32] If a person's private keys are compromised, unauthorised people could impersonate them or read their messages. Thus private key security is of paramount importance to users of PKC. This has been highlighted as a crucial weakness of the PKC system as currently used, because few key holders can guarantee the absolute security of their keys. Private keys may be the target of crackers, viruses or worms. Hardware and software systems currently provide very little in the way of security features. [33]

6.35 The CA is expected to assure that the user of a certificate is who they claim to be. If such an assurance is incorrect and a party's reasonable dependence on that assurance resulted in economic cost, then the CA may be considered liable. In practice, few CAs are willing to take on this responsibility. Their policy statements are usually phrased to limit their exposure to liabilities. In these circumstances, CAs cannot reasonably expect their offers of assurance to be taken seriously, if they are not willing to stand by that assurance.[34]

6.36 Another key point in the security of any PKI system is the fast and effective revocation of compromised keys. However, the Committee was told that Gatekeeper does not make adequate arrangements for managing the revocation of compromised keys. This is seen by some as a critical weakness.[35]

Recommendation 9

6.37 **The Department of the Prime Minister and Cabinet should review and report to the Committee on the cost effectiveness of Gatekeeper versus other commercially available public key infrastructure products and systems.**

32 Computer Associates, *Submission No. 52*, p. 3.

33 Mr Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure*, 3 May 2001, http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html , 28 October 2003, p. 7.

34 Mr Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure*, pp. 8-9.

35 Mr Clarke, *Submission No. 51*, p. 4; AUUG, *Submission No. 58*, pp. 3-4.

6.38 Finally, users may be required to submit to intrusive authentication processes, which could, even then, still be circumvented by a determined impostor.[36]

Alternative Systems

6.39 There are several companies which claim that they could provide a system which would at least match the security and performance of Gatekeeper. Some systems, it is claimed, could also be supplied at lower cost.

6.40 In the end, the decision on the system to be used lies with the Chief Executive of each agency, provided that the chosen system meets the security standards suitable to its purpose. The Committee, however, considers that all agencies should weigh other options against Gatekeeper, when reviewing their security needs and to carefully assess the costs and benefits of each system before reaching a decision.

PKI Framework for the Authentication of Individuals

6.41 An extension of the use of PKIs, such as Gatekeeper, is that they can be used to authenticate the identity of members of the public, in cases when they deal with government agencies either in person or electronically. As such, PKI frameworks have the potential to make a range of transactions between agencies and members of the public easier and more secure.

6.42 Authentication processes established under a PKI would allow individuals to reliably present an identity to Commonwealth agencies. An individual user would register their identity with a RA and receive a certificate from a CA. The individual could then use this certificate with all Commonwealth agencies, since they will be able to verify the identity of the client with the CA.

Once Only Proof of Identify

6.43 Currently, however, there is no whole-of-government approach to the authentication of an individual.[37] An individual conducting business with several Commonwealth agencies must go through the process of

36 Mr Clarke, *Submission No. 51,* p. 4.

37 Management Advisory Committee, Report 2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework,* 2002, p. 35.

registering their identity with each one. If, for example, that client's address changes, each of the agencies that they deal with must be separately informed.

6.44 Time and effort could be saved if each individual only had to register their identity once and report any changes once. The Privacy Commissioner recognised that the collection of private information into centralised datasets would require high levels of transparency, explanation and consultation with the public if such a strategy was to stand a chance of being accepted by the public.[38]

Preventing Multiple Identities

6.45 Authentication is a useful tool for the prevention of identity abuse. In the past, there have been cases of Centrelink clients fraudulently claiming multiple benefits using multiple identities.[39] If a rigorous authentication process is put in place, it should be able to detect when a person applies to register a second identity. Biometrics may soon make this a practical possibility. The information available to the RA should then prevent anyone from fraudulently registering a second identity.

Preventing Identify Theft

6.46 Authentication can also help to prevent identity theft. This occurs when an impostor acquires enough information to impersonate another person. For example, an individual's certificate may be stolen and then used to impersonate them in dealings with Government agencies. Using PKI, the certificate issued to an individual could include identifying information, allowing Government agencies to check that the holder of the certificate is the person to whom the certificate was issued. PKI allows any certificate to be quickly revoked if it is compromised.

Authenticating Individuals

6.47 The problem remains of how an individual, as distinct from an agency or organisation, can be reliably authenticated. Current practices to establish identities call for an individual to provide a number of identifying documents ('100 points'). The problem is that some identifying documents

38 Mr Crompton, *Transcript*, 2 April 2003, p. 212.

39 Computer Associates, *Submission No. 38*, p. 5; Mr Engleman, *Transcript*, 2 April 2003, p. 144.

can be obtained without rigorous proof of identity and these could then be used to obtain the other necessary identifying documents.[40]

6.48 Furthermore, PKI assumes that the owners of private keys will be able to ensure their security. A PKI being used by an individual to transact business with agencies via their home computer will only work successfully if the private key is kept secure. Private keys stored on software will only be as secure as the computer systems which store them and there are ongoing concerns about the security of home computers.[41] Similar practical problems will arise when private keys are compromised and attempts are made to revoke certifications and warn other users not to accept bogus certificates.

6.49 The MAC of the Australian Public Service Commission has recently considered the issue of authenticating individuals. Its recommendations aim to achieve a consistent approach across Government departments. This may involve establishing primary identity documents for registering with Government agencies, supported by the establishment of a national online identity document validation framework.[42]

6.50 Gatekeeper appears to be an expensive, technically successful PKI for ensuring the privacy, integrity and security of electronic information transmitted by Commonwealth agencies, despite its low take-up by agencies generally. The take-up is likely to improve if its cost to users is reduced and as the use of the internet as a communication medium between agencies, and between agencies and their clients, expands.

6.51 Challenges will remain in reliably authenticating members of the public who use Commonwealth services.

---

40 Mr Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy*, December 1994, http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html, 28 October 2003, pp. 14-17.

41 Mr Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure,* p. 7.

42 MAC, Report No. 2, p. 35.

7

Evaluation of Products under AISEP

Introduction

7.1 The Commonwealth requires the use of products with a high security assurance for the delivery of on-line services and the protection of official information.[1]

7.2 AISEP, the Australasian Information Security Evaluation Program, is the process conducted by the DSD Certification Group to evaluate software products and certify as to their suitability for the security tasks they are claimed to fulfil.[2]

7.3 The program operates on a commercial basis and offers IT security vendors the opportunity to benchmark their products against accepted international standards. Endorsement at the end of the evaluation process provides users, both government and non-government, with an independently assessed level of assurance that the product will meet their individual security needs. [3]

7.4 The Director, DSD has overall responsibility for AISEP, as part of DSD's role as the Commonwealth National Computer Security Advisory Authority. The Director delegates his operational management authority

---

1 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 1.

2 DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 2.

3 DSD *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 1.

for AISEP to the Australasian Certification Authority (ACA), that is, the Assistant Secretary, Information Security in DSD.[4]

7.5 AISEP operates under the guidance and advice of a Management Policy Board, chaired by the ACA. The Board provides guidance and advice to the ACA (and indirectly to the Director, DSD) on policy and objectives for the operation of AISEP. It has a broad membership, so as to take account of the requirements of customers, industry and other relevant parties. Its aim is the advancement of evaluation services in both government and industry, while taking account of essential security and commercial interests.[5]

Evaluation Criteria

7.6 When AISEP began in 1994, the evaluation benchmark applied was the Information Technology Security Evaluation Criteria (ITSEC), a standard already used by several countries in Europe. In 1998, an international standard accepted by the International Standards Organisation was incorporated into the system. This standard is based on what are known as the Common Criteria (CC).[6]

7.7 Most of the products currently on the Evaluated Products List were evaluated using ITSEC, which has seven evaluation levels – E0 the lowest, to E6 the highest. New additions are evaluated using the CC. While the CC also has seven levels of assurance, only four levels currently have an established methodology.[7] For the higher levels ITSEC is still used.

7.8 Adoption of an internationally accepted standard has permitted the formation of a Common Criteria Recognition Agreement (CCRA), which Australia and New Zealand joined in 1999. This agreement currently involves 14 countries which accept Certificates from other members of the group, without further assessment. There are two types of participants: seven Certificate Producers[8], who have their own certification / evaluation

4 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 6.

5 DSD, *Exhibit No. 22 Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 6.

6 DSD *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 1.

7 DSD, *Exhibit No. 22 Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 9.

8 Australia, New Zealand, Canada, France, the UK and the USA.

schemes and seven Certificate Consumers[9], who rely on the certificates produced by the Certificate Producer group. The agreement only applies to the first four CC levels. In addition, Australia, New Zealand and the United Kingdom have agreed to recognise their respective ITSEC certificates up to level 6.[10]

Evaluation and Certification Process

7.9 The process of evaluation and certification has three stages[11]:

- *Acceptance*: in which the Target of Evaluation is defined (that is the product or system to be evaluated) and the Security Target is developed (that is the formal statement of the claims made for that product or system). This stage may be undertaken by a licensed evaluation facility – but not by individuals who will be involved in the evaluation process itself.[12] The initial stage ends with DSD assessing the suitability of the Target of Evaluation and the Security Target, plus a preliminary review of any cryptography functions.
- *Evaluation*: The second stage in the process is the evaluation, carried out by a licensed third party known as an Australasian Information Security Evaluation Facility (AISEF).[13] The Certification Group in DSD monitors the work of the AISEF and arranges for the DSD Cryptographic Evaluation section to evaluate any cryptographic security features. When the evaluation is completed, the AISEF issues an Evaluation Technical Report.
- *Certification*: On successful completion of the evaluation, the Certification Group produces a Certification Report; the product is then listed on the Evaluated Products List (EPL) as Evaluated and a Certificate is issued by the ACA.

---

9 Finland, Greece, Italy, Israel, the Netherlands, Norway and Spain.

10 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, pp. 4, 23.

11 This section summarised from DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 1; DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, pp. 9-11.

12 It is a provision of the AISEF licensing agreement that: 'The AISEF shall not:
(b) allow a person who has been involved in the development of the Target of Evaluation to be involved in a Security Evaluation of that Target of Evaluation…' DSD, *Submission 66*, p. 3.

13 To be licensed as an AISEF a facility must be accredited by the Defence Security Branch and the National Association of Testing Authorities, Australia. DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, pp. 7-8.

7.10 Products successfully meeting the evaluation criteria are added to the EPL, which is available on the DSD website.[14] This is the definitive list for products evaluated for use in Australian Government systems. It also provides details on products evaluated and certified by other members of the CCRA and which can therefore be accepted for use in Australian Government systems without further evaluation.[15]

7.11 When an evaluation is carried out on a purely commercial basis, DSD charges the company a Certification Fee. That fee is determined from a scale of fees, which increase in line with the level of security assurance required. If the applicant has the written support of a Commonwealth sponsor, however, DSD waives its fee and therefore absorbs the cost.[16]

7.12 The bulk of the fees involved in the evaluation process are paid to the AISEF. The fees charged for pre-evaluation services and evaluations are established on a purely commercial basis between the applicant and its chosen AISEF.[17]

Benefits of AISEP

7.13 The AISEP provides a number of benefits to sponsors, developers and users. Certification under the system:

- gives users a level of assurance that the product will meet a determined level of security needs and comply with internationally recognised criteria;
- allows the product to be used within the Australian and New Zealand governments;
- allows Mutual Recognition by other members of the CCRA;
- gives an opportunity to developers to improve security features in line with customer requests;
- reduces or eliminates the need for further internal security testing;

---

14 DSD Evaluated Product List, http://www.aisep.gov.au/library/epl/epl.html, 28 October 2003.

15 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 5.

16 DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 3.

17 DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 3.

- enables users to obtain evaluated products from international vendors;
- helps to avoid mistakes which can leave data vulnerable to attack; and
- allows users to cost effectively match products to specified security needs, with an appropriately assured level of performance.[18]

Conflict of Interest

7.14 The commercial advantages to be gained through the certification of a product or process under the AISEP raise the possibility of a conflict of interest arising within an AISEF. Consequently, it is a provision of the AISEF licensing agreement that:

> The AISEF or any employee of the AISEF involved in a Security Evaluation shall not have any commercial, financial, personal or other interest in the outcome of the Security Evaluation.[19]

7.15 Optus expressed some concern that the three companies currently accredited to perform evaluations are also Optus' business competitors:

> We have a situation where we are directly competing against one of them for business and they have all our intellectual property…[20]

7.16 DSD reported that none of the currently licensed evaluation facilities has formally raised a conflict of interest issue. DSD considers that this is mainly due to '… stringent conflict of interest provisions which are contained in the licence agreements under which each of the facilities is required to operate.'[21]

7.17 In addition, each AISEF must operate '… as a separate entity from its parent company, if any, and any other party.'[22]

7.18 DSD gave its opinion that these compulsory contract provisions and the associated power, in the event of a breach, to withdraw an AISEF's status and suspend or terminate the licensing agreement, provides sufficient protection to discourage problems in this area:

---

18 DSD, *Exhibit No. 20, Australasian Information Security Evaluation Program*, Explanatory Booklet, pp. 3-4.

19 DSD, *Submission No. 66*, p. 3.

20 Ms Reich, *Transcript*, 2 April 2003, p. 202.

21 DSD, *Submission No. 66*, p. 3.

22 DSD, *Submission No. 66*, p. 3.

> Our view is that these conditions provide an adequate degree of separation between the operations of the AISEF and those of the parent company, even in circumstances where the parent company may offer products or services which are potentially in competition with a product that is under evaluation in their facility.[23]

7.19 The Committee has not drawn a conclusion on this issue.

Cost and Duration of the Evaluation Process

7.20 In its submission, Optus claimed that '… getting a product listed on the EPL is expensive and time consuming.' In giving evidence, it added the comment that the process '… acts as a deterrent to list new products.'[24] It also suggested that: 'this system should be less complex, less expensive and faster to complete.'[25]

7.21 Optus indicated that one problem arose from the 'broad-brush' approach of the Protective Security Manual guidelines, used to classify information in the Commonwealth system. This resulted in the highest classification applicable to any information in the system, being applied to *all* the data in the system:

> What tends to happen is that a classification is given which relates to the most valuable information. That then requires a gold-plated solution. Agencies, we think, would get better results and more economic solutions if they imposed multiple security classifications.[26]

7.22 A further comment from Optus, involved the perceived inflexibility of requirements once information has been classified as protected:

> In some instances this had led to the implementation of expensive and unnecessary security solutions.[27]

7.23 Optus' particular complaint is that the security features of the Optus private secure internet have not been recognised – it is treated, Optus said, as being 'untrusted' and no different to the public Internet. Optus noted

---

23 DSD, *Submission No. 66*, p. 4.

24 Mr McCulloch, *Transcript*, 2 April 2003, p. 192.

25 Optus, *Submission No. 30*, p. 6.

26 Mr McCulloch, *Transcript*, 2 April 2003, p. 193.

27 Optus, *Submission No. 50*, p. 2.

that this means that 'an expensive solution – and an unnecessary one, we would submit – needs to be implemented.'[28]

7.24 Indicating the inconsistent security standards applying '… between Commonwealth agencies, between governments and between all levels of government and business', Optus proposed adoption of a graded standard for all organisations handling Commonwealth or personal information.[29]

7.25 As a starting point towards overcoming these shortcomings and inconsistencies, Optus proposed that the process for EPL listing should be streamlined to reduce both the cost and the time taken to complete the requirements. It called attention to a similar recommendation by a Working Group of the MAC. The Working Group proposed:

> Investigating ways and means of improving the process for the Evaluated Products List … which may include a more proactive approach to endorsement to lower the costs and length of time involved in getting products evaluated and on the EPL.[30]

7.26 Optus suggested that classification should take account of the:

- value of the information being protected
- efforts the attacker must undertake to compromise the information; and
- additional costs associated with encrypting 'over classified' information.[31]

7.27 DSD was asked for comments on the evaluation process and its costs. The response noted that the evaluation process is a recognised international standard and that it is rapidly becoming the benchmark for such product evaluations.[32]

7.28 One of the main advantages of the process DSD said, was its international recognition:

> A less extensive process of evaluation would be unlikely to achieve similar international recognition, and would most likely result in vendors having to put their products through a separate evaluation process for every country in which they wished to sell –

---

28 Optus, *Submission No. 50,* p. 2; Mr McCulloch, *Transcript,* 2 April 2003, p. 194.

29 Mr McCulloch, *Transcript*, 2 April 2003, p. 194.

30 Optus, *Submission No. 50,* pp. 1-2; MAC, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework,* Australian Public Service Commission, 2002, p. 31.

31 Optus, *Submission No. 30,* p. 7; Mr McCulloch, *Transcript,* 2 April 2003, p. 194.

32 DSD, *Submission No. 66,* p. 4.

> the very problem which the Common Criteria was established to address.[33]

7.29 Regarding the costs of the process, DSD explained that its charges are a relatively minor part of the total – and, in fact, are waived when there is a Commonwealth sponsor. Charges for the pre-evaluation and evaluation phases make up the bulk of the cost and are purely commercial charges.[34]

7.30 DSD noted that the total cost of an evaluation is closely linked to the duration of the process. The main factors influencing overall cost are:

- the complexity of the product;
- the scope of the security functionality claimed;
- the level of assurance sought;
- how committed to (and experienced with) the process the vendor is; and
- the extent of the problems identified during the evaluation.[35]

7.31 As an example, DSD said that for a simple product with a low assurance evaluation and no cryptographic functions, the task could be completed in a few months and cost in the tens of thousands of dollars. In contrast, a higher assurance evaluation of a more complex product (such as an operating system) can take years and cost millions of dollars.[36]

7.32 Microsoft Australia was asked for a comparison with the cost of the process in the US. It responded that '… we have not conducted any kind of comparative study or assessment of respective evaluation and EPL processes.' Microsoft added that:

> Because receiving common criteria recognition is such a costly and time and resource-intensive process, we have focused on achieving CC recognition through the US system and are then seeking Mutual Recognition agreements with the national signatories, including Australia.[37]

7.33 The variations inherent in the product types submitted for evaluation make it difficult to compare AISEP with its equivalents overseas. DSD said, however, that vendors in several countries which have their own evaluation schemes have made the commercial decision to have their products evaluated under AISEP, not their own scheme. DSD said that

---

33 DSD, *Submission No. 66*, p. 4.

34 DSD, *Submission No. 66*, p. 4.

35 DSD, *Submission No. 66*, p. 4.

36 DSD, *Submission No. 66*, p. 4.

37 Microsoft Australia, *Submission No. 64*, p. 6.

this indicates that AISEP's performance is regarded as comparable to theirs and cannot be much more expensive.[38]

7.34 Optus said that '… as soon as any changes occur to that hardware or software … you are either living with an older technology … or you are forcing the manufacturer to go through the same process again of spending in the order of half a million dollars to $1 million, plus six to 12 months going through the approval process.'[39]

7.35 The Committee noted, however, that the handbook produced by DSD to explain the AISEP process, indicates in a section on Certificate Maintenance, that upgrades or changes to the product covered by an evaluation will only invalidate the Certificate if the changes affect security aspects.[40] DSD expanded on this concept in its evidence to the Committee:

> … rather than having a product re-evaluated, depending on the scope of the changes, it is possible to go back and assess the security impact of them and issue a certificate extension, which essentially says that the same level of assurance can be maintained about the product.
>
> If the changes are outside that scope or if they specifically add new security functionality requirements, that would mean re-evaluation. But the important thing to remember is that re-evaluation does not mean starting from scratch. If the product is substantially the same, there is reuse of existing material and it might be a relatively painless process.[41]

7.36 The Committee notes that mutual recognition may be a pathway to accreditation for major players like Microsoft, but is a pathway probably not available to smaller companies.

7.37 The booklet encourages the isolation of changes to specific areas of the design or code, so that:

- the changes can be more easily assessed;
- their impact on the Security Target can be more easily assessed; and
- the re-evaluation and re-certification process can be reduced to a minimum.[42]

---

38 DSD, *Submission No. 66,* p. 4.

39 Mr Kidd, *Transcript,* 2 April 2003, p. 195.

40 *Exhibit 22,* p. 17.

41 Mr Scotton, *Transcript,* 16 June 2003, pp. 271-2.

42 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 17.

7.38 As mentioned above, the AISEP Certificate Extension program encourages Sponsors and Developers to adopt a systematic approach to maintaining security assurance for new versions of certified products and systems, without necessarily submitting them to another full evaluation.[43]

Committee Comment

7.39 Initially, the Committee was concerned about claims by witnesses that the expense and time involved in having products accepted for the EPL are acting as a deterrent.[44]

7.40 DSD and NOIE indicated that charges in Australia are not markedly higher than those charged in comparable systems overseas. There was also evidence to indicate that applicants can often substantially reduce the costs and the time required for evaluation and certification, by careful planning and use of the Certificate Maintenance procedures.

7.41 The Committee noted Optus' comments on the need for flexibility in the application of data security measures.[45] It agreed that there should be provision for sensitive or confidential data to be 'quarantined' by the application of a higher level of security. This would be more efficient and cost effective, the Committee said, than applying a high level security classification to a large body of data, most of which would be more appropriately classified at a lower level.

7.42 The Committee strongly supported the comments by Optus and the MAC regarding the need to review and streamline the procedures for certifying products and systems under AISEP. It is important to ensure that security standards are not relaxed; but more efficient processes and procedures should be able to reduce the costs and resources required to ensure that those standards are maintained.[46]

7.43 The Committee believes that assessment should be fair and equally applied to all applicants.

---

43 DSD, *Exhibit No. 22, Australasian Information Security Evaluation Program*, Explanatory Booklet, p. 17.

44 Mr McCulloch, *Transcript*, 2 April 2003, p. 192.

45 Mr McCulloch, *Transcript*, 2 April 2003, pp. 193-4.

46 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, 31.

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

A

Appendix A — Electronic Information under Review by ANAO

In the last few years, a number of ANAO Audit Reports have addressed, wholly or in part, the issues of the management and integrity of electronic information. These include:

- *Internet Security Management* (No. 15 1997-1998)
- *Protection of Confidential Client Data from Unauthorised Disclosure* (No. 37 1997-1998)
- *Data Management in the APS* (No. 48 1997-1998)
- *Managing Data Privacy in Centrelink* (No. 8 1999-2000)
- *Information and Technology in Centrelink* (No. 39 2000-2001)
- *Information Technology in the Department of Veterans' Affairs* (No. 44 2000-2001)
- *Internet Security within Commonwealth Government Agencies* (No. 13 2001-2002)
- *Recordkeeping* (No. 45 2001-2002)
- *Information Technology at the Department of Health and Ageing* (No. 1 2002-2003)
- *Fraud control Arrangements in the Department of Veterans' Affairs* (No. 6 2002-2003)
- *Capitalisation of Software* (No. 54 2002-2003)
- *Control Structures as part of the Audit of Financial Statements of Major Commonwealth Entities for the Year Ending 30 June 2003* (No. 61 2002-2003).

B

Appendix B — List of Submissions

1. Department of the Treasury
2. Department of the Parliamentary Reporting Staff
3. Department of Health & Ageing
4. Mr Robert Rose
5. Department of Employment and Workplace Relations
6. EDS Australia
7. Tenix Datagate Pty Ltd
8. Australian Information Industry Association Ltd
9. Check Point Software Technologies (Australia) Pty Ltd
10. Dept of Agriculture, Fisheries and Forestry
11. Department of Foreign Affairs and Trade
12. Microsoft Australia
13. AUUG Inc.
14. Australian Taxation Office
15. Standards Australia International Ltd
16. Australian Bureau of Statistics
17. Australian National Audit Office
18. Centrelink
19. Australian Federal Police

20. National Office for the Information Economy
21. Department of Family and Community Services
22. National Archives of Australia
23. Department of Immigration and Multicultural and Indigenous Affairs
24. Attorney-General's Department
25. Environment Australia
26. State Government of Victoria
27. Department of Industry, Tourism and Resources
28. Australian Customs Service
29. Commonwealth Ombudsman
30. SingTel Optus Pty Ltd
31. Department of Transport & Regional Services
32. Australian Crime Commission
33. Office of the Federal Privacy Commissioner
34. CommandHub
35. Department of Education, Science and Training
36. Department of Defence
37. Australian Electoral Commission
38. Computer Associates
39. Commonwealth Scientific and Industrial Research Organisation
40. Department of Health and Ageing
41. Australian Electoral Commission
42. Australian National Audit Office
43. Australian Taxation Office
44. Department of Defence
45. Department of Health and Ageing
46. Department of Employment and Workplace Relations
47. Attorney-General's Department
48. Australian Taxation Office
49. EDS Australia

50. SingTel Optus Pty Ltd
51. Xamax Consultancy Pty Ltd
52. Computer Associates
53. Standards Australian International Ltd
54. Department of Family and Community Services
55. Commonwealth Ombudsman
56. Australian Bureau of Statistics
57. National Office for the Information Economy
58. AUUG Inc.
59. EDS Australia
60. The National Office for the Information Economy
61. Centrelink
62. Commonwealth Scientific and Industrial Research Organisation
63. Symantec Australia
64. Microsoft Australia
65. Department of Finance and Administration
66. Department of Defence
67. Health Insurance Commission
68. SingTel Optus Pty Ltd
69. Health Insurance Commission
70. Imperium Technologies
71. Office of the Federal Privacy Commissioner
72. The Swe-Tech Group
73. Australian Security Intelligence Organisation
74. Department of Transport and Regional Services
75. Auditor-General's Department
76. Department of Communications, Information Technology and the Arts
77. Department of Employment and Workplace Relations
78. Department of Industry, Tourism and Resources

79. Department of Health and Ageing

80. Defence Housing Authority

81. Department of Prime Minister and Cabinet

82. The Treasury

83. Department of Education, Science and Training

84. Department of Agriculture, Fisheries and Forestry

85. Department of the Environment and Heritage

86. Department of Defence

87. Department of Family and Community Services

88. Department of Transport and Regional Services

89. Savita Technology Pty Ltd

90. Australian Customs Service

91. Department of Veteran's Affairs

92. Defence Housing Authority

93. Business Security Systems

94. Department of Transport and Regional Services

95. EDS Australia

96. Department of Immigration and Multicultural and Indigenous Affairs

97. Department of Finance and Administration

98. Department of Foreign Affairs and Trade

99. Saker Security Consulting

100. Australian Customs Service

101. Department of Defence

102. Department of Defence

In addition, the Committee accepted two confidential submissions.

C

Appendix C — List of Exhibits

1. Microsoft Australia, *Trustworthy Computing Environment*
2. Department of Education, Science and Training, *Information Management Improving Report & Information Management Framework Project*
3. Australian National Audit Office, *ANAO Audits in ANAO'S Submission to the JCPAA*
4. Australian National Audit Office, *Internet delivery decisions: a government program manager's guide*
5. Centrelink, A folder of additional information
6. Australian National Audit Office, *Summaries of ANAO Reports No.9 of 2000-01 and No.14 of 2002-03*
7. Attorney General's Department, *OECD guidelines for the security of information systems and networks: towards a culture of security*
8. National Archives of Australia, *Recordkeeping Implications of Online Authentication and Encryption Process*
9. National Archives of Australia, *Keeping Government Publications Online: A guide for Commonwealth Agencies*
10. National Archives of Australia, *Report on a Survey of the State of Recordkeeping in Commonwealth Government*
11. Department of Health and Ageing, *National Health Privacy Code (draft) Consultation Paper*
12. The National Office for the Information Economy, *Productivity and Organisational Transformation: Optimising Investment in ICT*

13. Computer Associates, *Best Practices for Command and Control of Security: The eTrust Vision*

14. Defence Signals Directorate, *Information Security Guideline Collection*

15. Defence Signals Directorate, *Information Security Incident, Ready Reckoner*

16. Defence Signals Directorate, *Information Security Incident Reporting for Government Agencies*

17. Microsoft, *Law and Corporate Affairs*

18. The National Office for the Information Economy, Folder of Information on Gatekeeper

19. The National Office for the Information Economy, Hansard Transcript of Gatekeeper Briefing

20. Defence Signals Directorate, *Australian Information Security Evaluation Program*

21. Defence Signals Directorate, *Common Criteria for information Technology Security Evaluation*

22. Defence Signals Directorate, *Australian Information Security Evaluation Program*

23. Savita Technology Pty Ltd, *Submission No 89 – Appendix 1-3*

In addition, the Committee accepted one confidential exhibit.

D

Appendix D — List of Witnesses Appearing at Public Hearings

Canberra, Monday 31 March 2003

Australian National Audit Office

Mr John Meert, Group Executive Director

Dr Paul Nicholl, Group Executive Director

Mr Michael McFarlane, Auditor

Ms Jan Tankiang, Auditor

Department of Family and Community Services

Mr Tony Mee, Assistant Secretary, Business Information Solutions Branch

Centrelink

Mr Patrick Fegan, National Manager, Business and Information Protection

Ms Jane Treadwell, Deputy Chief Executive Officer, Digital Business and Chief Information Officer

Australian Bureau of Statistics

Mr Jonathan James, First Assistant Statistician and Chief Information Officer, Technology Services Division

Ms Marion Kathleen McEwin, Assistant Statistician, Policy Secretariat Branch

Australian Taxation Office

Mr Gregory Dark, Assistant Commissioner

Mr Chander Vohra, Assistant Commissioner, Trusted Access

Mr Gregory Douglas Farr, Second Commissioner

Department of Health and Ageing

Dr Robert Edward Wooding, First Assistant Secretary, Information and Communications Division

Dr Ron McLaren, Assistant Secretary, Information Management and Technology Strategy Branch, Business Group

Ms Eija Seittenranta, Assistant Secretary, Technology Services Branch, Business Group

Mr Gary Leslie Sutton, Director, Information Strategies Section, Information and Communications Division

Department of Employment and Workplace Relations

Mr John Burston, Chief Information Officer

Mr Jeremy O'Sullivan, Assistant Secretary, Legal and Risk Branch

Mr Tim Prydon, Technical Director, Employment Systems

Mr Brian Edward McMillan, Employment Counsel

Canberra, Tuesday 1 April 2003

National Office for the Information Economy

Mr Keith Besgrove, Chief General Manager, Regulatory and Analysis Group

Mr John Grant, Chief General Manager, Government Services and Information Environment Division

Mr Tom Dale, General Manager, Regulatory Branch

EDS Australia

Ms Sheelagh Whittaker, Executive Vice President

National Archives of Australia

Mr Stephen John Stuckey, Acting Director-General

Ms Kathryn Patricia Dan, Assistant Director-General, Government Record Keeping

Mr Adrian Edward Cunningham, Director, Record Keeping Standards and Policy

Office of the Commonwealth Ombudsman

Professor John Denison McMillan, Commonwealth Ombudsman

Mr John R. Taylor, Senior Assistant Ombudsman, Professional Standards and Administration

Australian Electoral Commission

Mr Paul Edwin Dacey, Deputy Electoral Commissioner

Ms Barbara Jane Davis, First Assistant Commissioner, Business Support

Mr Kenneth Robert Hunter, Assistant Commissioner, Information Technology

Mr Andrew David Moyes, Assistant Commissioner, Enrolment and Parliamentary Services

Ms Marie Patricia Nelson, Assistant Commissioner, Corporate Services

Mr David Norman Power, Director, IT Business Services

Commonwealth Scientific and Industrial Research Organisation

Mr Philip Gregory Kent, Executive Manager, Knowledge and Information Management

Mr Alan Geoffrey Morrison, Executive Manager, Information Security

Mr Anthony George Wyatt, IT Security Adviser

Attorney-General's Department

Mr Peter Ford, First Assistant Secretary, Information and Security Law Division

Mr Trevor Clement, Assistant Secretary, National Security Hotline

Mr Peter LeRoy, General Manager, Information and Knowledge Services Group

Sydney, Wednesday 2 April 2003

Computer Associates

Mr Christopher Robert Wilson, Regional Manager, Security

Mr Nicholas Engelman, Senior Architect

AUUG Inc

Mr Michael William Paddon, Spokesperson, Member and Past President

Standards Australia International Ltd

Mr Mark Bezzina, Director, Business Standards, Management and Business Communications, IT and eCommerce

Mr Panjan Navaratnam, Projects Manager, Communications, IT and eCommerce

Check Point Software Technologies (Australia) Pty Ltd

Mr Robert Scott Fergusson, Regional Director

Mr Jason Loveday, Systems Engineer

Mr Andrew Bruce Mostyn Hurt, Consultant

SingTel Optus Pty Ltd

Mr David McCulloch, General Manager, Government Affairs

Ms Jill Reich, Sales Executive

Mr David Kidd, Solutions Architect

Office of the Federal Privacy Commissioner

Mr Malcolm Crompton, Federal Privacy Commissioner

Mr Timothy Pilgrim, Deputy Federal Privacy Commissioner

Canberra, Monday 2 June 2003

Australian Federal Police

Mr John Ryles, Director, Information Technology

Federal Agent William Jamieson, Director, Professional Standards

Health Insurance Commission

Dr Brian Richards, Chief Information Officer

Ms Lyn O'Connell, General Manager, IT Services Division

Department of Finance and Administration

Ms Kathryn Campbell, First Assistant Secretary, Social Welfare Division

Mr Dominic Staun, General Manager, Financial and e-Solutions Group

Mr Matthew James Flavel, Branch Manager, Budget Coordination

Mr Mike Loudon, Branch Manager, Procurement

Mr John Nicholson, Branch Manager, Infrastructure Branch

Mr Antony Stinziani, Branch Manager, Strategy and Service Management Branch

Canberra, Monday 16 June 2003

Defence Signals Directorate

Mr Tim Burmeister, Acting Assistant Secretary, Information Security

Ms Lynwen Connick, Assistant Secretary, Information Security

Mr Stephen Merchant, Director

Mr Allan Louis Black, Manager, Government IT Security

Mr Michael Robert Scotton, Manager, Industry Liaison, Information Security Group

Microsoft Australia Pty Ltd

Mr Calum Russell, Group Manager

Canberra, Thursday 19 June 2003

National Office for the Information Economy

Mr Keith Besgrove, Chief General Manager, Regulatory and Analysis Group

Mr John Grant, Chief General Manager, Government Services and Information Environment

Ms Christine Elsley, Manager (Acting), Gatekeeper

Mr Paul Bambury, Assistant Manager, Government Authentication

Defence Signals Directorate

Mr Allan Louis Black, Manager, Government IT Security

Mr Glen Mattocks, Manager, Whole of Government Projects

Canberra, Thursday 26 June 2003

Department of the Treasury

Mr Ian Robinson, General Manager, Corporate Services

Mr Geoff De La Motte, Manager, Information and IT Technology Services

Canberra, Friday 17 October 2003

EDS Australia

Mr Michael Smith, Executive Director, Australian Federal Government Group

Australian Identity Security Alliance

Dr Edward James Essington Lewis, Convenor

Australian Security Intelligence Organisation

Mr James Alexander Nockels, First Assistant Director-General

Department of Transport and Regional Services

Mr David Banham, Chief Information Officer

Mr Robert Fisher, First Assistant Secretary, Corporate

Mr Andrew Tongue, First Assistant Secretary

Mr Peter Yuile, Deputy Secretary

Australian Customs Service

Mr Lionel Woodward, Chief Executive Officer

Mr Murray Harrison, Chief Information Officer

Ms Gail Batman, National Director, Border Intelligence and Passengers

Australian Federal Police

Federal Agent William Jamieson, Director, Professional Standards

Mr John Ashley Ryles, Director, Information Technology

Defence Signals Directorate

Mr Tim Burmeister, Acting Assistant Secretary, Information Security

Mr Stephen John Merchant, Director

Mr Steven Ronald Stroud, Acting Manager, Information Security Policy, Information Security Group

Mr Scott Cameron Macleod, Team Leader, Computer Network Vulnerability Team

Mr Steven Charles Mcleod, Acting Technical Adviser, Computer Network Vulnerability Team

E

Appendix E – Loss of IT Equipment from Commonwealth Agencies, 1998 - 2003

Table 1 Loss of IT Equipment from Commonwealth Agencies, 1998 - 2003

Agency	Laptops	Desktops	Other Hardware
Attorney-General's Department	60	30	22
Department of Agriculture, Fisheries and Forestry	16	15	0
Department of Communications, Information Technology and the Arts	7	5	1
Department of Defence	537[1]		16
Department of Education, Science and Training	24	3	7
Department of Employment and Workplace Relations	50	16	0
Department of Environment and Heritage	75	7	4
Department of Family and Community Services	117	94	5
Department of Finance and Administration	59	35	9
Department of Foreign Affairs and Trade	6	15	16
Department of Health and Ageing	73	37	22
Department of Industry, Tourism and Resources[2]	138	42	22
Department of the Prime Minister and Cabinet	29	2	0
Department of Transport and Regional Services	88	12	0
Department of Veterans' Affairs	16	0	2
Treasury	185	19	2

Source *On 16 September 2003, a letter was sent to the secretaries of all Government departments, requesting information on losses of IT equipment and breaches of security since July 1998. This table summarises their responses.*

1 The Department of Defence reports losing 521 computers, laptops and related hardware, but could not break the figures down further. The Defence Housing Authority reports losing a further 13 laptops and 3 desktops.

2 64 of these items were lost from the CSIRO.

F

Appendix F — Information Security

Public Key Cryptography

The traditional form of encryption, known as symmetrical encryption, used a single secret key to both encrypt and decrypt messages. The weak point is the need for both parties to have the same key. If the key is intercepted and copied while being transmitted from one to the other, the whole system is compromised. Another problem is that a separate key will be needed for each different recipient. If the same key is used, all recipients will be able to read every message, not just the ones directed to them.[1]

In the PKC system, an asymmetric encryption technique is used. That is, the system uses two different but complementary (mathematically related) keys. One of these is known only to the holder – the private key. The other is a public key that can be known to anyone. A message encrypted with the public key can only be decrypted with the corresponding private key and vice versa. This means that anyone can use the public key to send a message and only the holder of the private key can decrypt it.[2]

Practical systems use both symmetric and asymmetric encryption to provide confidentiality. Symmetric encryption is used to encrypt the message using a random key, called the 'message key'. The message key is then encrypted with the

---

1 NOIE, *Online Authentication: A Guide for Government Managers*, NOIE, 2002, p. 7; Roger Clarke, *Message Transmission Security (or 'Cryptography in Plain Text')*, http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html , 11 May 1998, p. 3; and Computer Associates, *Submission No. 52*, p. 2.

2 Roger Clarke, *Message Transmission Security*, pp. 3 and 10; NOIE, *Online Authentication*, p. 8; Mr Engelman, *Transcript*, 2 April 2003, p. 153 and Computer Associates, *Submission No. 52*, p. 2.

recipient's public key. Only the recipient has the private key to decrypt the message key, which can then, in turn, be used to decrypt the message.[3] This method is used to speed up the encryption / decryption process to a practical level because asymmetric encryption takes much longer to process.

To authenticate the identity of the sender or to ensure that a message has not been modified, the message can be sent with a digital signature. A digital signature is a special piece of data related to both the message being sent and to the sender's private key.

To create a digital signature, the message is first processed using a mathematical procedure (a hash function) which creates a hash value. The hash function is designed to be one-way, so it is computationally infeasible for someone to be able to change a message without changing that message's hash value. The hash value of the message is then encrypted with the sender's private key to create the digital signature. The signature is sent along with the message to the recipient.

The recipient can decrypt the signature using the sender's public key, and then check that the same decrypted hash value is obtained by hashing the message that was received. If they are the same, the recipient can be confident that the apparent sender was the real sender and that the message has not been modified.[4]

This process allows the recipient to know who originated the message, that it has not been interfered with and, also, that the sender cannot convincingly deny having sent it. It removes the necessity to safely transmit the key between the two users (It does not, however, provide a defence against a user who allows their private key to be compromised.).[5]

The Public Key Cryptography (PKC) system allows people who have no pre-existing security arrangement, to establish a secure method of information exchange. In an explanatory booklet, *Online Authentication*, the National Office of Information Economy (NOIE) commented:

> The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys and no private keys are ever transmitted or shared.[6]

The system '… is not a foolproof solution to identity management'.[7] If a person's private keys are compromised, unauthorised persons could impersonate them or read their messages. Thus private key security is of paramount importance to

3 NOIE, *Submission No. 57*, pp. 4-5.

4 NOIE, *Submission No. 57*, pp. 4-5; Computer Associates, *Submission No. 52*, p. 2.

5 NOIE, *Online Authentication*, p. 8.

6 NOIE, *Online Authentication*, p. 8.

7 Computer Associates, *Submission No. 52*, p. 3.

users of PKC. This has been highlighted as a crucial weakness of the PKC system as currently used, because few key holders can guarantee the absolute security of their keys.[8]

Even when used correctly, PKC does not absolutely establish the identity of the sender – only that the sender had access to a particular private key. This problem can be resolved by using a trusted third party to verify the association between a public key and the identity of the owner of the associated private key. Once that association has been verified and published in a digital certificate, other parties can trust that the person identified in the certificate holds the private key matching the public key in that certificate. To achieve this, a significant number of infrastructure elements must be in place and functioning securely and effectively.[9]

Benefits of PKC

PKC provides the following attributes for the communication of electronic information:

- **Integrity**: the contents of the message received must be the same as that which was sent;
- **Authentication**: the message can only have been sent by the purported sender; and
- **Non-repudiation**: the sender cannot credibly deny that they sent it.[10]

Public Key Infrastructure

To implement the large-scale use of PKC requires the establishment of a Public Key Infrastructure (PKI), that is:

> … a set of procedures and technology that … enables users of a basically unsecured public network such as the Internet, to securely exchange information through the use of public and private cryptographic key pairs that are obtained and shared through a trusted evaluated infrastructure.[11]

8 Roger Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure*, http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html , 3 May 2001, p. 7.

9 NOIE, *Online Authentication*, pp. 8-9.

10 Roger Clarke, *Message Transmission Security*, p. 2.

11 NOIE, *Online Authentication*, p. 8.

Through the PKI, digital certificates are issued to properly identified applicants. The certificates bind a public key with a verified identity and permit the accurate identification of an organisation or an individual.

The system consists of several components:

- Certification Authorities (CAs): trusted authorities which create and issue digital certificates. They may also create users' private keys (although, in practice, this is rarely done).
- Registration Authorities (RAs): check identities when new certificates are requested and process requests for renewal or revocation of existing certificates. In rare cases they also perform the CA functions of generating keys and certificates.
- Certificate or Key Holders: the end-user. They are issued with keys and certificates which enable them to digitally sign and encrypt electronic documents.
- Relying Parties: who receive, validate and accept digital signatures from key holders / subscribers.
- Repositories: which store and make available certificates and Certificate Revocation Lists (which are maintained by CAs).[12]

PKI employs a digital certificate, which is a digitally signed, structured message that asserts an association between an identity and a public key.[13]

A trusted third party (a CA) creates and distributes the digital certificates. The CA digitally signs each certificate using its own private key. The certificate is provided to the party that claims the particular key to be its own. That party then includes it in the messages that they send.[14]

A CA needs to undertake some form of authentication process in order to satisfy itself that the identity is actually associated with the public key. A conventional approach is to depend on the services of a Registration Authority (RA). A thorough authentication process is highly inconvenient, intrusive and expensive.[15]

PKI also requires an efficient and effective mechanism to revoke compromised certificates. If a certificate owner does not secure a private key, then an impostor can use it to issue certificates in the certificate holder's name. In this situation, the CA must act quickly to inform all interested parties that the certificate and associated key pair are no longer valid.[16]

---

12 NOIE, *Online Authentication*, p. 29.

13 Roger Clarke, *Fundamental Inadequacies of Conventional Public Key Infrastructure*, p. 4.

14 Roger Clarke, *Fundamental Inadequacies of Conventional Public Key Infrastructure*, p. 4.

15 Roger Clarke, *Fundamental Inadequacies of Conventional Public Key Infrastructure*, p. 4.

16 Roger Clarke, *Fundamental Inadequacies of Conventional Public Key Infrastructure*, pp. 5 and 7.

This model of PKI is inherently hierarchical. A CA issues digital certificates using its own certificate, which must be issued by a higher CA. This CA must, in turn, be certified by a still higher CA. Ultimately, a supreme CA is required, in which everyone must trust. This situation is unlikely to be achievable in reality.[17]

PKI assumes that the owner of a private key will be able to ensure its security. However, no CA can guarantee this. Private keys may be the target of crackers, viruses or worms. Hardware and software systems currently provide very little in the way of security features. Moreover, few products are available that enable consumers to graft such security features on to their systems. Those that are available require considerable expertise to install and configure. All of this contributes to the difficulty of maintaining the security of individual keys, which, as mentioned earlier, is a significant point of vulnerability in PKI.[18]

The CA is expected to assure that the user of a certificate is who they claim to be. If such an assurance is incorrect and a party's reasonable dependence on that assurance results in economic cost, it would be natural to assume that the CA would be held responsible. In practice, few CAs are willing to take on this responsibility. Their policy statements are usually phrased to limit their exposure to liabilities. CAs cannot reasonably expect their offers of assurance to be taken seriously, if they are not willing to stand by that assurance.[19]

Gatekeeper

The Commonwealth PKI system is known as the Gatekeeper project. NOIE commented that Gatekeeper is not a product, as many people think, but a framework of standards used to measure the capability of applicants seeking accreditation as service providers.[20]

In late 1997 a number of agencies were investigating ways to enhance their service delivery by conducting business electronically. PKC was emerging as an accepted means of authenticating users to ensure the security of electronic transactions. The Government decided to develop a national framework for the authentication of users of electronic online services. The then Office of Government Information Technology (OGIT) was charged with developing a strategy for the

17 Roger Clarke, *Fundamental Inadequacies of Conventional Public Key Infrastructure*, p. 6.

18 Roger Clarke, *Fundamental Inadequacies of Conventional Public Key Infrastructure*, p. 7.

19 Roger Clarke, *Fundamental Inadequacies of Conventional Public Key Infrastructure*, pp. 8-9.

20 Ms Elsley, *Transcript*, 19 June 2003, p. 290; Mr Besgrove, *Transcript*, 19 June 2003, p. 293.

Commonwealth Government's use of PKC. OGIT formally established Project Gatekeeper in October 1997, and it was launched in May 1998.[21]

Application of the Gatekeeper standards is not compulsory for most Commonwealth agencies – each agency must make its own assessment of its need for security. However, if the agency's assessment is that PKI is necessary, application of the Gatekeeper standards becomes compulsory for external use.[22]

On the other hand, firms or agencies wishing to become service providers must go through a long and comprehensive process to prove that they can meet all of the requirements of the Gatekeeper standards.[23]

Gatekeeper Accreditation

Firms or agencies seeking accreditation as Gatekeeper service providers – CA or RA – must meet stringent requirements which encompass all security enforcing aspects of their business and its operations. Accreditation is applied to the organisation, not their products. To use NOIE's words:

> The purpose of Gatekeeper accreditation is to provide an objective standard against which the competence of an organisation to deliver certification services can be assessed.[24]

Physical security of the premises is checked thoroughly by the Australian Security Intelligence Organisation (ASIO); the extent of the checks depending on what role is being requested under Gatekeeper. Different standards apply for CAs and RAs but in each case they would need to be assessed as Highly Protected by ASIO for their application to proceed.[25]

The Defence Signals Directorate (DSD) carries out a detailed evaluation of the security of the applicant's IT system. This process includes an evaluation of the software involved.[26]

Operational evaluation of the applicant is handled by NOIE, which examines the applicant's operations manuals, their disaster recovery and business continuity plans and carries out a legal evaluation. The latter is necessary to establish the required level of trust for clients of the applicant.[27]

---

21 Gatekeeper Strategy, *http://www.noie.gov.au/projects/confidence/Securing/Gatekeeperstrategy.htm*, 23 May 2003.

22 NOIE, *Online Authentication*, pp. 8-9.

23 Ms Elsley, *Transcript*, 19 June 2003, pp. 290-1.

24 NOIE, *Submission No. 57*, p. 4.

25 NOIE, *Submission No. 57*, p. 1.

26 Ms Elsley, *Transcript*, 19 June 2003, p. 292; NOIE, S*ubmission No. 57*, p. 6.

27 Ms Elsley, *Transcript*, 19 June 2003, p. 292.

A Certification Practice Statement is developed by each CA/RA which covers the operations, infrastructure and the certificates to be issued. For each different type of certificate to be issued, a separate Certificate Policy is developed.[28]

Security vetting of applicants is rigorous. The staff of each applicant must be vetted to the Highly Protected level. This is carried out by the Australian Security Vetting Service and the Australian Protective Service. Under the Gatekeeper arrangements, all service providers must also be on the endorsed supplier list administered by the Department of Finance.[29]

When all of the requirements have been met to the satisfaction of the Chief Executive Officer of NOIE, a contract is signed on behalf of the Commonwealth. The contract sets out in detail the obligations the service provider must fulfil. Every 12 months thereafter they must undergo a compliance audit to ensure that the Gatekeeper criteria are still being satisfied. The audits are carried out by one of a panel of auditors established and approved by NOIE.[30]

At the time of the inquiry, the NOIE advised that eight organisations had achieved full Gatekeeper accreditation:

- Secure Net Limited as CA;
- Pricewaterhouse Coopers (beTRUSTed) as CA and RA;
- Australia Post as RA;
- Telstra Corporation Limited as CA and RA;
- eSign Australia Limited as CA and RA;
- Health eSignature Authority Pty Ltd as RA;
- Baltimore Certificates Australia Pty Ltd; as CA; and
- Australian Taxation Office as CA and RA.[31]

In addition, the ANZ Bank was then undergoing the evaluation process for Gatekeeper accreditation.[32]

Commonwealth Agencies Using Gatekeeper

Government agencies participate voluntarily in Gatekeeper.[33] To date, very few agencies have chosen to participate. NOIE attributes this in part to the slow acceptance of PKC and the slow growth of the PKI market.[34]

28 NOIE, *Submission No. 57*, pp. 5-6.

29 NOIE, *Submission No. 57*, pp. 7-8; Ms Elsley, *Transcript*, 19 June 2003, p. 292.

30 Ms Elsley, *Transcript*, 19 June 2003, pp. 292-3.

31 NOIE, *Submission No. 57*, p. 5.

32 NOIE, *Submission No. 57*, p. 5.

33 Gatekeeper Strategy, *http://www.noie.gov.au/projects/confidence/Securing/Gatekeeperstrategy.htm*, 23 May 2003.

34 Mr Besgrove, Mr Dale, *Transcript*, 1 April 2003, p. 73

The Australian Tax Office (ATO) was the first agency to attain full gatekeeper accreditation for their Certification Authority in May 2000. The Health Insurance Commission uses the authentication services of Health eSignature Authority Pty Ltd, which is a Gatekeeper certified Registration Authority.[35]

Some Government agencies have little or no need for certification. The type of business conducted by the Australian Bureau of Statistics (ABS) does not warrant the Bureau seeking certification. As it commented: "People tend not to fraudulently lodge statistical returns on behalf of other people".[36] Similarly, the Attorney-General's Department said that it has not yet found a business use for Gatekeeper.[37]

Other Government agencies have found that their authentication needs are met by less formal PKC, such as the Secure Socket Layer (SSL) protocol. The Department of Employment and Workplace Relations said that it currently finds SSL to be sufficient:

> We believe that secure socket layer security is more than adequate for our interacting with the Job Network. …Certainly it is working well at the moment.[38]

Limitations of Gatekeeper

A frequent comment by Government agencies and private companies was that Gatekeeper is too complex and / or expensive.[39] NOIE at first estimated that achieving Gatekeeper accreditation costs around $300,000 but later commented that depending on circumstances and requirements, the cost has varied, in practice, between $200,000 and $2.2 million.[40]

Some Government agencies are using authentication services that are not Gatekeeper accredited. A number of private companies offer their own authentication services in competition with Gatekeeper. These include Computer Associates and Check Point Software Technologies (Australia) Pty Ltd. Agencies outsourced to these companies use their services rather than those of a Gatekeeper accredited provider.[41]

---

35 Mr Farr, *Transcript*, 31 March 2003, p. 38; Gatekeeper Accreditation, *http://www.noie.gov.au/projects/confidence/Securing/GatekeeperAccreditation.htm*, 28 May 2003.

36 Mr Palmer, *Transcript*, 31 March 2003, p. 34.

37 Mr LeRoy, *Transcript*, 1 April 2003, p. 134.

38 Mr Burston, *Transcript, 31 March 2003*, pp. 63-64.

39 Ms Treadwell, *Transcript*, 31 March 2003, p. 30; Mr Besgrove, *Transcript*, 1 April 2003, p. 73; Mr Wilson, *Transcript*, 2 April 2003, p. 148; Ms Reich, *Transcript*, 2 April 2003, p. 194.

40 Mr Grant, *Transcript*, 1 April 2003, p. 80.

41 Mr Engelman, *Transcript*, 2 April 2003, p. 147; Mr Ferguson, *Transcript*, 2 April 2003, p. 184.

A key point in the security of any PKI system is the fast and effective revocation of compromised keys. However, some witnesses considered that Gatekeeper does not make adequate arrangements for managing the revocation of compromised keys. This is seen by some as a critical weakness.[42]

AUUG expressed concern that the authentication needs of Government agencies will not always align with the needs of commercial Gatekeeper providers: "…a commercial organisation has different goals from government and from the citizenry as a whole." AUUG said that it is unclear how the alignment was to be maintained over a significant period of time.[43]

It was also claimed that there is evidence showing that Gatekeeper is fundamentally flawed. In addition to the problem of compromised keys, the main weaknesses are that:

- CAs do not stand by their product, and offer extremely limited warranties and liabilities;
- users cannot guarantee adequate protection for their private keys; and
- users may be required to submit to intrusive authentication processes, which could still be circumvented by a determined impostor.[44]

Authentication of Individuals

PKI can be useful for authenticating individuals in their dealings with Government agencies. However, there are many problems with applying authentication to individuals.

Authentication will allow individuals to reliably present an identity to Government agencies. An individual user would register their identity with a Registration Authority (RA) and receive a certificate from a Certification Authority (CA). The individual could then use this certificate with all Government agencies, since the agencies will be able to verify the identity of the client with the CA.

Authentication will improve the efficiency of Government service delivery. Currently, however, there is no whole-of-government approach to the authentication of individuals.[45] An individual conducting business with several

42 Mr Roger Clarke, *Submission No. 51*, p. 4; AUUG, *Submission No. 58*, p. 2.

43 Mr Paddon, *Transcript*, 2 April 2003, pp. 160-1.

44 Mr Roger Clarke, *Submission No. 51*, pp. 3-4.

45 Management Advisory Committee, Report 2, *Australian Government Use of Information and Communication Technology: A New Governance and Investment Framework*, 2002, p. 35.

Government agencies must go through the process of registering their identity with each one. If, for example, a client's address changes, each of the agencies that they deal with must be separately informed.

Time and effort could be saved if each individual only had to register their identity once and report any changes once. The Privacy Commissioner recognised, however, that there will always be some people who do not want their private information connected in this way – this complicates even further, what is already a difficult problem.[46]

Preventing Multiple Identities and Identity Theft

Authentication is a useful tool for the prevention of identity abuse. In the past, there have been cases of Centrelink clients fraudulently claiming multiple benefits using multiple identities.[47] If a rigorous authentication process is in place, it should be able to detect when a person applies to register a second identity. Biometrics will soon make this a practical possibility. The information available to the RA should then prevent anyone from fraudulently registering a second identity.

Authentication can also help to prevent identity theft. This occurs when an impostor acquires enough information to impersonate another person. For example, an individual's certificate may be stolen and then used to impersonate them in dealings with Government agencies. Using PKI, the certificate issued to the individual could include identifying information, allowing Government agencies to check that the holder of the certificate is the person to whom the certificate was issued. Biometrics will also have an application here. PKI allows any certificate to be quickly revoked if it is compromised.

Difficulties with the Authentication of Individuals

The problem remains of how an individual can be reliably authenticated. When an individual applies for a certificate, how does the RA establish that they are who they say they are? Biometrics does not help to solve this problem; it can only prove that the individual is the same one from whom the biometric data was gathered. Current practices call for the individual to provide a number of identifying documents, such as a driver's licence, passport or birth certificate. However, these documents do not conclusively prove identity. Some of them can be obtained

46 Mr Crompton, *Transcript*, 2 April 2003, p. 211.

47 Computer Associates, *Submission No. 38*, p. 5; Mr Engleman, *Transcript*, 2 April 2003, p. 144.

without rigorous proof of identity and these could then be used to obtain other identifying documents.[48]

PKI assumes that the owner of a private key will be able to ensure its security. The average individual does not have the understanding or skills to do this. Private keys stored on hardware devices, such as smartcards, can be lost or stolen. Private keys stored on software are only as secure as the computer system which stores them. Individuals cannot be relied on to completely secure their computer systems. Thus, private keys in the hands of individuals cannot be assumed to be secure and their certificates cannot automatically be accepted as genuine.[49]

Certificate revocation is not practical when applied to individuals. When a private key is compromised and its certificate revoked, every PKI user must be informed as soon as possible so that they do not accept the compromised certificate. If PKI is applied to individuals, then this would mean informing millions of users each time a certificate is revoked. This could happen several times each day, resulting in an enormous amount of communications traffic. Further, revocation assumes that all PKI users will act on revocation notices immediately and keep their certificate lists up to date. Individuals cannot be relied upon to systematically do this. Thus, there is no practical way to ensure that individual PKI users are not accepting bogus certificates.[50]

Is There a Solution in Sight?

There is no evidence before the Committee which provides a satisfactory solution to these problems. Therefore, the Committee suggests that there is still considerable work to be done before an attempt is made to implement a comprehensive PKI framework for the authentication of individuals.

The Management Advisory Committee (MAC) of the Australian Public Service Commission has considered the issue of authenticating individuals. Its recommendations aim to achieve a consistent approach across Government departments. This may involve establishing primary identity documents for registering with Government agencies, supported by the establishment of a national online identity document validation framework.[51]

The approach proposed by the Management Advisory Committee does not necessarily involve PKI, so it may not have the same difficulties. However, it does

48 Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy*, http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html , December 1994, pp 14-17.

49 Roger Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure*, p. 7.

50 Roger Clarke, *The Fundamental Inadequacies of Conventional Public Key Infrastructure*, p. 7.

51 MAC, Report No.2, p. 35.

not address the problem of how an individual's identity can be definitively authenticated, so that primary identity documents can be issued with confidence. The latter issue will need to be satisfactorily addressed before PKI can be confidently used to identify individuals.