December 2002

Dr Margot Kerley
The Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Dr Kerley

Review of the Management and Integrity of the Commonwealth's Electronic Information

The Australian National Audit Office (ANAO) welcomes the opportunity to provide a submission to the Joint Committee of Public Accounts and Audit "Review of the Management and Integrity of the Commonwealth's Electronic Information".

The ANAO agrees that it is timely to review the framework governing the Commonwealth's electronic information. The use of Information Communication Technology (ICT) within government agencies has become increasingly significant in recent years, particularly following the greater dependence on the Internet and organisational intranets, with a range of government services now provided directly to the public online. As a result, there is increasing dependence on information and the ICT systems that support these services, as well as a range of risks that have to be managed effectively. This has resulted in the continuing need to take advantage of ICT advances to achieve key business objectives and to improve service delivery. ICT is now a key component of business strategy and core business processing, and the management of ICT risk is a key part of corporate governance. Consequently, effective management of ICT is critical to the success of most entities.

Consistent with your request for an electronic copy, I will also arrange for a copy of this letter and the ANAO submission to be emailed to the JCPAA Secretariat. Please do not hesitate to contact Dr Paul Nicoll on telephone number 6203 7759 if you have any queries in relation to this submission, or there are any matters that you would like to discuss further.

Yours sincerely

P.J. Barrett

Submission by the Australian National Audit Office to the JCPAA Review of the Management and Integrity of the Commonwealth's Electronic Information.

TABLE OF CONTENTS **PAGE**

Executive Summary

This ANAO submission:

- outlines the Australian National Audit Office's (ANAO's) interest in the management and integrity of the Commonwealth's electronic information;
- identifies those ANAO performance, business support process, financial statement and related controls audits most relevant to the Committee's review; and
- summarises the major findings of these audits against each of the Committee's terms of reference.

The Commonwealth Government is a major user of information and communications technology (ICT). In its recent report, *Australian Government Use of Information and Communications Technology*, the Management Advisory Committee reported that the Commonwealth Government spends around $3.5 billion annually on ICT – (an estimated $2.1 billion recurrent and up to $1.4 billion capital).[1] The Parliament, Government and the community expect Commonwealth bodies to adopt sound practices to assure the integrity and security of information holdings, consistent with relevant legislation and guidance. Agencies' governance should give confidence in public administration and inform chief executive officers of both the performance of agencies and significant issues which may require attention concerning the management and integrity of electronic information.

In recent years, ANAO's audit reports have drawn attention to shortcomings in some areas, such as problems in control structures reviewed as part of financial statement audits, and generic issues raised in performance audits directly relevant to the Committee's terms of reference. These performance audits have addressed, for example, the adequacy of Internet security and of agency record keeping, and identified significant issues for agencies to review. In addition, the ANAO has completed several other performance audits which covered, in part, some of the issues that the Committee is examining. The findings from those other audits indicated both sound practice in some areas, and in others where agencies' management of Commonwealth electronic information could improve.

Key issues identified in ANAO's audits relevant to the Committee's terms of reference include:

- adequacy of agencies' implementation of the Privacy Principles when using ICT;
- the importance of agencies' security plans addressing privacy issues;
- reduced efficiency of computer-based identity fraud detection methodologies due to data coding errors;
- the continuing need for agencies to ensure the quality and integrity of their data;
- considerable variance in the adequacy of agencies' Internet security, with six of ten agencies audited with websites containing significant vulnerabilities, potentially exploitable by a malicious user;
- the importance of agencies consistently applying the Government's Internet security policies, thereby adopting a structured approach to Internet security;

[1] Management Advisory Committee, *Australian Government Use of Information and Communications Technology. A New Governance and Investment Framework*, Commonwealth of Australia, Canberra, October 2002.

- the difficulty of some agencies in providing Parliament with an assurance that all significant records were being kept in accordance with Archives Act requirements;
- the varying adequacy of the methods used by agencies – participating in a major audit of recordkeeping – to capture and manage electronic records;
- the existence of control weaknesses over the management of user access, maintenance of audit trails, monitoring and review of privileged users and in some cases the segregation of duties in important information technology systems;
- limited agency use of FedLink, which is a secure encrypted inter-agency communications service; and
- the consistency of advice and requirements in policies and procedures.

Introduction

ANAO's interest in the management and integrity of the Commonwealth's electronic information is based on the need for reliable, accurate and well-managed data to:

- maintain the trust of the individual, community and business clients in government programs. These clients of government programs will be more comfortable providing data if they have confidence in the management of those data;
- maximise the effectiveness and efficiency of program delivery where the latter relies on accurate and reliable data; and
- protect the Commonwealth's assets, including its data holdings.

The use of ICT within government entities has become increasingly significant in recent years, particularly following the greater dependence on the Internet and organisational intranets, with a range of government services now provided directly to the public online. As a result, there is increasing dependence on information and the ICT systems that support these services, as well as a range of risks that have to be managed effectively. This has resulted in the continuing need to take advantage of ICT advances to achieve key business objectives and to improve service delivery. ITC is now a key component of business strategy and core business processing, and the management of ICT risk is a key part of corporate governance. Consequently, effective management of ICT is critical to the success of most entities.[2]

The ANAO's audits have tended to focus on IT rather than on ICT. However, many of the IT findings apply to ICT as well. The ANAO has reviewed relevant aspects of IT within Commonwealth entities during the conduct of financial statement audits, and performance audits which can include, in part, IT or they can be full performance audits of the management of IT.

The CEOs of Commonwealth agencies, including those governed by the *Financial Management and Accountability Act 1997* and the *Commonwealth Authorities and Companies Act1997*, are responsible for the management of Commonwealth electronic information.

Electronic information includes:

- digital files such as email, word documents, spreadsheets, CD-ROM data;
- multimedia files such as videos and sound recordings;
- information system databases; and
- internal and external web-based information.

Electronic information activities include:

- information and communications technology and systems management and development;
- data management;
- recordkeeping; and
- transaction management underpinning public sector electronic business.

[2] ANAO Report No. 67 of 2001-2002, *Control Structures as part of the Audit of Financial Statements of Major Commonwealth Entities for the Year Ending 30 June 2002*, ANAO, Canberra, 2002.

Public sector personnel most involved in these tasks are:

- outputs and outcomes managers;
- information system specialists;
- records and archival specialists;
- information and communication technology providers;
- webmasters; and
- information and communications management specialists

The ANAO has conducted a number of different kinds of audits which are relevant to the JCPAA's review.

This submission draws upon the primary findings from the following ANAO audits:

- *Managing Data Privacy in Centrelink*, tabled in 1999;
- *Internet Security within Commonwealth Government Agencies*, tabled in 2001;
- *Management of the Provision of Information to Job Seekers*, tabled in 2002;
- *Integrity of the Electoral Roll* tabled in 2002;
- *Recordkeeping*, tabled in 2002; and
- *Control Structures as part of the Audit of Financial Statements of Major Commonwealth Entities for the Year Ending 30 June 2002*, tabled in 2002.

The submission refers to relevant findings from several other ANAO audits, where issues associated with the management and integrity of electronic information were addressed by ANAO as part of a wider focus. A complete list of relevant audits is provided in the Appendix.

ANAO's Audit Objectives and Findings against the Committee's Terms of Reference

The privacy, confidentiality and integrity of the Commonwealth's electronic data

The key issues that ANAO's audits have identified and addressed under this term of reference for the Committee include:

- adequacy of agencies' implementation of the Privacy Principles when using ICT;
- the importance of agencies' security plans addressing privacy issues;
- reduced efficiency of computer-based identity fraud detection methodologies due to data coding errors; and
- the continuing need for agencies to ensure the quality and integrity of their data.

Privacy and Confidentiality

The ANAO in recent years has completed a major audit of data privacy, *Managing Data Privacy in Centrelink*, tabled in 1999-2000[3]. A second audit, *Information Technology at the Department of Health and Ageing*, tabled in 2002-03[4], also covered aspects of the privacy of electronic data.

Centrelink

The ANAO data privacy audit objective was to assess Centrelink's data protection systems. This included reviewing policies, procedures and the administrative framework associated with data privacy and computer systems that are used to store and disseminate data.

The ANAO concluded that Centrelink had established key elements of a sound framework to meet the Information Privacy Principles in the Privacy Act and confidentiality provisions in other legislation. Generally, suitable policies, procedures and systems relevant to privacy issues were also in place. However, Centrelink's framework for the management of data privacy was incomplete at that time because an assessment of risks to data privacy and planning, and action to minimise those risks, had not been conducted at an organisation-wide level. As well, Centrelink's performance information on the actual number of privacy breaches or significant influencing factors was not adequate for performance management or accountability purposes. Consequently, Centrelink's management was unable to be assured of the effectiveness, in practice, of the elements of its framework . The ANAO made a number of recommendations aimed at improving the management and controls relevant to the collection, processing, storage, access, use and disclosure of personal information. Centrelink agreed with those recommendations.

During a subsequent audit, *Management of Fraud and Incorrect Payment in Centrelink* tabled in 2001-2002[5], the ANAO reported that Centrelink had made significant progress and had developed a Privacy Awareness Strategy. Centrelink had also established Area Privacy

[3] ANAO Report No. 8 of 1999-2000, *Managing Data Privacy in Centrelink*, ANAO, Canberra, 1999.
[4] ANAO Report No. 1 of 2002-2003, *Information Technology at the Department of Health and Ageing*, ANAO, Canberra, 2002.
[5] ANAO Report No. 26 of 2001-2002, *Management of Fraud and Incorrect Payment in Centrelink*, ANAO, Canberra, 2001.

Officers (APOs) in each area support office, to keep staff aware of the importance of maintaining the privacy of client data. In the twelve months leading to 30 September 2000, over 3700 Centrelink staff members received privacy awareness training. APOs are also responsible for investigating alleged privacy breaches and have access to customer record access monitor reports that can be used to identify cases where there has been unauthorised use of information, unauthorised access of information or unauthorised disclosure of information obtained from the mainframe.

Department of Health and Ageing (Health)

The ANAO's 2002 performance audit of information technology at the Department of Health and Ageing reviewed systems security. The ANAO reported that there were some privacy and confidentiality risk issues that required management attention.

At the commencement of the audit, the Health's Information Planning and Privacy Committee (IPPC) had not developed policy or guidelines to ensure compliance with the information privacy principles of the Privacy Act. Subsequently, the IPPC has identified Health's privacy principles compliance requirements. Resources have been assigned, and Health is working towards the development of privacy policy and guidelines by December 2002.

The ANAO's review of application security plans indicated that information privacy requirements had not been adequately addressed as none of the plans reviewed had considered privacy issues. Improvement opportunities were identified in the content and timeliness of completion of individual system security plans, and in the practice of using production data (that contains personal information) for testing purposes.

Data Integrity

The ANAO has conducted several data integrity reviews within the context of three performance audits. These are *Management of Fraud and Incorrect Payment in Centrelink*[6] and the *Integrity of the Electoral Roll,*[7] both tabled in 2001-2002; and *Information Technology at the Department of Health and Ageing* tabled in 2002-03[8].

Fraud Management

The ANAO fraud management audit objective was to assess whether Centrelink had implemented appropriate fraud control arrangements in line with the fraud control policy of the Commonwealth and whether these arrangements were operating effectively in practice.

The ANAO reported[9] that while Centrelink had a clear focus on prevention of fraud and had established appropriate procedures in relation to proof of identity, there were coding errors in 22 per cent of the claims reviewed. Inaccurate information held on Centrelink systems adversely affected the quality of Centrelink's electronic records. This, in turn, reduced the efficiency of existing computer-based identity fraud detection methodologies and resulted in additional administrative costs for Centrelink.

[6] ANAO Report No. 26 of 2001-2002, *Management of Fraud and Incorrect Payment in Centrelink*, ANAO, Canberra, 2002.
[7] ANAO Report No. 42 of 2001-2002, *Integrity of the Electoral Roll*, ANAO, Canberra, 2002.
[8] ANAO Report No. 1 of 2002-2003.
[9] ANAO Report No. 26 of 2001-02.

The ANAO also found that Centrelink had maintained an effective compliance function and had a range of controls for detecting fraud and incorrect payment. This included the use of an extensive data-matching program that matched data with a large number of Commonwealth, State and Territory agencies. This was guided by business rules and risk parameters designed to enable higher risk cases to be identified based on key criteria, such as recent employment history. Appropriate processes had been established by Centrelink for ensuring that the data-matching it conducted conformed with the requirements of data-matching and privacy legislation.

Data Integrity Management

The Australian Electoral Commission (AEC) performance audit objective was to provide an opinion on the integrity of the electoral roll, that is, its accuracy, completeness, validity and security. In addition, the audit examined how well the AEC ensured the integrity of the electoral roll.

The ANAO concluded[10] that, overall, the Australian electoral roll was one of high integrity, and it can be relied on for electoral purposes. AEC policies and procedures can provide an electoral roll that is accurate, complete, valid and secure. In particular, the AEC had mechanisms in place to provide assurance that the names and addresses on the electoral roll are legitimate and valid; and that people who are eligible to vote are registered properly.

At the same time, there are areas of AEC management of the roll that can be improved; in particular by better targeting and expansion of the data sources currently used to update the roll, by strengthening strategic relationships with the key stakeholders, and by better identification and management of risks to the integrity of the roll. [11]

Data Management

The ANAO's 2002 report, titled *Information Technology at the Department of Health and Ageing*[12], had as its objectives to determine whether Health's management and operation of its selected systems met industry better practice; met the required quality and service delivery parameters; and whether these systems operated effectively, efficiently and economically. The ANAO selected three major applications for evaluation, representing systems that process approximately $3.9 billion of expenditure.

The ANAO concluded[13] that, overall at the operational level, systems reviewed were delivering the required business outputs in an effective and controlled manner, and within acceptable error rates. Extensive testing of those systems found data to be accurate, complete and consistent and that Health had implemented an appropriate level of management reporting to monitor data integrity.

[10] ANAO Report No.42 of 2001-2002.
[11] The Joint Standing Committee on Electoral Matters has followed up the matters raised in the ANAO's report. Joint Standing Committee on Electoral Matters, *Integrity of the Electoral Roll, Review of ANAO Report No. 42, 2001-2002, Integrity of the Electoral Roll,* House of Representatives, Parliament House, Canberra, 2002.
[12] ANAO Report No. 1 of 2002-2003.
[13] ANAO Report No. 1 of 2002-2003.

The management and security of electronic information transmitted by Commonwealth agencies

The key issues identified in ANAO's audits and addressed under this term of reference for the Committee include:

- considerable variance in the adequacy of agencies' Internet security, with six of ten agencies audited with websites containing significant vulnerabilities, potentially exploitable by a malicious user;
- the importance of agencies consistently applying the Government's Internet security policies, thereby adopting a structured approach to Internet security;

Internet Security

Following the announcement of the Government Online initiative in 1997 and the requirement for Commonwealth agencies to have all appropriate services online by 2001, the Internet has become a major aid in the delivery of government programs.

The ANAO, in partnership with the Defence Signals Directorate (DSD), conducted an across-agency audit of Internet security. The audit reviewed Internet security in ten government agencies. The results were published in Audit Report No. 13 of 2001-2002, *Internet Security within Commonwealth Government Agencies*[14]. The objective of the audit was to form an opinion on the adequacy of Commonwealth agencies' management of Internet security.

The ANAO concluded that security levels across the audited agencies[15] varied significantly from very good to very poor. For the majority of agency websites covered in the audit, the level of Internet security was insufficient, given the threat environment and vulnerabilities identified within a number of agency sites. Further, while some agencies had produced good threat and risk assessments and documentation generally, these were not always effectively administered. Overall, a number of agencies had opportunities to improve performance in some key areas and all agencies had opportunities to improve performance in one or more aspects of managing Internet security. Generally, agencies approaches the management of Internet security in a way that was broadly consistent with Commonwealth policy directions, promoted in the Commonwealth Protective Security Manual and the Australian Communications – Electronic Security Instructions-33.

The key findings were that:

- Agencies approached the management of Internet security in a way that was broadly consistent with Commonwealth policy directions, promoted in the Commonwealth Protective Security Manual and the Australian Communications – Electronic Security Instructions-33;

[14] ANAO Report No. 13 of 2001-2002, *Internet Security Within Commonwealth Government Agencies,* ANAO, Canberra, 2001.

[15] The 10 participating agencies were: Australian Bureau of Statistics; Australian Competition and Consumer Commission; Australian Customs Service; Australian Electoral Commission; Australian Radiation Protection and Nuclear Safety Agency; Australian Taxation Office; Department of Agriculture, Fisheries and Forestry; Department of Employment, Workplace Relations and Small Business; Department of Health and Aged Care; and Department of the Treasury.

- All agencies had prepared an IT security policy, as required by the Protective Security Manual, but that these varied in quality and the extent to which they referred to an agency's Internet presence;

- Only the larger agencies, particularly those that managed their Internet presence using in-house resources, developed comprehensive security plans, disaster recovery or business continuity plans;

- Six of the ten websites tested by DSD staff were found to manage websites containing significant vulnerabilities, potentially exploitable by a malicious user over the Internet. In addition, the audit team identified other security issues in all sites;

- Where Commonwealth websites were hosted and managed using in-house resources, the level of co-ordination and communication between relevant groups was substantially better than when site management was contracted to an external service provider;

- Where intrusion detection systems were employed, usually in fairly large and complex Internet gateways, these were generally well-managed and represented a strong addition to the overall security of the gateway;

- Nine of the ten agencies had implemented anti-virus products appropriately;

- The testing program also revealed that policy and procedures for the review of audit logs was very poor. The ANAO highlighted the importance to agencies of the need to audit security logs in order to manage threats;

- The better performing agencies had comprehensive knowledge of their systems, clearly defined responsibilities for key players, an active approach to maintaining security and the ability to respond quickly to issues and incidents as they arise; and

- Agencies operating websites that involved the transmission of personal information or sensitive commercial information between clients and an agency were, in general, found to pay adequate attention to protecting the privacy of the individuals concerned.

Individual reports were presented to each of the ten agencies. These individual agency reports included managerial and technical recommendations on security policies, and on plans and management systems supporting the achievement of IT security policy objectives. Findings and recommendations varied in their importance.

The audit report made a number of recommendations with applicability to all Commonwealth agencies as follows:

- Agencies should adopt a structured approach to the management of Internet security, employing a sound risk management model. This is reinforced in the Commonwealth's published policy on information security;
- Agencies should ensure that appropriate risk assessments are conducted. Prior to introducing a new ICT system, web based application or instituting a major change to

current online services, a risks assessment should be undertaken to identify any new or untreated risks;

- Agencies should avoid default installations of operating system and web server software. These systems should be security hardened by removing unnecessary services and functionality which could represent risks to the integrity of the web servers;
- Agencies should test and install security patches in a timely manner. Knowledge of particular vulnerabilities spreads quickly on the Internet, and many hackers target recent vulnerabilities in the hope that web server administrators have not installed the relevant security patches;
- Security administrators should regularly review logs. Access logs and event logs are a rich source of information for the web server administrator. Analysing these logs may provide considerable insight into the usage patterns of a website and highlight suspicious or unusual activity;
- Agencies should ensure that applications which support transactions with users, such as active content, are reviewed for secure coding practices. Having such code revised by a third party, ie, someone not involved in writing or implementing the code, enhances the level of security associated with the application; and
- Agencies should ensure that relevant documentation is kept up to date. Security documentation (such as policies, plans and network descriptions) is of most use to security administrators when it is comprehensive and kept up to date.

The ANAO's interest in promotion of better approaches to Internet security was shown by the release in 2002 of a Better Practice Guide, titled, *Internet Delivery Decisions. A Government Program Manager's Guide.* The Guide included a component titled, *Internet Systems Security and Authentication for Government Programs.* The Guide's primary audience includes non-technical program managers. That is because they have an essential role in ensuring the implementation of the Government's requirements.

The management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks

The key issues identified in ANAO's audits and addressed under this term of reference for the Committee include:

- the difficulty of some agencies in providing Parliament with an assurance that all significant records were being kept in accordance with Archives Act requirements;
- the varying adequacy of methods used by agencies – participating in a major audit of recordkeeping – to capture and manage electronic records;
- the existence of control weaknesses over the management of user access, maintenance of audit trails, monitoring and review of privileged users and in some cases the segregation of duties in important information technology systems; and
- limited agency use of FedLink, which is a secure encrypted inter-agency communications service.

These issues are discussed under the separate headings of the management of electronic information, and the security of electronic information.

Management of Electronic Information

Two recent ANAO audits relating to information management activities across government are *Recordkeeping*[16] and *Management of the Provision of Information to Job Seekers*[17], both tabled in 2001-02. Information management relates to the processes of creating, collecting, accessing, modifying, storing, deleting and archiving information resulting from an agency's business.

Recordkeeping

This ANAO audit was undertaken in four Commonwealth agencies to determine if record keeping policies, systems and processes were consistent with the requirements of the Archives Act 1983, relevant government policies, and with accepted standards and principles. The audit was also designed to identify better practices and recommend improvements in both electronic and traditional records.

The ANAO found that for record keeping to be effective, it should be viewed as part of information management. The agencies audited were starting to appreciate the need to develop their record keeping and were at different stages of development. In respect of areas such as records of electronic transactions, the organisations were not able to provide Parliament with an assurance that all significant records were being kept in accordance with Archives Act requirements.

While record keeping controls existed for paper-based files, in practice, they were not applied as effectively as they should have been. Outside of the formal record keeping systems, agencies also had significant core business systems that did not fully meet their record keeping needs. Also, the methods used by the agencies to capture and manage electronic records did not meet record keeping requirements.

The audit report also detailed the record keeping better practices that were observed. The audit report made six recommendations that are relevant to all APS agencies in the assessment of record keeping needs; corporate record keeping policy and infrastructure; and controls over record capture, classification, tracking, disposal, and preservation. The organisations audited agreed with the recommendations.

Information Provision

One of the most important elements of employment services programs administered through the Department of Employment and Workplace Relations (DEWR), and delivered by Centrelink, is the provision of accurate and timely information to job seekers. For this reason, the ANAO conducted an audit of the management and provision of information to jobseekers[18].

The objective of the audit was to examine the administrative effectiveness of DEWR's management of the provision of information to job seekers with the focus on what and how

[16] ANAO Report No. 45 of 2001-2002, *Recordkeeping,* ANAO, Canberra, 2002.
[17] ANAO Report No. 39 of 2001-2002, *Management of the Provision of Information to Jobseekers,* ANAO, Canberra, 2002.
[18] ANAO Report No. 39 of 2001-2002.

the information is provided; and how DEWR can be assured that the information was delivered effectively.

The ANAO concluded that DEWR's management of the provision of employment services information to job seekers was generally effective. The audit highlighted issues relating to the currency of jobs listed on JobSearch, which is the computer-based system that links job seekers to the national vacancy database. The ANAO recommended, and DEWR agreed, to strengthen the monitoring of JobSearch and to remind Job Network members of their contractual responsibilities to maintain the currency of job vacancies on JobSearch.

Security of Electronic Information

In addition to the major review of Internet security described above[19], the ANAO in recent years has conducted several information security reviews within the context of the 2000-01 and 2001-02 financial statement audits and a performance audit, *Information Technology at the Department of Health and Aging*, tabled in 2002-03 and mentioned earlier. Information security deals with the preservation of confidentiality, which is ensuring that information is accessible only to those authorised to have access; integrity, which is safeguarding accuracy and completeness of information and processing methods and the availability of information; and with ensuring that authorised users have access to information and associated assets when required.

Across Government

In 2000-2001, joint financial statement audit and performance audits were conducted in several Commonwealth agencies[20]. The objectives of these audits were to consider whether each agency could rely on its systems[21] to support production of a reliable set of balances for the financial statements; and whether their systems' outputs met quality and service delivery targets. The audits included a review of the information technology environment, including system security and business continuity planning for key systems. The security reviews focused on assuring there was appropriate access control governing the key systems and associated data, and that access was restricted to authorised users. The business continuity plan reviews, which were part of the three audits, focused on the operational, administrative and accommodation requirements in the event of a disruption to essential services.

These audits concluded[22] that overall agency management of systems was satisfactory, and that the systems reviewed had adequate systems security in place and their business continuity frameworks assured continuous service. However, in one agency the financial management system controls could not be fully relied upon due to excessive access to the system, inadequate maintenance of account master data and sensitive transaction codes; and

[19] ANAO Report No. 13 of 2001-2002.
[20] ANAO Report No. 39 of 2000-2001, *Information and Technology in Centrelink*, ANAO, Canberra, 2001; ANAO Report No 44 of 2000-2001, *Information Technology in the Department of Veterans' Affairs*, ANAO, Canberra, 2001; ANAO Report No. 49 of 2000-2001, *Information Technology in the Health Insurance Commission*, ANAO, Canberra, 2001.
[21] The audited systems were DVA's systems supporting the Department's income support and compensation responsibilities; HIC's Medicare payments system, the PBS payments system, the financial accounting system, and the human resources and payroll system; and systems supporting Centrelink's income transfer responsibilities.
[22] ANAO Report No. 44 of 2000-2001; ANAO Report No. 49 of 2000-2001 and ANAO Report No. 39 of 2000-2001.

inadequate change control governing changes to systems. In another agency, the irregular monitoring by management of security software access and of privileged security software user access; inadequate contingency planning for key security software and an over-reliance on key staff for its operations continued to be issues but were being addressed.

Each year, the ANAO reviews the adequacy of agencies' controls structures as part of the ANAO's financial statement audits. The results for 2001-2002 were published in Audit Report No. 67 of 2001-2002, *Control Structures as part of the Audit of Financial Statements of Major Commonwealth Entities for the Year Ending 30 June 2002.* The audit [23] provided a comprehensive coverage of IT issues. It concluded that control deficiencies were identified in a significant number of entities that did not have business resumption plans in place. A business resumption plan ensures the uninterrupted availability of all key business resources required to support essential or critical activities. This plan is usually part of a more broadly based business continuity plan which addresses key issues relating to business resumption and IT disaster recovery planning.

As the use of, and dependency on, ICT for decision making increases, the need for sound resumption planning to ensure the continue availability of information f or critical business processes also increases. Over the last few years, business continuity planning (both business resumption and disaster recovery planning) has moved from a primary focus on disaster recovery and ICT, to being and essential element of an entity's risk management. For this reason, business continuity planning must be a shared responsibility of an entity's entire management team. The report identified a number of entities without a business resumption plan, still in the process of developing one, or where the existing plan was insufficient.

Most entities had IT security policies, plans and procedures in place for the protection of their computer systems and data, and in the majority of entities, security awareness was prevalent and promoted by management. However, for a significant number of entities, control weaknesses were identified over the management of user access, maintenance of audit trails, monitoring and review of privileged users and in some cases the segregation of duties over the financial management information system and the human resource management system. The ANAO identified that there was a need to establish clearly defined IT security responsibilities and regularly undertake reviews of IT system security and activity to ensure compliance with security policies and procedures.

Health

The ANAO audit of information technology in the Department of Health and Ageing[24] included a review of security. For the selected relevant systems, the ANAO assessed segregation of duties, access controls, and authorisations and found these to be effective. An information technology and security policy had been established. The policy, which is an example of good practice, requires a system security plan to be developed and maintained for each system. ANAO concluded that Health effectively managed its IT security and that responsibilities for security were clearly assigned, managed and enforced.

Fedlink

[23] ANAO Report No. 67 of 2001-2002, *Control Structures as part of the Audit of Financial Statements of Major Commonwealth Entities for the Year Ending 30 June 2002,* ANAO, Canberra, 2002.
[24] ANAO Report No. 1 of 2002-2003.

It is important that Commonwealth agencies have access to a secure network to communicate information electronically between them.

The Prime Minister, in his *Investing for Growth* industry statement of 8 December 1997, announced the Government's intention to create a government-wide Intranet (later named FedLink) for secure online communications by the end of 1998. The telecommunications network would facilitate the more timely exchange of information between government agencies, the Parliament and ministerial offices. The Intranet was expected to provide a full multimedia capability to agencies to communicate with and provide secure access to external telecommunications networks. It was the intention of the Government to work with industry to find innovative solutions for the network.

The interdepartmental committee advising the Prime Minister on this initiative considered that the telecommunications network would be used for all electronic intra-government communications. It would allow secure agency access from the Intranet to the Internet, and it would provide public access via the Internet and Intranet to appropriate agency information and transactions. Fedlink was to comprise two elements:

- a high capacity telecommunications infrastructure (phase 1); and
- information technology applications which supported Internet and Intranet communication and transactions in a secure environment (phase 2).

The Office of Government Information Technology (OGIT) was the coordinating agency. OGIT sought the services of the ANAO to provide an opinion on the probity of the methodology and procedures applied in the evaluation process for Phase 1. The ANAO reported the results of this probity audit in Report No. 11 of 1998-99, *OGIT and Fedlink Infrastructure.*[25]

Given the importance of secure communications between government agencies, the Government decided that agency heads should, by March 2001, formally assess their existing external communication security arrangements and ensure that they provide safeguards at least the equivalent of those embodied in the FedLink infrastructure. If they did not, existing networks were to be migrated to FedLink, or to infrastructure providing and equivalent or higher stand, by December 2001. For new networks, this requirement was to apply from July 2001.[26]

In July 2001, the Government announced that a private company had signed an agreement with NOIE to deliver FedLink- a proven technical solution for secure intra-government communication and an enabler for online government. It was announced that the network will ensure security of data transfer up to 'protected' level by sending information between participating users through encrypted tunnels.[27]

---

[25] ANAO Report No. 11 of 1998-99, *OGIT and Fedlink Infrastructure, Office of Government Information Technology, Department of Finance and Administration,* ANAO, Canberra, 1998.
[26] NOIE, National Office for the Information Economy, *Government Online Progress Report, December 2002,NOIE, Canberra, 2000.*
[27] *Government secure network – FedLink – goes live, 18 July 2001,*Media Release, Senator the Hon Richard Alston, Minister for Communications, Information Technology and the Arts, and Senator the Hon Ian Campbell, Parliamentary Secretary to the Minister for Communications, Information Technology and the Arts.

In March 2002, it was announced that the encrypted communications service, FedLink, was now operational with seven Commonwealth agencies fully connected and another eight in the process of completing the formal requirements to implement the system.[28]

The connection status in December 2002 was that 14 Commonwealth agencies were connected. Five of these were departments, and nine were other entities. There are 77 agencies subject to the Financial Management and Accountability (FMA) Act, and 113 bodies subject to the Commonwealth Authorities and Corporations (CAC) Act. Potentially, the great majority of these could benefit from use of Fedlink. The ANAO has not audited the reasons for the limited use by Commonwealth agencies of this secure network. It appears, however, that the potential benefits of a secure means of communicating Commonwealth information electronically have been only partially realized.

The adequacy of the current legislative and guidance framework

Information Management Framework

A matter worthy of review is the consistency of the advice and requirements in policies and procedures.

The Commonwealth public sector information management processes are governed by legislation that includes:

- *Privacy Act 1988;*
- *Electronic Transactions Act 1999;*
- *Commonwealth Evidence Act 1995;*
- *FMA Act 1997;*
- *Archives Act 1983;*
- *Copyright Act 1968;*
- *Freedom of Information Act 1982;*
- *Telecommunication Interception Act; and*
- *Disability Discrimination Act 1992.*

The Commonwealth public sector policy and procedural framework for managing information has been defined by the various stakeholders, and this framework includes the following items:

- Protective Security Manual, Attorney General's Department, Commonwealth of Australia;
- Australian Communications Electronic Security Instruction 33 (ACSI 33), Defence Signals Directorate;
- PKI Gatekeeper accredited products and services;
- Online security Guidelines for Government, National Office for the Information Economy;
- E-Permanence Guidelines, National Archives of Australia;
- Australian Archives Handbook, June 1996;

[28] *New Secure Communications System for Government Agencies, 26 March 2002,* Media Release, Senator the Hon Richard Alston, Minister for Communications, Information Technology and the Arts, Deputy Leader of the Government in the Senate.

- Several Australian standards, such as
    - AS/NZS 7799.2:2000 Information Security Management;
    - AS/NZS 4360:1999 Risk Management,
    - AS 4400:1995 Personal Privacy practices in health care information systems,
    - AS/ISO 15491.1:2002 Records Management – General, and
    - AS/ISO 15491.2:2002 Records Management – Guidelines;
- The World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines.

The above policies and procedures have been developed by a diverse group of professional stakeholders, each using their own professional language and each complying with their own professional standards. The ANAO has not reviewed the consistency of the advice and requirements in the above documents. Notwithstanding, it is likely that the above legislative and guidance framework contains inconsistencies because of the diversity of author organisations and stakeholders.

Concluding Remarks

This section of the submission summarises the major findings of the ANAO's audits earlier mentioned.

The privacy, confidentiality and integrity of the Commonwealth's electronic data

ANAO's audits identified how Centrelink and Health had problems in their approaches to managing the privacy and confidentiality of their data. Following the audits, both agencies were in the process of addressing those problems or had addressed them. Coding errors in clients' claims for benefits or entitlements affected the quality of Centrelink's electronic records, reducing the efficiency of claims processing and increasing administrative costs. Overall, the Australian electoral roll is one of high integrity, and it can be relied on for electoral purposes. ANAO found that in the Department of Health and Ageing, overall at the operational level, systems reviewed were delivering the required business outputs in an effective and controlled manner, and within acceptable error rates.

The management and security of electronic information transmitted by Commonwealth agencies

The ANAO's cross agency review of Internet security in ten Commonwealth agencies concluded that security levels varied significantly from very good to very poor. For the majority of agency websites in the audit, the level of Internet security was insufficient, given the threat environment and vulnerabilities identified within a number of agency sites. The ANAO made confidential recommendations to each of the ten agencies, and general recommendations for all Commonwealth agencies to consider as a means of strengthening Internet security.

The management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks

The ANAO's cross agency review of record keeping concluded that, in areas such as records of electronic transactions, the organisations were not able to provide Parliament with an assurance that all significant records were being kept in accordance with Archives Act records

disposal requirements. Organisations could not be sure they were capturing in their corporate record keeping systems all the electronically-sourced records that they should, both for legislative and management requirements.

ANAO's audit of the provision of information to job seekers highlighted issues relating to the currency of jobs listed on the Department of Employment and Workplace Relations computer system. The Department agreed to remind Job Network members of their contractual responsibilities to maintain the currency of job vacancies in the relevant computer system.

The ANAO's financial statement audits have raised issues associated with information security. Recent audits have concluded that overall agency management of systems was satisfactory, and the systems reviewed had adequate systems security in place, and that business continuity frameworks assured continuous service. Notwithstanding, control weaknesses were identified for a number of entities in the areas of business resumption planning and systems security. In a separate IT audit, ANAO concluded Health had an information technology and security policy that was well established. It concluded further that Health effectively managed its IT security. The exception, as described earlier, was that Health had an incomplete approach to data privacy issues.

Agencies require access to a secure network in order to communicate information electronically between them. The most important encrypted communications service for Commonwealth agencies is FedLink. There has been limited use by Commonwealth agencies of FedLink, which suggests that few agencies are taking advantage of the benefits of such a service.

The adequacy of the current legislative and guidance framework

There is a well developed legislative and procedural framework for the management and integrity of Commonwealth electronic data. The ANAO has not reviewed the consistency of the components of the framework to determine whether it contains any inconsistencies. However, because of the variety of author organisations and stakeholders involved, it is possible that some inconsistencies may have occurred in this framework.

APPENDIX

RECENT ANAO AUDITS AND BETTER PRACTICE GUIDES RELEVANT TO THE JCPAA's REVIEW

This Appendix lists recent ANAO audits most relevant to the Committee's review of the management and integrity of Commonwealth electronic information. The preceding paper draws upon these reports where relevant.

Financial Statement and Controls Audits

Audits of the Financial Statements of Commonwealth Entities for the Period Ended 30 June 2002, Summary of Results. (Publication in progress at the time of writing this submission).

Report No 67 of 2001-2002, *Control Structures as part of the Audit of Financial Statements of Major Commonwealth Entities for the Year Ending 30 June 2002.*

Business Support Process Audits

Report No. 15 of 1997-98, *Internet Security Management.*

Report No. 45 of 2001-2002, *Recordkeeping.*

Performance Audits

Report No. 11 of 1998-99, *OGIT and Fedlink Infrastructure*, Office of Government Information Technology, Department of Finance and Administration.

Report No. 18 of 1999-2000, *Electronic Service Delivery, including Internet Use, by Commonwealth Government Agencies.*

Report No. 8 of 1999-2000, *Managing Data Privacy in Centrelink.*

Report No. 39 of 2000-2001, *Information and Technology in Centrelink.*

Report No. 44 of 2000-2001, *Information Technology in the Department of Veterans' Affairs.*

Report No. 49 of 2000-2001, *Information Technology in the Health Insurance Commission.*

Report No. 26 of 2001-2002, *Management of Fraud and Incorrect Payment in Centrelink.*

Report No. 39 of 2001-2002, *Management of the Provision of Information to Job Seekers.*

Report No. 42 of 2001-2002, *Integrity of the Electoral Roll.*

Report No. 13 of 2001-2002, *Internet Security within Commonwealth Government Agencies.*

Report No. 1 of 2002-2003, *Information Technology at the Department of Health and Ageing.*

Report No. 17 of 2002-2003, *Age Pension Entitlements.*

Better Practice Guides

Internet Delivery Decisions. A Commonwealth Program Manager's Guide, 2001.