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

Foreword....................vii

Membership of the Committee.................... xi

Membership of the Sectional Committee....................xii

Duties of the Committee....................xiii

Terms of reference.................... xv

List of abbreviations....................xvii

List of recommendations.................... xxi

REPORT

1 Security and Integrity of Electronic Information....................1

Introduction....................1

The Setting....................2

The Committee's Inquiry....................4

Report Structure....................6

Existing Legislation....................6

2 Physical Security....................9

Introduction....................9

Physical Security of IT Networks....................10

Building Security....................10

Visitor Identification....................11

Survey of Equipment Losses....................13

IT Equipment Lost by Agencies 14
Telstra Incident 16
Laptop Computers 16
Committee Comment 18
Asset Registration 19

3 Management of Outsourcing Contracts 23

Accountability Remains with Agency 25
When is Outsourcing Appropriate 26
Addressing Security Issues in Outsourcing Contracts 27
Addressing Privacy Issues in Outsourcing Contracts 29
Committee Comment 30

4 Risk Management 31

Introduction 31
Broad Risk Management 32
Risk Management Lifecycle 33
Analysis 34
Implementation 40
Testing 43
Committee Comment 43

5 Data Preservation 45

Introduction 45
Archival Integrity 47
Media Degradation 47
Application Obsolescence 48
Business Continuity and Disaster Recovery 49

6 Information Security 53

Introduction 53
Public Key Cryptography 54
Digital Certificates 55
Public Key Infrastructure 55

Gatekeeper **56**
Gatekeeper Accreditation 57
Commonwealth Agencies Using Gatekeeper 58
Limitations of Gatekeeper 59
Alternative Systems **61**
PKI Framework for the Authentication of Individuals **61**
Once Only Proof of Identify 61
Preventing Multiple Identities 62
Preventing Identify Theft 62
Authenticating Individuals 62

7 Evaluation of Products under AISEP 65

Introduction **65**
Evaluation Criteria **66**
Evaluation and Certification Process **67**
Benefits of AISEP **68**
Conflict of Interest **68**
Cost and Duration of the Evaluation Process **69**
Committee Comment **73**

8 Other Issues 75

National Information Infrastructure **75**
Committee Comment 77
Report by Management Advisory Committee **78**
Whole-of-Government Approach 78
Data Sharing Between Agencies 79
Proposals and Conclusions 80
Committee Comment 81
Closed vs Open Source Software **81**
The Differences 82
The Arguments 82
Committee Comment 85

APPENDICES

Appendix A — Electronic Information under Review by ANAO 87

Appendix B — List of Submissions.. 89

Appendix C — List of Exhibits 93

Appendix D — List of Witnesses Appearing at Public Hearings........................... 95

Appendix E – Loss of IT Equipment from Commonwealth Agencies,

1998 - 2003 101

Appendix F — Information Security 103

Public Key Cryptography 103

Public Key Infrastructure... 105

Gatekeeper... 107

Authentication of Individuals.. 111

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.