CHAPTER SEVEN

CONTRACT PROVISIONS

> Drafting appropriate and effective contract specifications is considered to be the key element from which all other contracting responsibilities are tied. Some groups have stressed that the quality of contract specifications governs the success or otherwise of the contract objectives.
>
> Joint Committee of Public Accounts and Audit (JCPAA)
> *Contract Management in the Australian Public Service*[1]

7.1 Contractual arrangements are intended to provide an effective operational framework within which risks can be managed. They are intended to minimise the opportunities for poor performance or even serious wrongdoing by the vendor as well as promote best practice. During the course of this inquiry concerns were put to the Committee about particular issues and whether the contract provided adequate protection against any shortcomings or failures by the vendor.

7.2 This chapter looks at the contract provisions covering a number of key areas. Firstly, it examines the use of incentives and sanctions to maintain and improve performance against agreed service levels. It then looks at several areas in which there is uncertainty as to whether contractual arrangements with private companies are able to provide an appropriate level of service and security. All such issues discussed—privacy, data security and intellectual property—involve, in some way or other, the protection and management of information. Finally, the chapter considers the adequacy of contract succession arrangements.

Incentives and sanctions

7.3 Referring to questionable practices that have arisen in an outsourced environment, Professor Haque argued that information technology (IT) outsourcing may create the potential for wrongdoing by the vendor. He warned that without a close watchdog there could be serious abuse of public funds.[2] He suggested that in many instances of outsourcing, it is observed that a private vendor or contractor may under-perform but claim full payment. Professor Haque cited other examples of where a vendor can fall short in meeting the expectations:

> The vendors may deviate from original agreements, revise the terms of agreements in their own favour, ask for unnecessary contract extensions,

---

1 Joint Committee of Public Accounts and Audit (JCPAA), *Contract Management in the Australian Public Service*, October 2000, p. 57.

2 Professor M. Shamsul Haque, submission no. 29.

> and so on. These certainly represent a challenge to the proper use of public sector resources.[3]

7.4 Contracts are supposed to protect agencies, through incentives and sanctions, from such wrongdoing by the contractor. The ultimate penalty is termination of the contract. Contracts developed under the Initiative can be terminated if the contractor breaches conflict of interest, data security, confidentiality, privacy or intellectual property rights clauses.

7.5 According to the Office of Asset Sales and Information Technology Outsourcing's (OASITO's) Mr Hutchinson, the IT outsourcing contracts contain a graduated range of sanctions from directing the contractor to do the task again or to do it correctly—the notice of provisions—through to claiming of service credits. A service credit is 'conceptually, a deduction off the next bill' because of a deficiency in the service provided. He explained that the 'sanctions then range right through to termination of contract for cause with the contractor bearing the cost of putting in place a replacement contractor. There is a graduated range of provisions that are … spelt out in the RFT [request for tender]'.[4]

7.6 Although service penalties may be applied, this should occur in a constructive way, with the resolution of the problem foremost in mind. Ms Kava of the Department of Transport and Regional Services (DTRS) told the Committee:

> While we have applied service penalties, we do work actively with them [the provider] on a very regular basis to try [to] foster sensible and reasonable approaches to resolve problems. We are very keen that we see them as a business partner and that they get involved in active decision making about systems and processes and ideas about where we ought to go in the future…there is more to it than black letter type interpretation … the relationship is critical.[5]

7.7 Mr Simpson, also of DTRS, said that the value of service credits imposed to date by the department represented almost 9 per cent of its service charges. The credits had been imposed largely due to network availability service levels with the remainder made up by help desk related issues.[6] Ms Key (DTRS) explained further:

> There are five individual service levels that we look at every month before we determine the application of a service penalty. Each of those has a particular performance attached to it. From figures supplied we can assess whether or not they are meeting those standards. Some months they will do well on LAN availability, for example, and some months not so well…we

---

3 Professor M. Shamsul Haque, submission no. 29.

4 Finance and Public Administration Legislation Committee, *Hansard*, 4 June 1998, p. 420.

5 Committee, *Hansard*, 9 March 2001, p. 190.

6 ibid.

> had initial problems with help desk, for example, and now it is doing very well.[7]

7.8 Mr Comer of the Civil Aviation and Safety Authority (CASA), who admitted that problems with outsourcing had been experienced, explained that the terms of the contract provide for remedies for service level credits that can be exercised within a 12 month period. He noted that CASA had put Ipex on notice of the application of a service delivery credit for one of the months of that period but had not applied it as yet.[8]

7.9 In addition to the service credits already provided for in contracts, Customs, which outsourced its IT prior to the Initiative, suggested to the Committee that there should be incentives for early delivery of a quality product. This reflects the conclusions of the 1996 Industry Commission report which stated that 'In the end, it is the blend of contractual incentives and penalties which holds the key to encouraging good performance.'[9]

7.10 Customs also believed that there should be penalties for late delivery and for products that do not meet agreed performance requirements. They were concerned to enforce clarity in billing, stating:

> the contract should provide for financial disincentives for billing errors or omissions and late payment. Mechanisms for quick resolution of major differences of view on billing—including service delivery penalties—need to be included in the contract.[10]

7.11 There may be difficulties when it comes to applying the service credit arrangement outlined in the contract. The Australian National Audit Office (ANAO) report on the Initiative outlines the following complexities of imposing service credits that were experienced by Cluster 3:

- The cluster provided the contractor with a three month grace period during which it was not liable to pay service credits. The ANAO argued that if such a period is to be allowed, it needs to be more formally documented.
- Subsequent to service credits being imposed by Cluster 3, service credit levels accrued by the cluster were reviewed and reduced. A revised service credit regime and a lower minimum level of service was introduced. The ANAO considered that such reviews and changes should be more adequately documented, particularly in terms of the value for money analysis undertaken by agencies.

---

7 ibid., p. 180.

8 ibid., p. 194.

9 Industry Commission, *Competitive Tendering and Contracting by Public Sector Agencies*, January 1996, p. 332.

10 Australian Customs Service (Customs), submission no. 21.

7.12 The ANAO suggested that the early development of a strategy to consider potential trade-offs involving available service credits could help agencies protect the Commonwealth's interests when negotiating with contractors about non-performance.[11]

7.13 The Committee endorses ANAO's recommendation 13 that 'in managing IT outsourcing agreements, relevant agencies develop procedures for the conduct and documentation of the processes followed in evaluating options for the use of contractually-available service credits to facilitate effective delivery by the external service provider of contracted services'.[12]

Privacy

7.14 Many of the agencies undergoing IT outsourcing hold databases of personal information about individuals that must remain undisclosed. Concern has been expressed to the Committee by a number of agencies that personal information held by the private sector under IT outsourcing arrangements is not as protected from misuse as it would be if held by an agency. Additionally, there is concern that if such information were misused there would not be adequate means of complaint and remedy.

7.15 All contracts under the Initiative contain provisions relating to privacy that operate in the context of privacy legislation. The current legislation regarding the holding of personal information is the *Privacy Act 1988,* which applies to Commonwealth and ACT government employees or other persons directly in the service of the agency concerned. From December 2001, new legislation will pertain to the handling of personal information by the private sector.

Current legislative arrangements

7.16 The Privacy Act provides privacy safeguards which Commonwealth and ACT government agencies must observe when dealing with personal information. The Act sets down detailed Information Privacy Principles (IPPs) which cover:

- methods used to collect personal information;
- storage and security of personal information;
- notice of existence of record systems;
- access by individuals to their own records;
- accuracy and completeness of personal information; and

11 Australian National Audit Office (ANAO), *Implementation of Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative*, Audit Report No. 9 2000-2001, pp. 210-224.

12 ibid., p. 33.

- use of personal information and disclosure to third parties.

7.17 Adherence to the IPPs is overseen by the Office of the Federal Privacy Commissioner (OFPC). The OFPC investigates agency actions that might breach an IPP, as well as conducting audits of personal information kept by Commonwealth agencies to ensure that personal information is handled in accordance with the IPPs. The Attorney-General is informed of any action that, in the Privacy Commissioner's opinion, needs to be taken by an agency in order to achieve compliance with the IPPs.

7.18 Obligations under the Privacy Act, as it now stands, do not extend to independent contractors engaged by an agency. By means of contractual clauses personal information in the hands of contractors can be given 'a measure of indirect protection', however, the contracted clauses do not fully replicate measures that apply in relation to an agency.[13]

7.19 In particular, the path of complaint and remedy is complex and indirect for a complainant whose personal information has been misused by a contractor or employee of a contractor. If a contractor is alleged to have mishandled personal information, the only action the Privacy Commissioner can take is to investigate whether the agency has done everything 'reasonably within its power' to protect the information (IPP 4(b)). The Privacy Commissioner cannot investigate the contractor's actions directly.

7.20 Liability for any compensation ordered under the Privacy Act to an individual whose personal information has been mishandled by a contractor remains with the agency. The agency may then seek to recover from the contractor any compensation it has been obliged to pay. The contractor can subsequently take action against the employee who is found responsible for the improper handling. In his submission to the inquiry, the Privacy Commissioner described the current complaints handling mechanism as 'less than optimal'. He stated:

> The accountability chain between the data subject and the errant employee is long; while the data subject may be compensated for disadvantage suffered, it is less likely that the burden of that compensation will fall on the person responsible for the disadvantage. [14]

Privacy and the IT outsourcing initiative

7.21 In 1994 the OFPC issued a paper, *Outsourcing and Privacy*, that contained model privacy clauses for inclusion in contracts for IT and other services. The Privacy Commissioner has stated that contract provisions in existing IT contracts are in line with the recommended approach in the *Outsourcing and Privacy* guide.[15]

---

13 Federal Privacy Commissioner, submission no. 19.

14 ibid.

15 ibid.

7.22 All contracts under the Initiative contain privacy clauses referring to the Privacy Act. Most significantly, such clauses state that the contractor and subcontractors must comply with the Act as though they were included in the definition of an agency. If appropriate, the clause also states that the contractor must comply with all other legislation administered by the agency. The contract can be terminated by the agency if privacy clauses are breached.

7.23 Specific contractual obligations regarding privacy generally stipulate that the contractor:

- must only use personal information held in connection with this Services Agreement for the purposes of fulfilling its obligations under this Services Agreement;
- not disclose personal information to any third party without the agency delegate's prior written consent;
- comply with any relevant directions or determinations made by the Privacy Commissioner; and
- ensure that contract personnel and the subcontractors comply with the privacy clauses and sign a deed of undertaking relating to personal and confidential information.

7.24 According to the OFPC, OASITO regularly consulted the Office about appropriate privacy provisions for inclusion in RFTs and service agreements.[16] The OFPC had a threefold approach to ensuring that the arrangements regarding privacy under the Initiative were adequate—continuing consultation; examining the contracts to see if advice was implemented; and checking to ensure that the contracts were being abided by.[17]

7.25 The OFPC says it has received no complaints about, or reports of, privacy breaches associated with the Initiative.[18]

7.26 The ANAO report also briefly examined how privacy was being addressed in agency contracts. It found that the contracts 'largely' reflect the model clauses set out in the Privacy Commissioner's guidelines. The report did raise the following concerns about the privacy clauses contained in contracts:

- The standards required by privacy clauses may be higher than that of confidentiality clauses. It is therefore important that privacy and confidentiality clauses are adequately differentiated and clearly related to each other. This was

16 ibid.

17 Committee*, Hansard*, 21 May 2001, p. 602.

18 Federal Privacy Commissioner, submission no. 19.

not clear in the Australian Taxation Office (ATO), Cluster 3 and Group 5 contracts.

- The guidelines recommend that the contracts clearly state that disclosure of personal information is an offence under the *Crimes Act 1914* and other relevant Acts and that this clause is reproduced in a deed of privacy to be signed by the contract's employees. While this clause has been incorporated into the deed of confidentiality it is not contained in the body of the contract. The ANAO recommended that it is contained in the body of the contract.
- While the contracts provide for the auditing and inspection of compliance with privacy obligations, Group 5 and Cluster 3 were yet to undertake audits or develop a strategy for monitoring that compliance. The ANAO recommended that such a strategy for monitoring compliance should be developed.[19]

Privacy Amendment (Private Sector) Act 2000

7.27 When this Act commences on 21 December 2001, it will establish a 'co-regulatory scheme' that includes:

- a legislative framework for the handling of personal information by private sector organisations; and
- provision for organisations or industry sectors to develop privacy codes that can operate in place of the legislative framework and be tailored to their own industry needs (the Privacy Commissioner is required to approve such codes and may review their operation).

7.28 The new legislation establishes National Privacy Principles (NPPs) as the minimum privacy standards for the private sector. These are similar, but not identical, to the IPPs that apply to government agencies.

7.29 The application of privacy principles to government contractors is specifically addressed by the legislation. It provides that the principles that will apply to a government contractor will be the same as those that apply to the outsourcing agency—the IPPs.

7.30 The legislation enables a contract between a Commonwealth agency and the contractor to be the primary source of a contracted service provider's obligations with respect to the personal information collected or held for the purposes of performing the contract. The Act requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider does not breach an IPP. These provisions also apply to subcontractors.

7.31 The NPPs and industry codes may still apply to government contractors. If a clause in a Commonwealth contract is consistent with an NPP or there is no

19 ANAO, *Implementation of Whole-of Government IT Infrastructure Consolidation and Outsourcing Initiative*, Audit Report No. 9 2000-2001, pp. 232-5.

corresponding clause in the contract then the NPP will apply to the provider. However, where there is inconsistency between the terms of the contract and the NPPs, the terms of the contract that uphold the IPPs take precedence.

7.32 Contractors are explicitly prohibited from using or disclosing personal information collected under a Commonwealth contract for direct marketing purposes, unless it is explicitly allowed by the contract. They must also release on request details of privacy clauses in their contracts.

7.33 Importantly, the Act also brings complaints against Commonwealth contractors within the Privacy Commissioner's complaint handling function. An individual will be able to bring their complaint about a contractor directly to the Commissioner, who will have the same powers to investigate complaints against contractors as against Commonwealth agencies. Accordingly, the amendments shift liability for privacy breaches from the Commonwealth agency to the contractor where appropriate.

7.34 The amendments to the Privacy Act will have an impact on the private sector and some adjustments will have to be made to current practice regarding privacy safeguards. Mr Bell, CEO of Computer Sciences Corporation (CSC), told the Committee that CSC was preparing for the necessary changes:

> We have a task force that reports to our board at the moment, and it is assessing what the legislation will say, where we will have to make changes and what additional safeguards we will have to put in place…We will no doubt have to make some changes internally in the way we handle some information, and we will go ahead and do that. We do anticipate some changes. We do not think that they will be dramatic.[20]

7.35 The amendments to the *Privacy Act 1988* update the Act so that it better ensures adequate privacy safeguards in the private sector, and thus in an outsourced environment. The amendments reinforce the binding nature of the privacy obligations of an external service provider (ESP) contained in a contract and will support the past privacy provisions contained in contracts already signed.

7.36 To the Committee's and the Federal Privacy Commissioner's knowledge there has not been any significant breaches of privacy under the IT outsourcing initiative. The close consultation between OASITO and the OFPC when developing contract clauses has no doubt contributed to this absence of difficulties so far in the Initiative. In a devolved environment such consultation between agencies and OFPC should continue, both when establishing future outsourcing arrangements and in monitoring and evaluating current ones.

---

20 Committee, *Hansard*, 6 August 2001, p. 667.

Data security

7.37 In accordance with the *Protective Security Manual*, Section 6.3, Commonwealth agencies are required to protect all Commonwealth information from unauthorised access, disclosure, modification, manipulation or destruction.[21] The contractor bears this obligation when IT infrastructure is outsourced. Concern has been raised at the possibility that data held by the Commonwealth might be less secure if an ESP holds it for the Commonwealth.

7.38 In 1997 the Defence Signals Directorate (DSD), the Attorney General's Department and the Office of Government Information Technology (OGIT) released the *IT Infrastructure Security Framework for Outsourcing* (the DSD framework). The framework aimed to help agencies maintain their data security in an outsourced environment and identified tasks that must be conducted by agencies if they are to maintain adequate security under IT outsourcing arrangements. The DSD framework emphasised the need for each agency to have information security objectives, plans and processes in place before approaching outsourcing.

Data security clauses in contracts

7.39 All contracts contain data security clauses that generally refer to:

- ownership and use of the group data;
- provisions for safeguarding the data;
- security policies and planning;
- access requirements;
- an acknowledgment that the group holds highly sensitive information that must not be used improperly;
- a deed of confidentiality;
- the compliance schedule which contains information on procedures, including auditing and action on audit results; and
- breaches of data security clauses resulting in the termination of contracts.

7.40 The exception to the above list is the Cluster 3 contract. It does not contain a reference to policy and planning or an acknowledgment of the sensitivity of the material involved.

ANAO Report No. 9 2000-2001

7.41 The ANAO audit report on the Initiative examined the provisions and procedures to maintain data security under outsourcing, as well as compliance with

21 *Protective Security Manual*, 1991, Section 6.3, p. 131.

these provisions and procedures.[22] It looked at the completed contracts for Cluster 3, the ATO and Group 5.

7.42 The report found that the clustering of agencies with differing levels of data security requirements has considerable implications for the cost effectiveness of providing IT services to agencies in a group. Disparities in security requirements mean that different data security provisions and procedures may need to be implemented, making consolidation risky and inappropriate. In particular, it may not be cost effective to outsource in high security risk circumstances.

7.43 According to ANAO, there were differences between agencies in their approach to preparing for data security arrangements under IT outsourcing. Cluster 3 and Group 5 were less proactive than other agencies and there was scope for improving their preparation and planning.

7.44 The Cluster 3 contract required accreditation by DSD of the systems and facilities used to develop services. Full certification had not been obtained at the time the ANAO audit was completed in August 2000, although certification subsequently occurred during the following month. The contract has been in place since 1998. ANAO suggested that a likely reason for the delay was an inadequate appreciation of the resource commitment required to obtain the level of DSD sign-off being sought, as well as a lack of initial preparation.

7.45 ANAO noted that security accreditation by an external security agency is not appropriate for all groups. For instance, the ATO and Group 5 contracts set out security obligations that do not require accreditation. Certification can still be sought if required, although it is not clear who is responsible for the costs of gaining accreditation when this occurs.

7.46 According to ANAO, a formal analysis to determine the security requirements to be included in a contract, and whether it warrants accreditation by an external security agency, should be undertaken. The evaluation should look at a full range of risks, costs, and benefits of outsourcing for security arrangements.

7.47 ANAO also suggested that security arrangements and processes under outsourcing could be improved if tenderers were required to demonstrate an understanding of the security implications of their proposed solution. The Committee supports ANAO's proposal that if an independent security review is required, then it would be useful to include a form of service level for the management of security standards in the contract to encourage the contractor to be committed to completing the review.

7.48 DSD advised ANAO that agencies should prepare an 'Enterprise Security Architecture' document laying out agencies' operational security issues, necessary

---

22 ANAO, *Implementation of Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative,* Audit Report No. 9 2000-2001, pp. 224-232.

safeguards and a security plan showing how safeguards would be implemented. The Committee supports ANAO's recommendation 18, and noted the Government's agreement, 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.'[23]

Concerns surrounding data security under IT outsourcing

7.49 The possibility that a multinational ESP may hold Commonwealth data offshore is a sensitive one. Mr Broome, former head of the National Crime Authority (NCA), explained that the powers of the Commonwealth to renegotiate contracts and to maintain power over data are greatly reduced if that data is held overseas. He said if 'material is held in another country there must be concerns about the degree of security that could be afforded to that information'.[24] The contractual clauses concerning data security, privacy or intellectual property do not refer to the possibility that data may not be held offshore.

7.50 Customs told the Committee that mechanisms need to be put in place:

> to quickly resolve any security situation which can affect data holdings, relationships with clients and other service providers. It requires appropriate security vetting and an ability to deal quickly with requests for rapid security clearance of staff who are non-Australian nationals…There can be sensitive security issues to be resolved if off-shore applications development is contemplated. [25]

7.51 Science agencies, yet to be outsourced, expressed concern that IT outsourcing will increase the security risk for data they hold. For example, the Australian Nuclear Scientific and Technology Organisation (ANSTO) Combined Unions wrote:

> The nature of the intellectual property held by the Science Agencies is very different to the personal information held by many other government departments. Buried in the enormous amounts of data held by the Science Agencies are embryonic ideas, or pointers to embryonic ideas, that could be of enormous financial gain and which are not yet protected by any patent…The use of confidentiality agreements similar to those used in departments such as Taxation are not necessarily appropriate to the Science Agencies, yet they were considered adequate by OASITO. The increased risk following loss of a discovery or breakthrough because of outsourcing is

23 ibid.

24 Committee, *Hansard,* 17 May, 2001, p. 406.

25 Customs, submission no. 21.

> not adequately balanced against potential savings when considered in the evaluation process.[26]

7.52 That some agencies have high data security needs has implications for the implementation of IT outsourcing. These implications extend beyond the possibly greater cost of outsourcing agencies with such needs. The high security needs of agencies also have to be genuinely factored into any evaluation of the benefits and disadvantages of outsourcing and, if outsourcing is proceeded with, comprehensively addressed by the contracting process.

7.53 In the case of the NCA, the Committee was told that OASITO adopted a dismissive approach to their concerns about data security which were not seriously considered in deciding to outsource NCA's IT. Further, Mr Broome alleged that this disregard occurred because OASITO believed that if an agency with high security requirements was outsourced then other agencies' concerns about data security under outsourcing would be assuaged. He suggested that this was most likely the main motivation for including the NCA in Cluster 3, as its inclusion would not contribute to cost savings.[27]

7.54 The NCA eventually enlisted the aid of the Attorney-General to support their concerns about data security. The Auditor-General subsequently wrote to the Minister for Finance and attended meetings with OASITO and the NCA.[28]

7.55 The Australian Federal Police (AFP) also submitted that their central concern about the Initiative related to security. They had three major concerns.

- The AFP has large holdings from overseas law enforcement agencies often provided on the condition that it is not disclosed to other entities. Interpol has expressed a clear preference that the IT systems of member agencies, of which the AFP is one, are not outsourced. Information from national security agencies such as the Australian Security Intelligence Organisation and sections of the Department of Defence is also held.
- A large proportion of AFP investigations involve sensitive references, such as leak inquiries, political matters and national security issues, and a high level of protection is required.
- Information gathered via the AFP's telecommunications interception and surveillance product is very sensitive, not only because of its invasive nature, but also because the investigations it supports often relate to criminal networks or have national security implications.[29]

---

26 Australian Nuclear Science and Technology Organisation (ANSTO) Combined Unions, submission no. 12.

27 Committee, *Hansard*, 17 May, 2001, p. 404.

28 ibid., p. 405.

29 Australian Federal Police (AFP), submission no. 20.

7.56 The AFP's submission noted that the Government's intelligence and security agencies were exempted from IT outsourcing for national security reasons. The issues outlined above in relation to the AFP carry a similar level of risk to the Government's interests to that of the exempted agencies.

7.57 It its submission to the Humphry Review, the Federal Court expressed concerns about the security of judgements prior to their announcement. Judgements are held electronically and premature disclosure of such information has serious implications.[30]

7.58 Both the AFP and the Federal Court are part of the Group 10 cluster. The Humphry Review recommended that outsourcing should not proceed for this cluster until the agency heads are satisfied that all implementation risks are addressed (recommendation 10).[31] Data security is a significant implementation risk that needs to be thoroughly addressed.

7.59 For agencies that have undergone outsourcing to date, the evidence suggests that there have been no significant difficulties surrounding the maintenance of data security under the Initiative. In fact, outsourcing appears to have made agencies more likely to formalise security arrangements and procedures, in particular agencies with lower security requirements. This can be considered as an improvement on past procedures and practices. As Dr Willcocks told the Committee:

> Working in the field, a number of outsourcing suppliers make the point that, quite often, data is more secure now because they are more security conscious than the previous regime could have been.[32]

7.60 Nonetheless, the steps identified by the ANAO to improve the transition to outsourcing and ensure that security requirements and procedures are followed should be implemented.

Recommendation No. 14

For agencies with distinctive data security needs, such as the science agencies, and agencies with high security needs, for example the AFP, a credible argument has been put forward that IT outsourcing is far more complex. The Committee endorses recommendation 10 of the Humphry Review and recommends it be extended to apply to the evaluation of the implementation risks of all other agencies.

---

30 Federal Court, submission to the Humphry Review.

31 Richard Humphry, *Review of the Whole of Government Information Technology Outsourcing Initiative*, Commonwealth of Australia, December 2001, p.18.

32 Committee, *Hansard*, 17 May, 2001, pp. 510-511.

Intellectual Property

7.61 The management of intellectual property under IT outsourcing touches on a number of aspects of implementation of the Initiative. It is related to, for example, workforce planning, commercial-in-confidence claims, privacy and the estimation of savings. This section will largely focus on the contractual provisions relating to the protection of Commonwealth intellectual property. As Professor Haque advised the Committee:

> Without strict measure of property right or copyright, a contractor can make use of the software program or expertise developed through public sector contracts, and transfer it to some private firms for more profits.[33]

7.62 In the Committee's view, agencies should ensure that the Commonwealth benefits from any such profits. Intellectual property in IT outsourcing is concerned with computer hardware, software, 'knowhow' and data. The intellectual property of computer hardware and software includes the IT solutions and innovations that an agency has delivered. 'Knowhow' lies in the accumulated expertise of staff that is created and gained in developing and delivering government policies and programs. Intellectual property is a valuable resource that needs to be carefully managed through workforce planning. Government data is the information that is stored using IT. It is covered by copyright and, in some circumstances, the sale of data is recognised as a legitimate means by which to raise revenue. Other data sources are protected under legislation by the *Privacy Act 1988*.

7.63 Factors to consider when managing IT intellectual property include:

- generation of royalties to the government;
- the protection of the value of government assets;
- provision of goods or services directly to the public;
- purchasing goods and services from the private sector;
- stimulating industry development; and
- cost effectiveness.[34]

7.64 It has been suggested that government outsourcing could be used to stimulate industry development by allowing the commercialisation of intellectual property. For example, *The Goldsworthy Report* (1997) and the *Information Policy Advisory Council (IPAC) Report* (1997) both suggested that management of Commonwealth IT

---

33 Professor M. Shamsul Haque, submission number 29.

34 Mr A. Tegart, *Approaches to the Commercialisation of Government Intellectual Property*, Centre for International Research on Communication and Information Technologies, Research Report no. 26, 2000, pp. 24-25.

intellectual property could be used to promote industry growth, although they proposed different models.

7.65 The Prime Minister's 1997 statement, *Investing for Growth*, stated that the Government aimed to develop guidelines 'to facilitate licensing of rights to intellectual property to Australian-based firms for commercialisation developed within Government contracts'.[35] The result of this commitment was *The Commonwealth IT Intellectual Property Guidelines—management and commercialisation of Commonwealth intellectual property in the field of IT* (2000). These guidelines aim to provide decision-makers with information about intellectual property law and practice, and to contribute to their thought on issues, options and risks that arise in the management of IT related intellectual property, including legal and contractual decisions. It should be noted that the guidelines are not written specifically for the circumstances of the outsourcing Initiative but give 'advice on how to draw up contracts in the future'.[36] The guidelines will be reviewed after two years.

7.66 The guidelines point out that a flexible approach must be taken to the management of intellectual property resources in IT. The guidelines advocate a case-by-case evaluation that takes into account, for example, the functions of the agency concerned, the contracting party, whether there is already some existing intellectual property, and savings that can be made by forfeiting ownership of intellectual property.

7.67 In this respect the guidelines reflect the Commonwealth Procurement Guidelines (CPGs) which state:

> The Government's approach to the management of intellectual property arrangements between itself and suppliers is to be flexible. This enables the Commonwealth, on a case by case basis, to grant industry the use and/or ownership of intellectual property that is developed as a result of a contract…An agency should obtain the rights it needs for least cost and effort to support its business needs. Whatever approach an agency adopts, it is essential that the contract clearly reflects the arrangements.[37]

Contractual Provisions

7.68 Although the contract clauses concerning intellectual property are tailored to the specific circumstance of each group, generally the clauses included in contracts address the following:

---

35 www.isr.gov.au/growth/html/it.html (25 July 2001).

36 Dr K. Daniels, Department of Communications, Information Technology and the Arts (DOCITA), Committee, *Hansard*, 18 May 2001, p. 539.

37 Department of Finance and Administration (DOFA), *Commonwealth Procurement Guidelines: Core Policies and Principles* (CPGs), 1998, p. 20.

- that neither party has any right to pre-existing intellectual property rights of the other party and that an intellectual property rights register must be created and maintained;
- the licensing of the Group's intellectual property to the contractor and the licensing of the contractor's intellectual property to the Group for the duration of the contract;
- the modification of intellectual property;
- intellectual property rights to new material developed by the contractor/subcontractors to the Group;
- protection of the agency's rights;
- treatment of contractor owned material;
- protection of contractor's rights; and
- treatment of third party contractor material and software.

Science agency concerns

7.69 Concern was raised in submissions and at hearings by the Commonwealth Scientific and Industrial Research Organisation (CSIRO) Staff Association, ANSTO and the Community and Public Sector Union (CPSU) that the outsourcing of Group 9 would place intellectual property of the agencies at risk. Group 9 agencies are scientific research agencies, including the Australian Institute of Marine Science, ANSTO, the Bureau of Meteorology, CSIRO, Australian Antarctic Division, and the Australian Geological Survey Organisation.

7.70 Research and knowledge-based agencies have a need to protect intellectual property that is distinct from other agencies. The Committee recognises the close relation between IT and innovative research in such agencies, making the protection of intellectual property a more complex and urgent issue. This relationship makes it more difficult to separate out and protect the agencies' intellectual property. The CSIRO Staff Association expressed concern about the access a multinational would have to an agency's intellectual property, telling the inquiry that 'the security of existing IP [intellectual property] accessible or identifiable in the system that may or may not be protected by quarantining is not trivial. It includes even the simple knowledge that certain work is being done'. The Association also advised that '[t]he use of penalties is not sufficient to protect important new IP that may be worth much more than the penalty to the external service provider'.[38]

38 Commonwealth Scientific and Industrial Research Organisation (CSIRO) Staff Association, submission no. 14.

7.71 The Committee was also told that when IT is separated from the agency there is a risk that intellectual property will not be developed to the extent it has been in the past. CSIRO Staff Association and ANSTO Combined Unions highlighted the close relation between scientific skills and IT operational skills and its contribution to the creation of intellectual property.[39]

7.72 The science agencies' concerns about intellectual property were alleviated to some extent by the Humphry Review. Mr Humphry observed that the science agencies faced unique implementation risks because of the difficulty of separating scientific and operational IT requirements, as well as a potential loss of staff who have a mix of IT and scientific skills and knowledge.

7.73 The Humphry Review recommended that the outsourcing of Group 9 should not proceed until 'the Chief Executives of each agency are satisfied that the implementation risks have been adequately addressed.'[40] In addressing the implementation risks of IT outsourcing, agency heads will need to carefully consider the impact of IT outsourcing on intellectual property innovation and its protection.

7.74 The Committee welcomes recommendation 9 of the Humphry Review and the Government's agreement to it. It suggests that any agency with similar concerns to the Group 9 agencies should follow the same process.

7.75 The management of intellectual property, as stated in the Commonwealth IT Intellectual Property Guidelines, is not simply about avoiding a negative impact. It is also about maximising the benefits to be gained from intellectual property developed by the Commonwealth through royalties and industry development. In its submission to the inquiry, Customs said that intellectual property 'could be used more purposefully than Australian Customs Service has done in the past'. They advised that an 'outsourced environment focuses senior managerial minds on Intellectual Property as financial returns to the outsourcer and to the Commonwealth are involved'.[41]

7.76 If such focus were to be fully taken advantage of, it might address the situation described by Mr Anthony Robey of the Information Industries Development Board (IIDB):

> …all governments in Australia have pretty much insisted in their contracts that they own the IP. Examples of the government then taking any advantage of the ownership of that IP are as close to zero that it does not matter. So a great asset of the Australian nation sits incarcerated under some contractual clauses, rather than being liberated and exercised. It makes very little sense because some of that IP would be of great use to particularly

39 ANSTO Combined Unions, submission no. 12, and CSIRO Staff Association, submission no. 14.

40 Richard Humphry, *The Review of Whole of Government IT Outsourcing Initiative*, Commonwealth of Australia, December 2001, p. 18.

41 Customs, submission no. 21.

> indigenous companies in terms of providing them with the basis for what might then become an internationally viable and useable product.[42]

7.77 While the new guidelines seek to change past intellectual property management practices, there is concern that changing such practices will require greater effort. Mr Rob Durie of the Australian Information Industries Board (AIIA) said:

> At the moment, both from a technical and an emotional point of view, if you like—a cultural point of view—government assumes that they need all the IP. They are not looking for partnerships where a company might develop the product for them and then commercialise it elsewhere, with the agency's support. The new guidelines provide a framework for that but, from the evidence we have, they have not even sent them around and, even if they do send a copy of this 100-page set of guidelines to every purchasing officer, that is not going to change behaviours. We need some proactivity.[43]

7.78 Regarding the implementation of the guidelines, Ms Holthuyzen of the Department of Communications, Information Technology and the Arts (DOCITA) said:

> All the guidelines have been sent out to them [departments] and certainly there will be follow-up encouraging them to take this into account, but there will be no direct involvement of the department in actually managing or looking at the IP elements of contracts.[44]

7.79 While there have been no overwhelming concerns expressed about intellectual property management under the Initiative, neither has there been any evidence presented to the Committee suggesting that the Initiative's approach has maximised the benefits to be gained from Commonwealth intellectual property.

7.80 The Committee identifies here a lack of vision and level of inactivity that is neglecting the potential of the intellectual property held by agencies throughout the Commonwealth.

Recommendation No. 15

The Committee recommends DOCITA conduct an evaluation of the outcomes of the Initiative's intellectual property management clauses in existing contracts. The evaluation to include, but not exclusively, an examination of the generation of government royalties, the protection of government assets and the contribution to industry development.

---

42 Committee, *Hansard*, 18 May 2001, p. 554.

43 Committee, *Hansard*, 17 May 2001, p. 432.

44 Committee, *Hansard*, 18 May 2001, p. 539.

7.81 The Committee recognises that the IT intellectual property generated and possessed by Commonwealth agencies constitutes a significant resource that should be utilised to its maximum potential. Presently there is no publicly available inventory documenting the variety and extent of Commonwealth IT intellectual property, which means that other agencies and the private sector are generally unaware of its availability.

Recommendation No. 16

The Committee notes that an intellectual property rights register is a feature of current contracts under the Initiative. It recommends that DOCITA investigate the feasibility of publicising and marketing this information, as well as details of intellectual property held by agencies that are not outsourced, with a view to maximising returns on Commonwealth intellectual property.

Effective succession plan at the conclusion of the contract

7.82 If an agency wishes to re-tender or renew its arrangements with a vendor at the end of a contract, effective succession arrangements are essential. The ANAO report on the implementation of the Initiative notes that the succession phase at the end of the contract is often overlooked at the time the contract is awarded. ANAO advises:

> It is important not to underestimate the planning and management effort required to ensure that there is a smooth transition from one contract to another. The uninterrupted delivery of goods and services is key to continued delivery of organisational outputs or business continuity, one of the risks the organisation must manage at this stage.[45]

7.83 One of the most important situations to avoid is that of becoming locked into continuing an arrangement simply because the supplier already has the contract. Professor Haque told the Committee:

> A long term contract with a particular vendor may reduce flexibility, constrain alternative options when needed, and create unnecessary dependence of government on this already agreed upon but obsolete vendor, in other words, the claimed advantage of flexibility is questionable.[46]

7.84 An effective succession plan should, if possible, prevent such inflexibility from occurring. The re-tendering of a contract should be as open as the initial tender. Mr Kelaher of the Health Insurance Commission (HIC) told the Committee that his agency did not consider itself captive to any provider or contractor. He said 'we start from the position that we have got a commercial relationship that we want to work

---

45 ANAO, *Contract Management: Better Practice Guide*, February 2001, p. 79.

46 Professor M. Shamsul Haque, submission no. 29.

with IBM GSA, as we have all sorts of other people, but we do have disaster recovery plans'.[47]

7.85 The current Cluster 3 agreement expires on 30 June 2003. The Department of Immigration and Multicultural Affairs (DIMA) noted that the cluster will be required to make a decision by the end of June 2002 about whether it wishes to extend the Agreement for an initial two-year term. It will have to take into account a number of issues if it wishes to extend the contract, including the appropriate composition of the cluster and the appropriate model of outsourcing.[48]

7.86 The absence of clear succession arrangements poses a serious risk not only to the agency, but also leaves ESPs in a situation of confusion and uncertainty. As connect.com.au, contracted to Customs before the Initiative, submitted to the inquiry:

> the transparency of the tender process has also been reduced by the lack of clear or public indication of what transition arrangements may be contemplated by ACS [Australian Customs Service] following the apparent abandonment of existing contracts between connect.com.au and Tradegate and the ACS and Tradegate.[49]

7.87 A well thought-through succession plan addresses the concerns of both agencies and suppliers. ANAO advises:

> Ideally a succession provision should be documented in the contract once it has been awarded rather than negotiating one during the contract period…If there is no provision made in the contract, then the succession phase should be negotiated with the provider well in advance of completion of the contract term. If succession is covered in the contract it should be reviewed and updated as necessary, before the end of the contract.[50]

The Committee has not been presented with convincing evidence that adequate measures for succession were devised during the development of contracts under the Initiative.

7.88 Of particular importance is the question of treatment of the assets bought by the contractor from the agency at the beginning of the contract. In particular, it is important that a contractor does not gain any undue advantage in any re-tendering process by having possession of such assets at the end the contract.

7.89 Clauses are included in contracts that aim to prevent the current contractor's possession of relevant assets from prejudicing the outcome of the re-tendering process. Schedule 11 of the Department of Health and Aged Care (DHAC) contract

---

47 Committee, *Hansard,* 9 March 2001, p. 164.

48 Department of Immigration and Multicultural Affairs (DIMA), submission no. 6.

49 Connect.com.au, submission no. 2.

50 ANAO, *Contract Management: Better Practice Guide,* February 2001, p. 79.

with IBM GSA (Disengagement Assistance) says that upon expiration or termination of the contract, the contractor:

> irrevocably and unconditionally offers to sell to Health or a nominee of Health, all Equipment owned by the Contractor and substantially dedicated to perform the Removed Services. Health may, at its option, purchase all or any part of that Equipment for the written down book value.

7.90 This clause accords with the evidence regarding IT outsourcing in general given by Mr Bell, CEO of CSC, that in his experience of outsourcing assets are sold back to the client at 'some sort of book value, some sort of fair view of the…value of the asset.'[51]

7.91 That agencies will need to develop a strategy for the expiration of contracts is discussed in the Humphry Review. Recommendation 4 of the Review, agreed to by the Government, states:

> When current IT outsourcing contracts expire, there is little benefit in mandating that agencies adhere to their existing groups. Within the overall government policy to outsource, agencies should exercise their own discretion on how to approach re-tendering or contract renewal.[52]

7.92 The re-tendering or renewal of contracts will take a significantly different form to the initial contracts. So that agencies can gain advice on these processes, there is an urgent need to act on the ANAO's recommendation, agreed to by the Government, which reads in part:

> a specific agency is assigned responsibility for the conduct and coordination of market surveillance and analysis to support and inform strategic planning by agencies for the re-tendering…[53]

7.93 A unit, the Commercial and Project Branch of the Business Services Group, has been set up within DOFA to deal with transition advice.[54] This unit will give advice on transition arrangements on a fee for service basis. At this stage the Committee has not been supplied with enough information to determine whether this unit is an adequate response to the ANAO's recommendation. Dr Boxall did not reassure the Committee with the following description of the state of the unit:

> The government's response to the Humphry Report said that we would establish a unit on a fee for service basis and at the request of agencies. We

---

51 Committee, *Hansard,* 6 August, 2001, p. 662.

52 Richard Humphry, *Review of the Whole of Government Information Technology Outsourcing Initiative,* Commonwealth of Australia, December 2000, p. 6.

53 ANAO, *Implementation of Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative*, Audit Report No. 9 2000-2001, p. 28. Recommendation no. 1.

54 Committee, *Hansard,* 19 June 2001, p. 650 and Committee, *Hansard,* 7 February, p. 91.

> will wait and see what sort of business we get. When we get the business we will resource it.[55]

7.94 In the Committee's view the services provided by such a unit should include advice about planning for contract succession. This should include information about the review and evaluation of contractual arrangements. As ANAO states, the 'contract succession phase…also includes a review of the successes and failures that occurred over time in the contract arrangements'.[56] While in a devolved environment the effectiveness of contract provisions needs to be evaluated for each agency, some coordination of knowledge and experience of the adequacy of contractual arrangements is also required. The Committee draws attention to the need for a mechanism to coordinate the accumulated knowledge gained through agencies of the effectiveness of current contractual arrangements for re-tendering and future outsourcing arrangements.

7.95 This matter of a special service unit is discussed at greater length in Chapter eleven.

7.96 The effectiveness of contractual arrangements discussed in this chapter in managing risks under IT outsourcing have been tested to greater and lesser degrees. The operation of service credits as a sanction provided for by contracts has been tested, and where appropriate, revised to be more workable. But while it might be said that the absence of any major breaches of intellectual property, data security and privacy clauses signifies the soundness of contractual provisions, concerns remain about such provisions. For example, do the provisions concerning intellectual property ensure that the benefits to be gained by the Commonwealth from its IT intellectual property are maximised? It has been said that more is required on the part of agencies to achieve this. Is it appropriate for data to be held offshore and, if so, how should this be managed? The measures for redress if privacy, data security or intellectual property are seriously compromised by a ESP have not yet been tested. The Committee believes that all these issues need to be examined and clauses updated in the process of contract review before re-tendering.

---

55 Committee, *Hansard,* 7 February 2001, p. 216.

56 ANAO, *Contract Management: Better Practice Guide,* February 2001, p. 67.