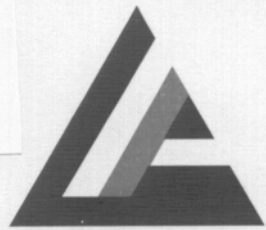




Submission No. 42



**Australian National
Audit Office**

15 May 2003

Mr Tas Luttrell
Principal Research Officer
JCPAA
Parliament House
CANBERRA ACT 2601



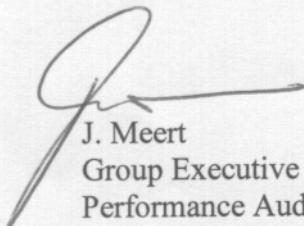
Dear Mr Luttrell

**INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC
INFORMATION IN THE COMMONWEALTH**

Attached is the Australian National Audit Office's response to the questions raised by the Committee following the 31 March 2003 meeting of the JCPAA Hearing into the management and integrity of electronic information in the Commonwealth. Your letters of 29 April 2003 refer.

If you or Senator Lundy require any further information on this matter please do not hesitate to contact Dr Paul Nicoll on telephone number 6203 7759 or myself on telephone number 6203 7360.

Yours sincerely



J. Meert
Group Executive Director
Performance Audit Services Group

ANAO's Response to JCPAA's Requests

Questions on Notice for the Australian National Audit Office

Transcript, 31 March 2003, p.6

1. Three ANAO Audit Reports into IT outsourcing contracts (*Information Technology in the Health Insurance Commission*, No. 49, 2000/2001; *Management of an IT Outsourcing Contract*, No. 46, 2001/2002; *Health Group IT Outsourcing Tender Process*, No. 14, 2002/2003) revealed difficulties with the prescriptive nature of the outsourcing contracts as a result of their negotiation by a third party. These reports also found that security arrangements were not effectively prescribed in those contracts, leading to a series of issues that you subsequently identified.

- The Committee asked that you confirm that this is the case and recall the ANAO's findings and observations on these subjects?

ANAO's comment on the question

The principal findings of the above audits were different from those stated above. Two of the audits mentioned in the above question, *Information Technology in the Health Insurance Commission*, and *Health Group IT Outsourcing Tender Process* did not consider either the management of IT outsourcing contracts, or the difficulties arising in the management of security resulting from the outsourcing of IT. The third audit, *Management of an IT Outsourcing Contract*, considered the Department of Veterans' Affairs, which negotiated the contract. That is, while the audit made comment on the contractual arrangements for the management of data, a third party did not negotiate the contract.

The risks inherent in IT outsourcing contracts are similar to those inherent in any contract. Of particular interest are: security of data, cost control, control over services, quality assurance of services provided under a contract and ownership of intellectual property.

The ANAO has conducted a number of audits where some of the issues raised by Senator Lundy were considered as part of the audit. The audits are:

Report No.9 of 2000-2001, *Implementation of Whole-of-Government Information Infrastructure consolidation And Outsourcing Initiative. Across-agency.*

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

Report No.46 of 2001-2002, *Management of an Outsourcing Contract. Department of Veterans' Affairs.*

The issues

The security issues that need to be addressed by an agency where a provider supplies IT services are:

- developing security objectives, plans and processes before outsourcing commences, and ensuring that the tender process and resulting contract reflect those objectives, plans and processes;

- including specific clauses in the contract signed with the external service provider to address security and privacy issues, and ensure sub-contractors are aware of and adhere to those clauses; and
- monitoring the service provider during the period of the contract to ensure that security and privacy issues are appropriately addressed.

These issues are addressed here in turn.

Development of security objectives, plans and processes

In our audit of *Implementation of Whole-of-Government Information Technology Infrastructure and Outsourcing Initiative*, the ANAO identified differing approaches between agencies in respect of recommended preparatory steps for the security aspects of outsourcing IT infrastructure. Some agencies, such as the NCA, PM&C and ATO, placed particular emphasis on this aspect of their preparation and planning for participation in the IT Initiative. However, other agencies appeared to have been less active, with scope for improvement in the extent, and timing, of attention to the recommended preparatory steps in the Cluster 3¹ and Group 5² tenders.

In that report the ANAO recommended that, where appropriate in outsourcing IT infrastructure services, agencies develop, in consultation with the Defence Signals Directorate, 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.

The report also noted that, unless agencies of similar requirements have been grouped, the security requirements of one agency can have an effect upon the cost-effective provision of IT services to other agencies within the group. Alternatively, the security environment of one agency can represent a security risk to others in the group. This is particularly the case where the solution proposed by the service provider relies upon consolidation to achieve efficiencies.

Contractual clauses

The principle mechanisms through which an agency is able to control or direct service provider actions in regard to security concerns is through the requirements set out in the IT contract or agreement, and its actions in managing compliance with those requirements. The formalisation of security requirements for inclusion in outsourcing Agreements can, in some cases, represent an improvement over the internal security arrangements previously existing within agencies. For example: the Cluster 3 Agreement sets out a number of requirements for the external accreditation by Commonwealth security agencies of the IT systems and facilities used by the service provider to deliver the services. The service provider was required to obtain accreditation for physical and logical security by the commencement date, and there was an ongoing requirement to ensure the service provider's personnel had the

¹ Cluster 3 comprises the Department of Immigration and Multicultural Affairs (DIMA); the Australian Electoral Commission (AEC); IP Australia; Australian Surveying and Land Information Group (AUSLIG); Australian Government Analytical Laboratories (AGAL); Ionospheric Prediction Services; DOFA for the Electoral Offices System (EOS); and former bureau customers of DOFA, including the National Crime Authority (NCA).

² Group 5 comprises the Department of Industry, Science and Resources (DISR); the Department of Communications, Information Technology and the Arts (DoCITA); the Department of Transport and Regional Services (DoTRS); the Department of the Prime Minister and Cabinet (PM&C); and the Australian Competition and Consumer Commission (ACCC).

appropriate security clearances. At the time of the audit the ANAO found that although a number of these requirements were satisfied, there had been significant delay in the service provider obtaining the required security certification of the Cluster 3 network. The Secure Internet Gateway (SIG) was given an interim accreditation in December 1998, but there continued to be significant delays in progressing full accreditation of the SIG and the Cluster network. As at August 2000, full security certification of the Cluster 3 network had not yet been obtained in line with the contractual requirements.

In our audit of *Implementation of Whole-of-Government Information Technology Infrastructure and Outsourcing Initiative* the ANAO found that contracts with service providers explicitly state that engagement of any proposed sub-contractors must be agreed in writing by the relevant agency, and the sub-contractors must sign a non-disclosure undertaking. Similarly, the ANAO's audit of DVA's *Management of an IT Outsourcing Contract* found the IT outsourcing contract requires the contractor's employees, agents and subcontractors to sign a deed of confidentiality, and to abide by the Commonwealth's IT security legislation and practices. The contractor was prohibited from using equipment to provide IT services to another person or organisation unless the security requirements specified in the contract are met.

Monitoring

In its audit of *Implementation of Whole-of-Government Information Technology Infrastructure and Outsourcing Initiative*, the ANAO noted the Privacy Commissioner's Guidelines in relation to outsourcing contracts provide that monitoring by agencies of a service provider's compliance with privacy requirements should be undertaken on a regular basis. Shortly after the ATO outsourcing Agreement commenced in June 1999, the ATO Internal Audit Branch commenced audits of the service provider's compliance with its privacy requirements, the ATO advised the ANAO in August 2000 that its Internal Audit Branch had completed its reports into *Privacy, Security and Access*, and that '*the actions to address the issues identified are being implemented.*' At the time of the audit Cluster 3 and Group 5 were yet to develop a strategy for monitoring the respective service providers' compliance with their privacy obligations.

In the audit of DVA's *Management of an IT Outsourcing Contract*, DVA advised the ANAO that it was satisfied that the privacy of client data was assured by its contractor's approach to data handling. However, DVA had not reviewed the contractor's processes; and it did not monitor data movements on the IT infrastructure, which would have provided assurance that controls and systems were operating effectively.

The ANAO audit of *Internet Security in Commonwealth Agencies* found some of the contracts for website hosting services examined during the audit, failed to specify expected service levels or lacked clear performance indicators. This contributed to a reduced ability on the part of agency staff to be appraised of the security measures applicable to their website hosting and so to effectively manage the security outcomes for their agency.

For example, under the heading of security, one contract simply stated that the contractor is responsible for the integrity of the data held on the agency's website. While it may be appropriate to identify expected outcomes in a contract, without the support of a service level agreement or clear performance indicators, those managing

the contract are likely to be less well informed about the nature and quality of services delivered. In this example, there was little indication of how website security would be achieved, nor how data integrity would be monitored and reported to the agency. While many agency contract managers appeared to inform themselves of the security arrangements at the commencement of the hosting agreement, primarily in regard to the technical level controls, without regular communication between the parties it is possible that a 'set-and-forget' mentality will be adopted.

In one case an agency had outsourced its IT infrastructure, as part of the Whole-of-Government IT Infrastructure Consolidation and Outsourcing Initiative, while maintaining an arrangement with a different contractor for the provision of a range of network services in support of a major business function. When the agency decided to establish an Internet site, it chose for the network services contractor to sub-contract for web hosting services.

The original contract for network services did not include a provision for Internet connectivity. Consequently the contract contained nothing in the way of service level expectations, minimum standards or performance measures in respect of Internet security. During the audit, agency staff claimed to have little knowledge of the nature of any contract between their network services contractor and the sub-contractor. Agency staff relied totally upon the network services contractor to manage the delivery of appropriate Internet security measures for their website. In such circumstances, it is unclear how the agency IT staff might reliably assure themselves or their Chief Executive Officer that appropriate Internet security measures were being realised.

Summary of ANAO's audit findings

In summary the ANAO found:

- differing approaches between agencies in respect of recommended preparatory steps for the security aspects of outsourcing IT infrastructure. Some agencies placed particular emphasis on this aspect of their preparation and planning for participation in the IT Initiative. However, other agencies appeared to have been less active, with scope for improvement in the extent, and timing, of attention to the recommended preparatory steps;
- in the contracts examined by the ANAO, clauses relating to security and sub-contractors were included. However, the audit of Internet Security found that expected service levels were not specified, and that contracts after lacked clear performance indicators; and
- some agencies have conducted audits of service providers compliance with security and privacy requirements.

In our audit of *Implementation of Whole-of-Government Information Technology Infrastructure and Outsourcing Initiative*, the ANAO commented that the experience of Cluster 3 and Group 5 has also demonstrated that, while there are benefits to the aggregation of IT infrastructure across agencies, there are also potential drawbacks in that multiple agencies now have a stake in the issues that affect the security of that shared infrastructure. This has increased the complexity involved in establishing and managing a secure IT environment, highlighting the need for agencies to adopt a structured, strategic approach to this issue early in the tender process.

ANAO's Response to Additional Questions

Further Questions for the Australian National Audit Office

General

1. The ANAO submission mentions audits concerning privacy and confidentiality, fraud management, data management, internet security, recordkeeping, information provision and security.
 - Which of these are the most critical to the management and integrity of the Commonwealth's electronic information?
 - Are there any other issues, not included in that list, which are important?
 - How receptive are agencies to the issues raised by the ANAO during its audits?

ANAO's Response

The ANAO considers that all the issues mentioned in the question are important and critical to the management and integrity of the Commonwealth's electronic information. However, unless appropriate and strong controls are in place to provide security all the other items cannot be assured.

There are a number of other issues relating to data integrity such as back up and recovery, authentication, ownership, data models, data representation standards, and legal and regulatory requirements. In the interests of brevity the ANAO did not address these issues in its JCPAA submission as they are secondary to the main issues identified above.

During the course of ANAO audits we ensure that agencies are kept fully informed of all issues arising. The issues are then fully explored with the relevant agency, including examination of the likely effects of the agency not addressing the issues, and potential solutions to the issues. The result of this process is that, generally, the agencies are not surprised at the findings and are in agreement with the findings and recommended solutions. In a time of fiscal constraints, agencies correctly adopt a risk management approach to issues raised by the ANAO, balancing risk against the cost of addressing the risk.

Software

2. A recurring theme of reported privacy breaches concerns the accidental release of confidential information. For example, cases where a government officer legitimately releases public information in the form of an electronic file or email, which also contains confidential information that the officer is unaware of. The following cases illustrate the problem:
 - The Office of the Federal Privacy Commissioner reported that in November 2001 the Child Support Agency sent an email that accidentally contained 400 client email addresses.

- An ANAO audit into the Health Group IT Outsourcing Tender Process at the Department of Finance and Administration investigated an incident in July 1999, where an Excel spreadsheet was released to IBM GSA containing information about its tender but which also contained information on other tenders.
- The Committee discovered that some of the submissions sent to this Inquiry contained draft versions that could be accessed with the word processing program's reviewing functionality.
- How can agencies, including the ANAO, prevent the accidental release of confidential information in this way?

ANAO's response

In our audit report *Health Group IT Outsourcing Tender Process*, the ANAO found the release of the disk containing tender information (referred to above in the second example), lacked sound procedures. The ANAO found the agency managing the tender process made no contemporaneous record, prior to providing IBM GSA with the disk, of:

- receiving a request from IBM GSA for an electronic version of the document previously faxed to it;
- the request by an agency officer or a member of the evaluation team for an electronic copy of the document, including the nature of that request;
- a disk containing confidential tenderer information being removed from the secure Evaluation Centre;
- the identity and contents of the document contained on the disk; or
- a disk containing pricing information being provided to a tenderer.

No correspondence was prepared to accompany the disk. There was no examination made of the disk's contents prior to it being handed over to the tenderer. Nor was a hardcopy of the electronic document contained on the disk produced or retained at that time as a record of the information provided.

This error highlights the need for agency officers to examine information and documents before releasing them outside the agency. While mistakes can never be eliminated, sound procedures and appropriate training will reduce the number of mistakes, and eliminate the most obvious and significant mistakes.

In the case of the Committee receiving electronic documents with draft changes visible within the document. The authors should have 'accepted all' in the track changes menu on finalisation of the document. Authors sufficiently expert to use the 'track changes' feature should be aware of the need to 'accept all' changes on finalisation. Conversion of the document to the commonly used Adobe Acrobat (.PDF) format will also ensure the draft changes disappear. A full version of Microsoft Word is necessary that allows document saving in Acrobat format.

However, as Adobe Acrobat has less features than Microsoft Word, some formatting may be lost.

In summary, mistakes will occur, whether by simple error, lack of understanding of the technology, or by poor work practices. The latter two can be addressed by appropriate training.

Social Engineering

3. Social engineering is the use of deception, influence and persuasion to overcome security measures.

- How aware are agencies of this potential threat?
- What action is the ANAO taking to in relation to this issue?

ANAO's response

The ANAO does not include Social Engineering tests as part of its security test program for agencies. The ANAO considers attempting such tests as likely to undermine our relations with the audited agency, and the staff of the agency. This is a view also held by many agencies, although some do use consultants to conduct such tests. In the ANAO audit *Management of e-Business in the Department of Education Science and Training, Report No.33 2002-03*, the ANAO noted DEST limits penetration tests to 'standard tests' against the firewall from a remote location. 'Social engineering', for example, 'tricking' DEST staff into providing their user-id and password to external false bodies, is not attempted by DEST. DEST advised the ANAO that it had decided against conducting such tests.

It is important to understand the context in which tests of security are undertaken to ensure against a false sense of security. Remote 'hacking', while important to guard against, is only one of a number of security risks.

The ANAO has addressed the security risks in our Security Policies document, last revised in October 2002. Prior to being granted access to any ANAO IT system, users are required to sign an undertaking that advises them of their responsibilities. IT security training is incorporated into ANAO's induction processes. Social Engineering tests are not conducted by the ANAO on its own staff.

Disaster Recovery

4. A potential threat to the integrity of the Commonwealth's electronic data is the physical disruption caused by an earthquake or fire.

- How suitable are agencies' disaster recovery plans?
- How confident are you that data stored by the ANAO would survive a disaster such as a fire?

ANAO's response

The ANAO is currently addressing the issues of Business Continuity Management and Disaster Recovery for agencies in general in our report *Control Structures as Part of the Audits of Financial Statements of Major Commonwealth Agencies for the Period Ending 30 June 2003* due to be tabled in July 2003. We are conducting an in-depth audit of Business Continuity Management at Centrelink due to be tabled in August 2003. The ANAO will be pleased to provide Senator Lundy with a briefing on the contents of the reports at the time of tabling. The ANAO's contact for the controls report is David Crossley, Executive Director, Assurance Audit Services Group, contact phone number 6203 7663, and for the Centrelink report, Fran Holbert, Acting Executive Director, Performance Audit Services Group, contact phone number 6203 7691.

The ANAO's Disaster Recovery Plan (DRP) was reviewed in February 2002 and incorporated into an updated Business Continuity Plan (BCP). External consultants tested the BCP, including the DRP, in December 2002, gaps were identified and recommendations accepted. A further review by the ANAO's Internal Auditor confirmed the DRP as being an appropriate response to minimise the threat to the Commonwealth's electronic data held by the ANAO.

The ANAO's DRP was developed in collaboration with our outsource service provider, Unisys. The plan provides for critical data stored on personal computers to be copied to servers when PCs are connected to or closed down on the ANAO's office network. The servers holding this data, other ANAO data, and ANAO databases are backed up daily. The back-up tapes are taken offsite daily to secure storage remote from the ANAO. Our arrangement with Unisys provides that, in the event of a loss of facilities at the ANAO, for example, by way of destruction of the ANAO's premises, Unisys will provide facilities at their premises for restoration of the data. Therefore, in the event of a destruction of the ANAO's premises, the ANAO may potentially lose up to one day's data. The ANAO has considered the risk inherent in this potential loss, and the criticality of the data held by the ANAO, and considers the loss an acceptable risk.

Archival Integrity

5. Another potential threat is the gradual degradation of data over time, for example due to changes in the software used to store and access the data.

- Is this issue being addressed by government agencies generally?
- What action is the ANAO taking to ensure the long-term archival integrity of the Commonwealth data that it holds?

ANAO's response

In our audit *Recordkeeping Report No. 45 2001-02*, the ANAO concluded that the four audited organisations were at different stages of development of their corporate recordkeeping. Most of the audited organisations had just started systematically to assess their recordkeeping needs across their organisations and their various functions. All were starting to appreciate the need to develop their recordkeeping and,

increasingly, the potential for this to be part of business process re-engineering and of a strategy for improved information management more broadly. None of the organisations reviewed in the audit fully satisfied the criteria under the recordkeeping model applied on the audit. Each organisation had several recordkeeping environments that met the criteria to varying degrees.

The ANAO is currently conducting a further audit of recordkeeping that is due to be tabled in July 2003. The ANAO will be pleased to provide Senator Lundy with a briefing on the contents of the report at the time of tabling. The ANAO contact for this report is John Hawley, Executive Director, Assurance Audit Services Group, phone number 6203 7464.

The issue of access to data over the longer term extends beyond just the simple changes to software. It also includes changes to hardware – that is, equipment provided by manufacturers no longer made, and perhaps where the manufacturer is no longer in existence. There is no simple solution to this problem. We are aware that there are organisations in the USA that specialise in the retention of outdated equipment and software specifically to assist organisations to address this difficulty.

The National Archives of Australia has an 'e-permanence' project dealing with the preservation of electronic records and has produced a Green Paper: *An Approach to the Preservation of Digital Records* (available http://www.naa.gov.au/recordkeeping/er/digital_preservation/Green_Paper.pdf). The e-permanence project requires that agencies hold their own archived electronic records (paper records can be archived by the NAA), and update those records so they can be read by the agencies' current technology.

The ANAO's administrative records are paper-based and archived using normal archival processes for paper-based records. The ANAO will be considering adopting the guidelines on 'e-permanence' provided by the NAA.

ANAO Better Practice Guide

6. The ANAO has produced a Better Practice Guide on Internet Delivery Decisions.
 - Does the ANAO intend to produce Better Practice Guides for any other aspects of electronic data management?
 - How often do you intend to review your Better Practice Guides?

ANAO response

The ANAO has no current plans for any Better Practice Guide on any aspect of electronic data management, in addition to the current BPG, "Internet Delivery Decisions".

The development and publication of Better Practice Guides (BPGs) is a relatively recent inclusion in the ANAO program of work. The first BPGs were published by the ANAO in 1996. The inclusion of BPGs in the work program is part of the ANAO strategic planning process. The Auditor-General determines the work program and advises the JCPAA on an annual basis.

Current practice is that some guides are produced on an annual basis, for example, the Amodel accounts guides. Generally, the development of guides follows a series of audits on a particular topic, and where the ANAO considers other guidance is lacking. The ANAO also uses the guides as a basis for conducting future audits.

The core business of the ANAO is audit. While we are pleased to assist agencies by producing BPGs, the effort and expense of producing the guides is at the cost of a reduction in the number of audits undertaken by the ANAO. Therefore, decisions on each BPG, or a review of existing BPGs, are considered individually in the context of the overall ANAO audit program.