3

Management of Outsourcing Contracts

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

(i) complementing modern management practices;

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

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

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

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

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

---

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

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

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

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

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

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

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

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

---

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

Accountability Remains with Agency

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

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

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

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

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

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

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

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

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

---

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

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

When is Outsourcing Appropriate

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

Addressing Security Issues in Outsourcing Contracts

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

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

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

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

---

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

21 Mr Merchant, *Transcript*, 17 October 2003, p. 394.

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

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

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

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

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

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

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

---

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

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

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

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

Addressing Privacy Issues in Outsourcing Contracts

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

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

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

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

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

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

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

---

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

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

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

Committee Comment

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

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

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

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

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