WALTER & TURNBULL

Chartered Accountants

Office of Asset Sales and IT Outsourcing

IT Outsourcing - Group 9

Scoping Study

Draft for Discussion

13 September, 2000

Canberra Office
1st Floor
19-23 Moore Street
Turner ACT 2601
G.P.O. Box 1955, Canberra ACT 2601
Tel (02) 6247 6200 Fax (02) 6257 6655

Sydney Office
Level 18
109 Pitt Street
Sydney NSW 2000
G.P.O. Box 3808, Sydney NSW 1044
Tel (02) 9233 2599 Fax (02) 9233 2123

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

2 BACKGROUND

2.1 Introduction

The Government decided in 1997 that IT infrastructure and services across all budget funded Agencies would be outsourced subject to the outcome of a competitive tendering process. In 1998, the Prime Minister reiterated general Government policy that outsourcing of IT infrastructure should proceed unless there is a compelling business case on a whole of government basis for not doing so. The Government again reinforced the importance of early implementation of the outsourcing reform program in 2000. To assist Government entities operating under the Commonwealth Authorities and Companies Act 1997 (and other enabling legislation), the Government decided to issue Notices of General Government Policy to facilitate implementation of the policy by those entities.

The Government has mandated the following areas as within the scope of the Government's IT Infrastructure Initiative (the "Initiative"):

- Desktop and LAN services – including:
  - desktop computers, portable computers, handheld computers, monitors, keyboards, pointing devices, multimedia peripherals such as speakers and microphones, printers, scanners etc.
  - file, communications, electronic messaging, gateway, print, firewall, proxy web and other servers.
  - hubs, routers, bridges and other LAN related equipment and resources
- Midrange application servers
- Mainframe services
- Data communication services
- Cross Platform services (such as technical support and help desk)

The infrastructure described above exists in various environments for various uses. For example use of a PC in an Agency that performs primarily administrative functions can be quite different from the use of a PC in a scientific and research environment. Both PCs are within the scope of the Initiative.

Through the outsourcing of IT&T infrastructure, the Government (and each of the Group 9 Agencies) expects its business needs to be met and to pursue financial and other benefits through economies of scale and opportunities for consolidation, rationalisation, and standardisation of IT&T operating environments. In accordance with Government directives, all of the foregoing mandated services are in scope.

The Agencies that form Group 9 are:

- Australian Antarctic Division (AAD);
- Australian Geological Survey Organisation (AGSO);

- Australian Nuclear Science and Technology Organisation (ANSTO);
- Bureau of Meteorology (BOM); and
- Commonwealth Scientific and Industrial Research Organisation (CSIRO).

Because Group 9 is comprised of scientific and research Agencies, outsourcing the IT infrastructure of the Group may present some special issues that may justify modification to the outsourcing model used by the Initiative to date. Accordingly OASITO initiated this scoping study in order to identify the IT equipment and systems which may require special treatment in RFT documentation and the resultant contract and to identify how such IT equipment and systems should be handled.

The study team has identified potential treatment of IT equipment and systems presented to them during the course of the scoping study visits. The identified treatment is not definitive in all cases. Because the study team only saw representative equipment and systems, the percentage of equipment actually viewed may be only 5% of all the IT equipment in the Group 9 Agencies. The effect the potential treatment may have when applied to the actual volume of equipment and systems, together with other economies associated with outsourcer support may lead to alteration of the treatment.

2.2 Study Objectives

The objective of this study is to ascertain whether there are reasons justifying submission of a proposal to the Minister for Finance and Administration seeking to vary the scope of IT infrastructure to be outsourced in the Group 9 process.

The results of the scoping study are intended broadly to identify the categories of IT infrastructure to be included in the outsourcing contract as well as any variations that may need to be made to the standard outsourcing model to cater for the specific issues raised.

The specific objectives, as determined by the Group 9 Agencies and OASITO, were to use the following considerations as a guide to clarify and determine scope boundaries:

- The particular use to which IT&T equipment and systems are put.
- Whether specialist scientific equipment or systems use IT infrastructure which prohibits the achievement of efficiencies through aggregation and economies of scale.
- The effect on proposed IT&T outsourcing contract arrangements and the objective to achieve end to end performance accountability from the outsourcing provider.
- Whether a viable market exists, or can be created, for the support of particular equipment and/or systems.
- The operational practicality, including staffing issues, of particular decisions to leave equipment/systems in or out of scope with the object of ensuring that Agencies are able to continue to meet their scientific obligations and other business needs efficiently and effectively.
- Options for the treatment of particular equipment and/or systems in the outsourcing – i.e. whether there are grounds to consider alterations to the standard outsourcing model involving full provision, support and maintenance of infrastructure by an outsourcer.

- Commercial, legal and contractual implications for research contracts and arrangements, including intellectual property developed by Group 9 Agencies and their partners.

2.3 Approach

The study team was made up of representatives from Walter & Turnbull and OASITO.

Members of the study team visited locations identified by Group Agencies. Each Agency presented systems that are indicative of the complexity of IT usage within the Agency concerned. Accordingly the systems presented to the study team are representative and not exhaustive. A list of the locations visited is included as Appendix A to this report.

The study team met with key research, IT and other Agency personnel and viewed the systems identified. Agency personnel described and demonstrated the usual functions of such systems.

These visits and discussions resulted in the development of a list of issues arising from the use of IT infrastructure by the Group 9 Agencies that must be considered in the outsourcing process. The issues identified are included as Appendix B to this report. The study team analysed the issues raised during the site visits in order to identify the potential treatment of the equipment and systems viewed. This Scoping Study Report reflects the analysis undertaken by the study team.

3 THE INITIATIVE OUTSOURCING MODEL

3.1.1 The presumptive IT&T outsourcing model

Consistent with the scope of the Initiative endorsed by the Government, the 'presumptive' or 'standard' IT&T outsourcing model adopted by all previous Groups (Cluster 3, the ATO, Group 5, the Health Group, Group 8 and the soon to be released Group 11) has the following characteristics:

- The ownership by the outsourcer of most IT hardware and associated operating systems, network infrastructure (routers, firmware/software) is transferred to, and in the case of new equipment is provided by, the outsourcer.

- Data telecommunications carriage is provided by the outsourcer or procured by the outsourcer as the Commonwealth's agent under Whole –of-Government arrangements.

- The asset management function resides with the outsourcer.

- The provision, maintenance and support by the outsourcer of IT hardware and associated operating systems (including databases and middleware), and network infrastructure (cables, routers, firmware/software). Support services also include the provision of desktop, LAN and cross platform services (such as technical support, help desk and the provision of soft and hard Moves, Adds & Changes). The integration and management by one prime contractor of the IT&T environment enables end to end accountability for the entire system.

- The procurement, maintenance, support and integration by the outsourcer of desktop application suites, automated system management tools, and other off the shelf applications.

- Applications development and maintenance (and associated software tools) are usually retained as an Agency responsibility, but Agencies have the option of including applications development and maintenance in the scope of the IT outsourcing.

- Voice telecommunications is optional.

- End user training is optional.

This presumptive model is labeled 'Model 1' in Appendix C. It may be applied where specialised scientific applications are installed on machines that are also used for routine desktop purposes such as word processing, Email communications and web access. Commercial off-the-shelf software tools that assists with the application development process, such as data visualisation packages (e.g. IDL and XRT) and graphical user interface packages like UIMX could be included in the presumptive model.

The presumptive model for addressing IT infrastructure outsourcing is flexible and has catered for the different business needs of Agencies. If an Agency's business requirements indicate that variations to the presumptive model are warranted, OASITO is willing to accommodate these requirements through various means, including variations in scope, the use of different pricing strategies, service levels or other contractual provisions.

Other specific flexibilities that are part of the standard IT outsourcing contract used by the Initiative include the ability of the Agency to:

- Direct the outsourcer to procure specific IT equipment, which may include the model or brand of the equipment required;
- Take systems and equipment out of scope;
- Acquire equipment directly from third party sources and give it to the outsourcer to manage and support;
- Retain control over any decision, including timing, of equipment refresh, changes to operating systems, desktop applications and any other infrastructure that Agencies wish the outsourcer to procure, install and/or support.

3.1.2 The Care and Feed Variation

A particular variation to the presumptive model is known as the 'Care and Feed' Model.

Some Agencies in Group 8 had made significant investment in mid-range systems to perform specialised functions relating to research and scientific applications. To cater for the need of these Agencies to control some IT infrastructure at the operating system level, these Agencies varied the presumptive model for IT outsourcing as they related to the research and scientific mid-range systems. For these systems, the variation had the following characteristics:

- The ownership of most IT hardware and associated operating systems, network infrastructure (routers, firmware/software) is transferred to, and in the case of new equipment is provided by, the outsourcer. The asset management function resides with the outsourcer.

- Data telecommunications carriage is provided by the outsourcer or procured by the outsourcer as the Commonwealth's agent under Whole –of-Government arrangements.

- Support services by the outsourcer are limited to the support of hardware and the procurement, installation and upgrading of operating systems. Agencies, as in the presumptive model, retain control over any decision, including the timing, of changes to operating systems.

- The Agency retains responsibility for management of all software products on the system.

- The monthly service charges under Care and Feed may be lower than under the presumptive IT outsourcing model because there is no support given for software.

- The outsourcer is not accountable for non-performance of IT systems which result from problems with Agency managed software. Accordingly, service levels for system availability would be targets not guarantees, and no service credits would be payable for system non-availability which results from Agency actions. Guaranteed service levels on hardware support (e.g. break/fix response time) can be applied.

- The outsourcer is still responsible for recovering the IT system in the event of outages caused by the Agency and recovery service levels are applied. If outages are caused by the Agency, the outsourcer is obliged to assist with recovery of the system.

The 'Care and Feed' variation is labeled Model 2 in Appendix C.

The Care and Feed approach was developed to apply in circumstances where there is a need for Agencies to have frequent access and control over the operating systems in the normal course of their business. For example, where research and development work leads to regular modification of operating systems either through kernel code changes or through selective patch upgrades. Under Care and Feed, the outsourcer will provide the systems and/or equipment and set it up for use by the end user. Operating systems would be procured and installed, including any required upgrades, but ongoing operating system support is the Agency's responsibility. The user would be free to modify the operating system from that point onward. However, as indicated above, the treatment of service levels under Care and Feed is different from that in the presumptive model, as the outsourcer cannot be made accountable for performance failures of the IT infrastructure arising from Agency actions or modifications.

Alternatively, if the need to modify operating systems is infrequent, Agencies can use the presumptive model but exempt the outsourcer from service levels where outages are caused by Agency modifications. The advantage in adopting the presumptive model approach is that the outsourcer is still contractually bound to guaranteed service levels for systems availability for the whole of the IT environment. The Agency has the right and the discretion to access the IT infrastructure (including systems software), but the outsourcer is protected by general exclusions in the Service Levels Schedule from outages caused by Agency personnel.

Whether Agencies choose to accommodate users' needs to access systems software, including at the operating system level, through the Care and Feed approach or by using the presumptive model with general exclusions language in the Service Levels Schedule of the outsourcing contract, Agencies will need to be mindful of the effect that such a choice may have on the outsourcer's incentives. For example, under Care and Feed, a break/fix mindset is engendered in the outsourcer. If the outsourcer is confident that it will be able to repair all malfunctioning infrastructure within the contracted service levels, the outsourcer may have an incentive to acquire lesser performing equipment. Under the presumptive model, the payments and incentives regime is structured so that the mindset of the

outsourcer is focused on making the IT infrastructure work, and not merely fixing the infrastructure if it breaks.

3.1.3 Further variations to the IT outsourcing models

The study team considers that the bulk of the Group 9 IT&T systems could be outsourced under the existing variants of the presumptive IT outsourcing model (Model 1 or Model 2 above). Even so, the team considers there are IT systems in Group 9 which might not be adequately catered for by the current variations to the presumptive model. Three additional variations to the presumptive model are suggested to cater for the following circumstances where Agencies:

- Require complete control of the IT&T environments for hardware development (Model 3);

- Support the IT infrastructure owned by third parties (e.g. students, visiting scientists, CRCs, clients) (Model 4); and

- Need to take full responsibility for the ownership, procurement, maintenance and support of IT infrastructure, operating systems and applications (Model 5) because it is uneconomic or unrealistic for a service provider to support.

These additional variations are discussed below.

3.1.4 Model 3 – IT infrastructure procurement and management

The characteristics of this variation to the presumptive model are:

- The procurement by the outsourcer of IT hardware and network infrastructure (routers, firmware/software).

- The outsourcer is responsible for the maintenance of the procured hardware and network infrastructure;

- Agencies retain responsibility for asset management, procurement of the operating system, support of the procured hardware, network infrastructure, maintenance and support of system software and provision of helpdesk advisory services. The Agency also retains responsibility for the installation, maintenance and support of operating systems, database management systems and middleware associated with the system. However, at its option, Agencies may engage the outsourcer on an ad hoc basis, to assist Agencies with any aspect of their retained responsibility for the system.

- If the outsourcer provides support under this approach it would still be responsible for recovering the IT system in the event of outages caused by the Agency and recovery service levels could be structured to cater for this similar to a traditional maintenance

contracts. If the outages are caused by the Agency the outsourcer would be obliged to assist with recovery of the system.

- The outsourcer would not be solely accountable for any non-performance of IT systems resulting from problems with Agency managed hardware or software. Accordingly service levels for system availability would be targets not guarantees, and service credits would not be ordinarily payable for system non-availability.

This approach would be applied in circumstances where the user intends to undertake experimentation on IT&T hardware. This could involve complete dismantling and reconstruction and in some cases inclusion of hardware designed and built exclusively for the research process. This scenario would apply where hardware is to be fundamentally changed. Ownership of the IT hardware, and the asset management function could be retained by the Agency concerned. However, through the RFT process, Agencies could explore with tenderers what flexibility is available in leasing arrangements to avoid being left with a residual asset management function.

3.1.5 Model 4 – IT infrastructure support

This approach seeks to provide for the support of IT infrastructure brought to the Agency by visiting scientists and IT infrastructure not owned by the Agency but located at Agency sites as part of a joint venture, a Cooperative Research Centre (CRC) or other collaborative venture.

The characteristics of this variant to the presumptive model are:

- No ownership or procurement of the IT hardware by the outsourcer; this function resides with the owner of the IT equipment (i.e. the visiting scientist or student, CRC or client).

- The outsourcer supports the IT hardware and associated operating systems and desktop applications on an ad hoc basis as requested by the user. To the extent the service provider is not able to provide full support, i.e. the software is written in Japanese Katana character set, the level of support could be varied. There are various payment options available, including time and materials, or a set fee for a particular type of support service provided to a visitor.

Potentially, this approach could also be applied to equipment and/or systems that receive a lower level of support in accordance with Models 2 or 3, but the user still requires some additional services. An example may be a PC that is not fully supported because the user is developing software that requires modification to the operating system. As a result it is designated as equipment that falls into Model 2. Despite the high level of IT expertise of the end user, he or she may still desire support in the form of assistance with the standard Microsoft Office software suite or other services that are not within the user's knowledge base. In such situations, it may be preferable to use Model 4 to provide support to the user.

3.1.6 Model 5 – Agency responsibility for IT infrastructure

This refers to those service functions that are retained by Agencies.

Some equipment would not be classified as IT infrastructure. Although a case might be made that this non-IT equipment should be outsourced, it does not fall within the mandatory scope of the Initiative. Examples of such equipment are instruments that have embedded IT functionality that are so integral to the working of the instrument that they cannot reasonably be managed separately from the instrument. Generally these are purchased as an integrated item from a vendor who then maintains and supports the instrument directly with the scientists using it. Examples of this infrastructure are Automated Weather Stations (AWS) operated by BOM, expendable balloon sondes operated by BOM and environmental sensing equipment installed by CSIRO in bulk grain storage dumps.

The study team saw computing infrastructure which is so integrated with the instrument that it was not recognisable as a "PC" as it does not have a screen or keyboard and in normal operation interacts directly with the instrument without direct human intervention. In other cases, the study team saw PCs which were attached to the scientific instrument and whose sole purpose is to operate the instrument. The study team considers that PCs whose only function is to operate or support a scientific instrument might best be treated as an integral part of the scientific instrument and therefore excluded from the outsourcing.

To the extent that a PC is re-deployed from operating a scientific instrument to some other purpose, at the time of redeployment, the PC is in scope and should be treated in the same manner as a 'new' PC arriving in to the Agency IT environment. If a PC is attached to an instrument and the function of that PC is to collect, analyse and distribute data through the network, that PC is included in the scope of the IT outsourcing.

In determining the scope of the IT infrastructure to be outsourced, Government policy has made it clear that all IT infrastructure should be outsourced unless there is a compelling business case on a whole of government basis for not doing so. Through the outsourcing of IT infrastructure, the Government and each of the Group 9 Agencies expects their business needs to be met. The Guidelines for the Scoping Study raised the following considerations regarding decisions to exclude IT infrastructure from the scope of the Group 9 IT outsourcing:

- No viable market exists, or can be created, for the support of particular equipment and/or systems;
- The decision to leave equipment and/or systems in scope is operationally impractical, potentially due to staffing issues; or
- There are unworkable commercial, legal and contractual implications for research contracts and arrangement.

The question of whether a viable market exists, or can be created, for the support of particular equipment and/or systems is not answerable at this time for every type of equipment shown to the study team. The determination of the existence, real or potential, of

a market will have to be determined through discussions with industry participants either prior to or as result of the tender process. There may be unique equipment or a system that is clearly not economical to outsource or realistic to think that an outsourcer could effectively support, but for the most part this will need to be part of an ongoing examination concurrent with the development of the RFT.

An overriding consideration will be the operational practicality of decisions of scope. There are a few issues that need to be considered. Multiple boundaries make contract management more difficult. The more equipment and/or systems that are removed from scope, the more boundaries there are to manage. Contract management will be simplified if boundaries are minimised. In addition, in an outsourced environment, Agencies may have reduced resources available to support equipment or systems that are removed from scope. As a result, the retention of responsibility for equipment and/or systems may not be an attractive option to Agencies.

Finally there may be commercial, legal or contractual reasons for removing equipment and/or systems from scope. As discussed in this Scoping Study Report (section 4.7.4) there are certain projects or areas within Agencies that involve confidential information or intellectual property of Agency clients. As a result of the needs or demands of clients, such projects may need to be quarantined from the normal scope of the services being provided by the outsourcer. In these cases, the outsourcer may still have some asset management control of the IT hardware, but no other involvement with the IT infrastructure. In other circumstances, even the asset procurement and/or management responsibility may be removed and retained by the Agency.

Other circumstances exist that may cause IT equipment and/or systems to be removed from scope. These may include contractual relationships that do not allow the Agency to replace itself with the outsourcer. OASITO has provided the Group Agencies with draft contract clauses to insert in new contracts for the procurement of IT&T equipment and software. The purpose of these contract clauses is to preserve Agency flexibilities in the IT outsourcing process. The contract clauses provide Agencies with the right to terminate, transfer, assign or novate IT&T contracts to the outsourcer at no cost to the Agency and without the need to obtain the prior approval of the third party supplier. The insertion of the contract provisions will give Agencies the flexibility of retaining the services of important third party IT&T suppliers, but under the management of the outsourcer, thereby retaining end to end accountability for the provision of IT&T services with the outsourcer as prime contractor.

There may be cases where assignment or novation of a third party contract to the outsourcer is not possible and the equipment and/or systems involved will have to be left under the control of the Agency for some period of time. In some ways, this movement is analogous to the movement of equipment as a result of changes in circumstances described in section 3.1.7.3 below. To the extent the conflict of interest is resolved through realignment or modifications in the project or area involved or the project is completed, the equipment or systems could move back to become the outsourcer's responsibility in a similar fashion to equipment coming in from field work or from Antarctica.

3.1.7 Flexibilities of the IT outsourcing model

3.1.7.1 Additional services option

All the variations to the presumptive IT outsourcing model include the ability for Agencies to obtain additional services from the outsourcer on an ad hoc basis. This is represented in Appendix C as the areas coloured in green. The green areas denote functions that could be performed by the outsourcer or Agency staff. Whether the outsourcer provides these services should be determined largely on the basis of operational and economic considerations. Possible examples of additional service provision on an ad hoc basis are:

- A user would like additional support above and beyond what is contemplated on a daily basis for particular equipment and/or systems. This may be utilised in the process of developing a new application where the developer would like input from the outsourcer or where a user has a basically unsupported machine but would like the outsourcer to replace a hard drive or perform other maintenance or support functions.

- A CRC wishes the outsourcer to install the upgrades to an operating system on a machine that is owned by a third party participant.

This option gives Agencies the flexibility to access the resources and expertise of the outsourcer on an ad hoc basis and to meet unexpected demands for IT infrastructure and other services that Agencies are not able or do not wish to meet from their own resources. The difference from the Agency point of view between a service that is included in the scope of services under the IT outsourcing contract on a permanent basis and one that is acquired from time to time on an ad hoc basis are:

- Additional Agency overheads in specifying and managing the ad hoc service; and

- Likely higher total service charges.

While accountability and performance standards for ad hoc services need not differ from services that are obtained on a permanent basis, the total service charges are likely to be higher in a contract that includes a large number of ad hoc services in comparison with the total service charges for exactly the same services if such services had been included in the scope of the contract rather than obtained on an ad hoc basis. If a service is included in the scope of the outsourcing contract, it is included in the predictable volume of services that the outsourcer will use to determine its staffing requirements. The outsourcer should then use the cost of these staffing requirements to determine various unit rates. By including a service in scope, the outsourcer can develop the most efficient staffing requirements (i.e., by combining fractional Full Time Equivalents (FTEs) required to accomplish various diverse services in order to assign the fewest number of actual personnel to the project). If a service is provided on an ad hoc basis, the tenderer does not have a predictable volume of services over which costs can be spread, and therefore must price these services on a per-incident stand-alone basis. Therefore, the outsourcer may not be able to smooth out the inevitable fractional FTEs, which is likely to result in higher actual service charges payable for a given

number of ad hoc incidents as compared with the actual service charges that would be payable had the same number of incidents been included within the base services. This result is likely to eventuate whether ad hoc services are priced on a unit rate basis or on a 'time and materials' basis.

It is therefore important for Agencies to strike the right balance as between the responsibilities to be allocated to outsourcer and Agencies. Whether an Agency chooses the additional ad hoc services option in a given situation may depend on how often the Agency needs to take up this option and the likely staffing profile at the site.

3.1.7.2 Specification of equipment

Under any variant of the presumptive model, the Agency or user may specify particular characteristics of the equipment needed. Obviously, economies can be obtained through standardisation. As a result, Agencies will benefit the most from specifying baseline requirements in the form of processing power, memory needs, ports, slots, necessary cards as well as other criteria and leave the choice of exact equipment to the outsourcer. This approach can be highly effective in standardised office environments.

In circumstances where the Agency requires a high degree of flexibility in the specification of equipment, baseline specifications can be omitted and future requirements can be specified on a case by case basis. In that situation, the outsourcer's responsibility is to procure the equipment specified by the Agency, install it and then provide, maintain and support the equipment in accordance with the general service definitions.

3.1.7.3 Changing circumstances

The presumptive IT outsourcing model and the variants discussed above will cater for occasions when the circumstances of the use of the IT infrastructure changes. This can happen in a variety of ways. Examples are:

- An Agency deploys equipment from home base to Antarctica.
- A scientist takes a laptop into a remote area on field work, which may include down a mine shaft or into the eye of a tropical storm.
- A research project group determines that the equipment it was using for administrative functions will be used to conduct experiments involving hardware development.

The first two examples relate to circumstances whereby the outsourcer will not be able to provide physical support to IT equipment which the outsourcer usually supports (except under Model3 which has no IT hardware support component unless requested by the Agency) at home base. The third example relates to occasions when IT infrastructure needs to move between models. These circumstances can be catered in the following ways:

The Antarctica scenario

- When IT infrastructure is deployed, for example from Kingston to Antarctica, the equipment may not change its original model allocation. An administrative PC in Kingston becomes an administrative PC in Antarctica and will remain in Model 1.

- Where remote control and support of the IT infrastructure by the outsourcer is possible, the only services that the outsourcer cannot provide for the administrative PC in Antarctica are the hard Moves, Adds and Changes (MACs) and on-site break/fix services.

- Physical support – i.e. the hard MACs - (e.g. changing hard disc drives) will need to be undertaken by the Agency, with support if required by the outsourcer through the Helpdesk. In the RFT hard MACs are priced separately from other services and Agencies only pay for hard MACs when they are required. The cost of soft MACs is usually structured as part of the charges for helpdesk services.

- A requirement for the outsourcer to provide adequate stock of spare equipment and parts in Antarctica should enable a continuation of current standards of service for Antarctica at a minimum.

The Antarctica approach can be extended to other circumstances whereby remote control and support of IT infrastructure is possible, e.g. in ocean going vessels such as the Southern Surveyor, in 'clean' or quarantined laboratories such as CSIRO Animal Health Laboratories, and where the requirement for the physical presence of the contractor staff would be reduced if possible because of limited berths on vessels or stringent safety or quarantine requirements.

There are, however two constraints on the successful implementation of remote management as envisaged above.

- Remote management of LAN connected machines has become possible with the use of UNIX and Microsoft NT based machines. The relatively frequent use of the DOS operating system in equipment that is attached to scientific instrumentation in areas such as the Radio Pharmaceuticals laboratory in Lucas Heights is likely to reduce the capacity for effective remote LAN management at such sites. This outmoded operating system does not allow for multiple users and multiple processes running concurrently, which is a requirement for remote machine management.

- Whilst the Inmarsat satellite communications are used as ship to shore communications in CSIRO and AAD vessels its use is constrained by high cost and restricted bandwidth. Online sessions are restricted and most communications such as email and data transfer are carried out in batch format in proprietary compressed files**.** Remote management of shipboard LAN equipment is possible but is likely to be extremely expensive.

The advantages of remote LAN management are:

- the outsourcer retains ownership and asset management control of the IT equipment; and

- Agencies need not maintain pre-outsourcing levels of IT expertise to support IT infrastructure in the event that that IT infrastructure is deployed by the Agency in circumstances where the outsourcer cannot physically support the infrastructure.

The 'Down the Mine' scenario

In circumstances where, for example a laptop goes down a mine shaft or is used to record the progress of a tropical cyclone, for the duration of this activity the outsourcer may not be able to provide physical support of the equipment. Telephone support by the outsourcer through the Helpdesk may still be possible, but for practical purposes, if the equipment malfunctioned, current practices would continue.

The widespread geographical dispersion of Group 9 Agencies could enable scientists, when working out in the field to drop off malfunctioning IT equipment at any Group 9 Agency site or outsourcer location for repair and/or replacement. For example, an AGSO geologist working in Darwin could leave a malfunctioning laptop at a BOM office or outsourcer location and obtain a working laptop as replacement. The geologist could return the borrowed laptop to the outsourcer on return to AGSO in Canberra, with the repaired laptop also returning to Canberra. This would be a major benefit to those staff operating in a range of locations. Obviously Agency cooperation is a prerequisite for this service. Some effort may be involved to ensure contractor billing and asset management systems could cater for this extra service.

The changing circumstance scenario

The issue in this scenario largely revolves around tracking and charging for the IT infrastructure. Because Agencies, in conjunction with the outsourcer will need to devise a mechanism to track the circumstances or locations of IT infrastructure, monthly service charges can change as equipment moves from one circumstance to another. Logistical issues will need to be worked out jointly between Agencies and the outsourcer to determine the actual procedures for handling movements from one circumstance to another.

3.1.7.4 Implications of multiple variations to the presumptive model

The particular IT&T service requirements that arise from the functions the Group 9 Agencies perform can be met through varying the presumptive model of IT outsourcing. However, in order to meet the need for flexibility expressed by all the Group 9 Agencies, the implementation of the contract for services becomes more difficult. The existence of multiple variations to the presumptive model will require discipline in contract management. At the same time, reporting systems (at both the outsourcer and the Agency end) need to operate at high levels of efficiency and effectiveness. For example, if an administrative PC is not reported as transferring from Kingston to Antarctica where such movement could decrease

the level of support given by the outsourcer, the Agency could pay higher charges than necessary for a year.

3.1.8 Classification of equipment

The study team has classified for Agencies other than CSIRO, the equipment and systems it was shown during site visits. The equipment and systems that would fall into the presumptive model or any of the variations shown on the chart in Appendix D are listed under the applicable headings in Appendix E. In the case of CSIRO, further information is necessary in order to classify equipment and systems.

4 DETAILED ASSESSMENT

4.1 Particular use to which IT&T equipment and systems are put

Study Findings

In the course of the site visits, the study team identified the following ways the Group 9 Agencies use IT in the support of their work:

- In support of the documentation of their research and its results and for general administrative purposes;

  The requirements for this process are similar to the requirements of those involved in administration. That is to say it usually involves the use of common desktop software suites. Word-processing, spreadsheets, databases, presentational graphics and printing are employed for these purposes.

- In support of communications and access to existing knowledge bases.

  This role for IT infrastructure is more of a routine desktop function. It allows researchers access to resources such as the internet both for knowledge bases and a vehicle of communication with distant research colleagues as well as the transfer of data collected internally or by third parties. In some cases this included the development and implementation of extranets or limited access information sharing mechanisms.

- To provide automated control of research instrumentation;

  PC style equipment is attached to scientific instrumentation and devices via interface cards. These most commonly are serial in nature and may require 8, 16, or 32 bit interfaces to the computer concerned. Computers receive data from the instrument and then may issue feedback control instructions to the instrument. Usually this requires "real-time" processing capability and CPU, data bus and communication timing is critical.

- To acquire data from sensing devices incorporated in research or scientific instrumentation;

A system used in this way must have the ability to receive data from sensors that form part of instrumentation. Most commonly these will be custom made and will have particular requirements as to the interface card employed. Interface cards are most commonly designed and built in-house. The nature of the sensor/computer interface may also dictate the type of operating system employed and the software used to drive the system. Commonly this will give rise to a requirement for the use of outmoded hardware and/or software.

- To analyse and investigate collected data;

  This process usually involves the intensive processing of numerical data and commonly will culminate with the generation of graphical visualisation of the results derived from the analysis process. Requirements here are commonly for processors with the capability of high throughput and floating point calculations.

- To develop and visualise models of the environment and data under research;

  This process, like the data analysis process, has a requirement for extremely high computational throughput. This area has one of the highest needs for computing power and large data storage and transfer. This area generally requires leading edge IT technology. A further example of this is the use of high end and sophisticated graphical work stations to present three dimensional visualisations of data sets. This was seen at the Queensland Centre for Advanced Technology where researchers were converting numerical data information into three dimensional models of mining sites.

- As a service delivery medium for results of data analysis;

  An example of this requirement was seen in BOM where this organisation is under obligation to provide timely advice of weather forecasts to the aviation industry. This information has an inherently short "shelf-life" and delayed transmission results in the information becoming irrelevant. BOM also uses a system called CMSS that deals with numerical weather prediction data. Network failure can result in the complete irrecoverable loss of this data.

- As a platform for the development, testing, maintenance and support of hardware and software for clients or in support of research activity.

  IT infrastructure used in this way has a requirement that it must closely match the environment for which development is being carried out. This implies the potential need for infrastructure modification to meet the requirements of the project that is undertaken. It also implies that configuration and usage of the IT may be novel and necessary customisation could move far from manufacturer's original design and specification. As a result, the infrastructure may be modified beyond recognition in the course of experimentation. There is also the possibility of permanent damage to the equipment.

- As the object of research activity.

  Research is being carried out in relation to the use of IT infrastructure. As in the previous dot point this can involve fundamental alteration and customisation of infrastructure in an experimental mode.

- Mass Data Storage.

  The data acquisition activities used with scientific instrumentation can frequently give rise to vast quantities of data. There is a need to be able to store that data such that analysis may be re-performed and that reference may be made to it at a future time. Often data is required to be kept for extended periods of time. This requirement brings with it the implications of inherent problems in safe archival of the information that will prevent data loss or corruption.

The study team found IT&T equipment used to support scientific research to be installed in the following environments:

- Office environment. This environment is common to all Agencies. The functions performed within the environment go beyond normal administrative functions. They include, among others, the support of software development, data analysis and visualisation and general documentation processes.

- Laboratory environment. IT infrastructure used in a laboratory environment was frequently used to support scientific instrumentation and data acquisition processes. The environment could involve hazardous working conditions. Environments the study team was shown included hazards such as risks of exposure to nuclear radiation, laser light radiation, biological hazards, chemical substances and hazardous gases.

- Laboratory/Workshop environments. The laboratory/workshop environments include areas dedicated to the building or manufacturing of equipment related to the particular scientific undertaking. Often IT infrastructure in this environment is being used to support manufacturing and industrial processes under development. Some of these areas are also hazardous environments because of the machinery involved in the manufacturing process.

- Inaccessible environments including;
  - On board ocean-going vessels;
  - On board aircraft;
  - On board large mining equipment;
  - Down mines;
  - Mobile seismic observation caravans;
  - Mobile instrumentation caravans such as the LIDAR sensor and the “Big Foot” seismic research device;
  - Small outpost sensing stations used for Seismic and Climate observation;
  - Remote Climate research and observation stations; and
  - Antarctic research stations.

The different environments are not always distinct. The environments may overlap and equipment may be used in more than one environment.

The way in which IT infrastructure is used in scientific research, the delivery of products and services, the diverse nature of research and service delivery that is being undertaken and the environments in which equipment is located has resulted in a highly diverse range of computer hardware, operating systems and applications comprising the IT infrastructure of the Group 9 Agencies. This is reflected in the broad range of skills of the Agency personnel involved in the use and support of the IT infrastructure.

In the course of the review the study team noted at least nineteen different operating systems, each of which were present in several versions, including:

- AIX;
- DOS;
- HP-UX;
- IRIX;
- Linux;
- LynxOS;
- MacOS;
- Microsoft Windows NT;
- Microsoft Windows version 3.1;
- Microsoft Windows version 9x;
- OS/2;
- QDOS;
- QNX;
- Solaris;
- SunOS;
- Super-UX;
- True 64;
- UNICOS; and
- VMS.

In common with the diversity of operating systems the study team also noted a similar diversity in systems hardware. This diversity included:

- Hardware manufacture ranging from "tier-one" brand name machines to "no-name" machines;
- Machines from the leading edge of computer technology;
- Aged machines using long outmoded technology; and
- Componentised computers such as small form-factor PC cards.

Many of the Agencies employ a "trickle down" process as a more economic means of meeting the needs of high end users. Certain of the high-end users require frequent upgrades of equipment to keep up with improving technology. The refresh rates for these users may be as often as every six months or less. Economic considerations have resulted in Agencies re-deploying such equipment to other personnel whose needs do not require

leading edge technology. The "trickle down" process is used to enable hardware to have a longer life within the organisation. The "trickle down" process has also facilitated the need for retention of outmoded equipment to be used as spares required to support the use of outmoded equipment attached to scientific instruments and devices.

4.2 Issues relating to location of equipment

4.2.1 Support of systems in hazardous environments

The study team found that a significant number of systems are located in what could be described as hazardous environments. These include laboratory areas in which biological hazards exist such as the CSIRO Animal Health Laboratories, quarantine areas as exist in CSIRO Entomology areas, laboratory areas that are devoted to the processing of radioactive materials and areas within the nuclear reactor installation which exist at ANSTO, Lucas Heights. Currently, support of equipment located in these areas is provided by research staff who access the areas in the course of their normal business activities and to a lesser extent staff from IT support areas. IT support staff are generally called on to provide assistance with networking issues.

Some hazardous areas, such as those subject to quarantine requirements, have specific processes concerning the entry and exit of people and equipment. In some cases, equipment cannot be taken out of the environment without following strict decontamination procedures that cause unrecoverable damage rendering the equipment totally unusable.

Exposure to radiation presents a particular problem in that the level of exposure an individual may absorb is strictly monitored and regulated. In the event that established thresholds are exceeded in a given period, the recipient is precluded from re-entering the site for a twelve-month period.

The risk of staff exposure to nuclear radiation, has the potential to place a contractor in the position of having to plan for the possibility of staff being rendered unusable at the site for a period of one year in the event of excessive radiation exposure. Designated "radiation" workers are permitted to be subject to doses of radiation twenty times higher than the general public. Whether an IT service contractor and/or its staff would go through the processes to be given that designation is simply not known at this stage. If the contractor's staff obtain "radiation worker" designation the risk of staff being rendered unusable due to exceeding acceptable radiation doses would be diminished.

At times, some BOM systems may need to be supported during hazardous weather conditions. While the equipment involved may generally not be located in a hazardous environment, during periods of extreme weather conditions, the equipment or systems may fall into this category.

In each case, there are safety and monitoring procedures that must be strictly adhered to. These procedures are well developed and IT support staff are obliged to observe and work within the requirements of these procedures. These rules have to be followed at all times

and the consequences of a breach could be very serious, including the potential loss of life or financial costs. No untrained staff can be allowed to work in these controlled environments. In some cases, compliance with these procedures may be time consuming.

The requirement for safety and procedural training and the additional time involved in complying with safety and other procedures will have to be explained to tenderers so that the specific requirements of Agencies are understood by tenderers.

Potential Treatment

Hazardous environments, by themselves, do not impact the type of services required of an outsourcer to support IT equipment. The impact of the location of IT equipment within hazardous environments is to impose an obligation on an outsourced service provider to educate itself on the applicable safety and other procedures and ensure that its employees comply with them.

As a result the IT equipment and/or systems located within hazardous environments should be outsourced in accordance with the models described in section 3. The ability of the industry to provide support under such conditions will have to be explored through the RFT process.

4.2.2 Use of equipment in hostile environments

Most Agencies visited advised that equipment used in field experimentation was frequently used in an environment hostile to the machine. This includes the risk of salt spray in the case of machines placed in the marine environment, abnormal amounts of dust in the mining and seismic research environments, and in all cases where infrastructure was placed in ships, planes or motor vehicles there was the risk of abnormal physical shock. In several cases the study team were shown equipment that had been "ruggedised" with a view to minimising the risk of shock. See also section 4.4.3 for a discussion of the implications of modifications made to the hardware in order to accommodate use in hostile environments.

Potential Treatment

The use of infrastructure in these environments expose the equipment to abnormal wear and tear. This is an issue that will have to be taken into account in contract development. The level of care taken by scientists carrying equipment out into the field appears to be quite high under the current system. However, the unusual situations in which some of the Group 9 Agencies use IT infrastructure may create a higher level of concern by an outsourcer. Presumably, the arrangement would work in a similar fashion to that existing in other contexts. The outsourcer would repair the equipment and a mechanism for payments would need to be determined. This would be developed in the tender process.

4.2.3 Infrastructure located in remote locations

Many of the Agencies visited have equipment that is permanently located in extremely remote locations. In some cases travel to and between these locations, for example the Antarctic bases, is restricted to a relatively small window of time annually. Additionally, accommodation at these bases is restricted. A further example is the observatories maintained by BOM on difficult to reach islands.

In other circumstances, for example observation posts maintained by CSIRO, BOM and AGSO, the equipment is placed in remote locations in outback and rural Australia.

Support of remote observation posts maintained in Australia by AGSO is provided by the custodians of the equipment living in the remote areas in which the equipment is found. Specialist support is provided only when the local support is unable to resolve a problem.

BOM remote observation stations are manned by staff who are primarily "observers". These personnel are given adequate skills to maintain infrastructure on their stations and these are backed up by telephone help from the main centres.

In some cases support of infrastructure by dedicated IT support personnel is impossible. Limitations imposed by available accommodation for example on board a ship, aeroplane or at an Antarctic base make it impracticable for the inclusion of dedicated IT support personnel. Additionally access to and between the Antarctic stations is not possible for lengthy periods of the year and would result in significant idle time on the part of specialist IT support staff. Several of the BOM island observatories are only accessible by helicopter in fair weather.

Potential Treatment

There is no reason an outsourcer could not own and procure the equipment, maintain it on a back to base basis and provide remote support for IT infrastructure which is located in remote locations. To the extent equipment has been deployed into the field and that equipment malfunctions, the user could potentially bring the equipment to any Group 9 Agency site for service. As discussed in section 3.1.7.3 an AGSO geologist working in Darwin may be able to leave a malfunctioning laptop at a BOM office and obtain a working laptop as replacement.

Some equipment will be more suitable for remote support. For example the Australian Antarctic Division maintains local area networks on its Antarctic Stations at Mawson, Casey, Davis and Macquarie Island. These are used, in addition to scientific activities, for routine administrative purposes including email communications and Internet access. Staff at Antarctic Division headquarters in Kingston Tasmania currently manage the LAN facilities on these stations remotely. Naturally physical maintenance of hardware and network connections is dependent upon technicians who are at the bases year round.

In other situations, such as the use of IT equipment running under DOS, the ability to provide remote support will be more limited. To the extent that the locations are remote but not inaccessible, the outsourcer should be able to service the sites when necessary.

The determination of what Model the IT equipment in this category will fall into depends equally on the nature and use of the equipment, not just its location (see also section 3.1.7.3 above).

4.2.4 "Itinerant" equipment

Several of the Agencies visited support activities that require the movement of infrastructure from the office or laboratory environment into remote environments such as ships for marine research, aircraft for atmospheric research or extreme weather monitoring/reporting, motor vehicles for seismic research and into mines for industrial research. This commonly involves the periodic installation of equipment in a ship, plane or truck together with networking capability. At the end of the expedition the equipment is restored to its office or laboratory environment.

An additional complicating factor in relation to the use of equipment in the marine or aviation environment is the limited accommodation that is available for staff who have to support the equipment. Currently, support is commonly provided by the scientists who accompany the equipment and who have the responsibility for conducting research or monitoring/reporting functions.

It is possible that this equipment could be supported by the outsourcer when it is located in the "normal" office environment but revert to Agency responsibility when it is being used in the field. When the systems are in the field they would be supported by the scientists using them and support would revert to the outsourcer when the equipment returned to base. However, when the systems are out in the field the outsourcer may still be able to provide some remote support, an example of which would be help desk services.

An issue presented by this division of responsibility is the need for scientific staff to maintain a sufficient level of expertise to be able to adequately support the equipment whilst in the field. Scientists providing support at some times and not at others could result in a lower overall level of expertise and familiarity with the equipment and may result in reduced levels of support when the equipment is in the field.

Potential Treatment

The model applicable to itinerant equipment while in the home location will depend on the nature and use of the equipment. When it goes into the field it will either have some support envisioned by Model 3 or fall into Model 5.

4.3 Equipment used in support of instrumentation

4.3.1 Support of machines associated with scientific instruments

Most Agencies make extensive use of instruments such as Electron Microscopes, Gas Chromatographs and Mass Spectrometers that utilise PC style hardware for instrument

control and data acquisition. It is not unusual for more than one PC to be incorporated into such instruments. PC hardware, software and interfaces between the instrument and the PC hardware is usually specifically configured at the time of manufacture. Control and data acquisition software is usually written and supported by the instrument manufacturer. The successful functioning of the instrument is highly dependant upon the integration between the instrument and the IT hardware and software that is supporting it.

These machines are usually subject to warranty arrangements for the initial period of the instrument's life and subsequently are commonly subject to a support maintenance arrangement and as such are supported by the instrument vendor. The study team found that at the end of the warranty period and where maintenance support for the instrument is not available, support is commonly provided in-house. This ongoing support is dependant upon collaboration between scientific staff who use the instrument and members of the in-house IT support group.

In the event of failure of an instrument, the identification of the required remedy involves a knowledge of the instrument itself, the interface between it and the PC and the workings of the PC hardware and software.

Often the Agency has maintained the same level of PC hardware and operating system for the life of the instrument which may be ten years or more. Technology refresh cycles in relation to PC hardware incorporated in the instruments is usually linked to the life of the instrument rather than the conventional lifecycle of desktop equipment.

The ongoing use of these instruments without upgrading the associated IT infrastructure for a period of ten years or more results in the associated IT infrastructure becoming increasingly difficult to support and maintain due to declining availability of spare parts and a decreasing knowledge base. (The issue of supporting outmoded equipment is discussed in section 4.3.2 below.) The users of these instruments informed the study team that upgrading to current levels of technology can be expensive and time consuming as a result of the need to redevelop device drivers and data interfaces to sensors.

On relatively rare occasions the supporting PC hardware and operating system is upgraded during the life of the instrument. This upgrade may involve the redevelopment of drivers for the new operating system and hardware that allows continued interface to the instrument. This redevelopment is commonly done "in-house". Based upon the information provided to the study team during the course of the visits, any such upgrades are made by the project or group involved in the use and operation of the instrument. In essence, although they were done in consultation with the IT support group in the particular location and with the manufacturer, these upgrades were done in isolation.

Potential Treatment

PCs (irrespective of age or uniqueness of operating systems) whose only function is to operate or support a scientific instrument may be treated as an integral part of the scientific instrument. To the extent that a such a PC is re-deployed from operating a scientific

instrument to some other purpose, at the time of redeployment, the PC is in scope and should be treated in the same manner as a 'new' PC being installed in the Agency IT environment. If a PC is attached to an instrument and the function of that PC is to collect, analyse and distribute data through the network, that PC should be treated under model 1. In the event that user requirements are such that system superuser access is required the system should be treated under Model 2.

In many cases, scientific instruments with PC components are bought subject to support arrangements in the form of warranty or other type of maintenance contract. During the period of such a support arrangement, the vendor would support both the instrument and the PC component. At the expiration of the support arrangement, support would revert to the outsourcer under Models 1 or 2 as described above. Mechanisms for the transition of responsibility and potentially the transition of ownership will have to be determined in the course of the tender process.

In each case, the outsourcer would provide network connectivity for the PC component of the scientific instruments as part of the support provided in conjunction with the LAN/WAN.

4.3.2 Constraints upon the use of current equipment

In this report we use the term "outmoded" to describe IT equipment that is no longer current technology. Change in technology has significant impact upon the way in which equipment operates. These changes can result in current equipment being physically and logically incompatible with instruments and sensors that were designed to operate with technology that was current at the time of their construction.

The study team found that all Agencies make extensive use of outmoded IT equipment. Most commonly this IT equipment is found supporting scientific instrumentation. The study team was advised that, in general terms, the life of most scientific instruments and sensors is in the order of ten years. In comparison the life of most PC equipment in common use today is in the order of three years. This life span is, in the main, dictated by the rate of technological advance. Often scientific instrumentation is highly specialised in nature. Commonly the instruments are rare and very expensive. These instruments often use dedicated PC based equipment for control and data acquisition. The PC component is usually a relatively trivial part of the overall cost of the instrument.

The study team was informed that PCs used in this way require specialised interface hardware and software to enable them to perform their role. Normally, if instruments are manufactured by commercial instrument makers, the PC support is supplied as an integral part of the new instrument and is supported by the manufacturer for at least the duration of the warranty period applying to the instrument.

Over the life of the instrument the IT infrastructure supporting it, if not upgraded, becomes outmoded. This situation does not cause any degradation in performance of the instrument concerned, however it does create potential difficulties in the support of the hardware and

software associated with the computing component. Although upgrade is not impossible, the study team was told that it can be a difficult and time consuming task requiring the development of upgraded hardware interfaces and driver software. The study team found that most Agencies tend to avoid changing PC support infrastructure in these circumstances and rely upon the ability of support staff to cannibalise parts from similar equipment set aside for the purpose of repairing the outmoded equipment.

In some instances, the study team found that use of outmoded IT equipment is being mandated by the need to support aged software that is still in use. On occasions, the aged software is required to access and interpret data that has been created and stored through the use of the software. The incentive to maintain outmoded equipment in this circumstance is that the application software and/or data in question still performs a useful role, at a suitable performance level, or must be maintained for record keeping purposes. Again, in this instance, the study team was told that redevelopment of the software would involve a cost that the Agency or project in question preferred not to bear.

A further reason for the retention in service of outmoded infrastructure is the need to interface with specialised interface cards that have been designed to interface with outmoded ISA bus technology and in many instances must operate in 8 bit mode. More recent technology mandates 16 or 32 bit operation.

Outmoded IT equipment is also being retained if timing issues associated with sensing devices are critical and current technology is unable to operate slowly enough to permit correct error free data collection from this equipment. The study team observed the continued use of Zylog Z80 chips, Intel 8088, 80186, 80286, 80386, 80486 and 80586 chips to support this need. Most commonly, the use of this hardware involves the use of versions of the DOS operating system.

The need to accommodate the use of outmoded equipment has resulted in a practice of "trickling down" equipment. When equipment becomes too outdated to use for general research purposes, it is often recycled to use as the IT component of instrumentation. An accompanying practice is to place decommissioned equipment in storage to facilitate the cannibalisation process.

Potential Treatment

To the extent outmoded equipment supports instrumentation, the study team considers that PCs (irrespective of age or uniqueness of operating systems) whose only function is to operate or support a scientific instrument may be treated as an integral part of the scientific instrument. To the extent that such a PC is re-deployed from operating a scientific instrument to some other purpose, at the time of redeployment, the PC is in scope and should be treated in the same manner as a 'new' PC being installed in the Agency IT environment. If a PC is attached to an instrument and the function of that PC is to collect, analyse and distribute data through the network, that PC should be treated under model 1. In the event that user requirements are such that system superuser access is required the system should be treated under Model 2.

In some circumstances, outmoded equipment is being maintained to support old applications and to enable access to old data. To the extent that outmoded equipment used in this manner does not have extensively modified hardware and/or operating systems, it would fall into the presumptive model. To the extent there are extensive modifications, the equipment may fall into Models 2 or 3.

4.3.3 Use of specialised or specific operating systems

The study team observed several instances where systems used in support of scientific instruments required the use of unusual, specialised or specific operating systems. (See also section 4.4.4) Most commonly, the operating system employed is determined by the manufacturer of the instrument and, in the cases observed, change in the operating system has the potential to render the instrument unusable.

Operating systems seen to be in use in the circumstances described were:

- MacOS;
- DOS (in many variations);
- Microsoft NT;
- OS/2;
- OS9;
- Linux;
- VMS;
- HP-UX;
- SunOS; and
- Solaris.

It was not unusual to see a laboratory with four or five of these operating systems represented and commonly they were represented in differing versions.

Potential Treatment

PCs (irrespective of age or uniqueness of operating systems) whose only function is to operate or support a scientific instrument may be treated as an integral part of the scientific instrument. To the extent that such a PC is re-deployed from operating a scientific instrument to some other purpose, at the time of redeployment, the PC is in scope and could be treated in the same manner as a 'new' PC being installed in the Agency IT environment. If a PC is attached to an instrument and the function of that PC is to collect, analyse and distribute data through the network, that PC should be treated under model 1. In the event that user requirements are such that system superuser access is required the system should be treated under Model 2.

4.3.4 Real time data acquisition and feedback control

The need to perform data acquisition and feedback control in a real time environment has resulted in the use of several operating systems that facilitate this need more simply than

operating systems such as the Microsoft Windows and NT family of operating systems that rely upon virtual machine capability. This has resulted in the proliferation of operating systems such as:

- DOS;
- QDOS;
- Linux;
- LynxOS; and
- QNX in this area.

Older, simpler, operating systems such as DOS are used because it is fairly easy to access hardware devices and to catch interrupts. This can be done in more modern systems by writing device drivers but the task is more complex. It was also common that the operating systems used were modified at the kernel level to enable them to function in the desired manner.

Systems that need to guarantee response times, such as controlling a robot arm, often use specialised real-time operating systems. These are a distinct class of systems, quite different from normal desktop operating systems.

In most cases seen by the study team, the writing of the drivers and control programs for these instruments is a task undertaken by the scientists and their technical support people, commonly from the IT group. Supporting these systems requires knowledge of the science and detailed knowledge of the computing technology.

This area gave rise to the most frequent occurrence of the use and maintenance of outmoded hardware and operating systems.

The needs of real-time data acquisition and feedback control in research experiments give rise to a large diversity in hardware and software. It also is an area that gives rise to the greatest need for those involved in support of infrastructure to have a good understanding of the science involved (the business process).

In general, however, the systems once configured tend to be stable and do not require frequent change, update or tuning. Agencies retain these systems because they enable direct access to hardware devices, and they provide guaranteed response time to external events rather than because there is a disinclination on the Agency's part to upgrade. These systems have the added benefit of being quite reliable.

Potential Treatment

PCs (irrespective of age or uniqueness of operating systems) whose only function is to operate or support a scientific instrument may be treated as an integral part of the scientific instrument. To the extent that such a PC is re-deployed from operating a scientific instrument to some other purpose, at the time of redeployment, the PC is in scope and could be treated in the same manner as a 'new' PC being installed in the Agency IT environment. If a PC is attached to an instrument and the function of that PC is to collect, analyse and

distribute data through the network, that PC should be treated under model 1. In the event that user requirements are such that system superuser access is required the system should be treated under Model 2.

4.4 The need for access to operating systems and hardware

4.4.1 Software development

Several Agencies are engaged in software development under contract to commercial and other external organisations or for their own production purposes. Most software development processes require developers to have access to the operating system. Additionally these areas need to be able to change their operating environment. Often this includes modifying the operating systems and interfaces to match a client's environment.

Industry practice is to segregate developmental environments from production environments. Developers (with the exception of the mainframe environment) usually have superuser access to the development environment. Increasingly superuser access to particular functions within a system are controlled through the use of applications such as SUDO. These applications enable users who have a legitimate need for limited superuser access to systems to be granted that access without compromising overall system security. In addition applications such as SUDO maintain an audit trail of the users who do use superuser access.

Potential Treatment

There are two approaches that accommodate users' need to have access to the operating system. Both approaches are variations to the presumptive model of IT outsourcing. Flexibility to retain Agency access to operating systems are the same under both approaches, but the applicable service levels and the resulting incentives are different (see also Section 3.1.2).

The presumptive model is used in the first approach. The outsourcer is responsible for support of the system up to and including support and maintenance of the operating system. However, the Agency retains the right and the discretion to access system software, including the operating system, at any time. But, if the user's action result in an outage in the system the outsourcer will be relieved of service level requirements only for that particular outage. Regardless of the cause of any outage, the outsourcer must restore the system following any outage, subject to service levels relating to problem resolution. The benefit of this approach is that the outsourcer is responsible for the performance of the entire IT&T environment and except for exclusions resulting from Agency actions, service levels are guaranteed.

In the second approach, the outsourcer is responsible for the procurement, maintenance and support of IT hardware and the procurement, installation and upgrading of operating systems (model 2). The agency retains responsibility for support and maintenance of operating systems. A different service level regime operates under this approach. Service

levels for system availability are treated as targets not guarantees because the outsourcer does not have control over the entire IT&T environment. Regardless of the cause of any outage, the outsourcer must restore the system following any outage, subject to service levels relating to problem resolution..

The study team recognises that using the presumptive model gives an Agency the benefit of obtaining end to end accountability. It may also result in lower overall costs to an Agency. (A further discussion of the benefits of the first approach is located in Section 3.1.2.) As a result, Agencies may prefer the presumptive model. However, to the extent that users are constantly accessing the operating system, Agencies may prefer to use variation 2. The use of this variation lessens the potential for disputes over accountability by relieving the outsourcer of any responsibility for maintaining system availability.

4.4.2 Frequent environment reconfiguration

In some of the areas visited, particularly those involved in software development, the study team found that users need to have the freedom to reconfigure their operating environment. In certain cases reconfiguration is driven by the need to replicate a client's environment in order to develop software or hardware to suit that client's needs. This could involve the use of non-current operating systems or operating systems with varying levels of patch upgrades applied. Environment reconfiguration exists both in the UNIX environment and in the Microsoft NT environment. Often reconfiguration includes the need to change interface cards in the system.

The degree of access is dependent on the actual needs of the user. As a result, some reconfiguration may be done in conjunction with services provided by an outsourcer and more complicated configurations may significantly limit the outsourcer's involvement.

Potential Treatment

The presumptive outsourcing model provides wide flexibility to maintain unique configurations of IT hardware and software, and the requirement for a non-standard configuration per se does not dictate any other treatment. Depending on the degree and frequency of user access to operating systems, Model 2 treatment may be appropriate. If a particular installation requires frequent hardware and software configuration changes, Model 3 treatment may be appropriate.

4.4.3 Hardware experimentation

Several areas visited in the course of the study were involved in the development of hardware solutions, either to support scientific experimentation or in response to commercial contract. The experimentation observed involved either the mixing and matching of commercial hardware products with a view to finding optimal solutions or the design and fabrication of components to achieve a solution.

In some instances solutions were being developed to permit the use of PC functionality in highly specialised form-factors for use in particular industrial applications. In several instances the study team saw developmental work on the "ruggedisation" of IT equipment to enable it to withstand extreme conditions. In another instance the study team observed the "rendering safe" of IT equipment to enable its safe use in a potentially explosive atmosphere.

There were other areas visited where the nature of the work involved dictates the hardware configuration of the system used. As such users require the ability to specify particular componentry to be included in the hardware configuration.

Experimentation and research carried out on IT infrastructure implies a high level of interaction between hardware and operating systems. It implies the need to make frequent changes to system configuration. In the event that an experiment fails to operate as expected, damage to the hardware may occur. The product of the experiment may also render the hardware unrecognisable.

Potential Treatment

Obtaining service level undertakings from contractors in relation to the performance of hardware and operating systems where Agency personnel are conducting research of this type is unlikely to be possible. However considerable potential remains for outsourcing the procurement of required conventional IT hardware and software. The procurement of electronic componentry is not envisaged to become part of an outsourcer's responsibilities. As a result equipment and/or systems of this nature may fall into Model 3.

4.4.4 Infrastructure configuration modification

Agency needs have resulted in significant diversity in the use of IT infrastructure. To this end the team discovered that a large number of scientists have frequent need to modify the hardware configuration of their machines (through changing interface cards), the operating systems (through use of operating system patches), device drivers, (many of which are written by the researcher), and script files used to control the behavior of applications that are to run on the systems. It should be noted, that the need for a specialised network interface card is not the same as modifying the infrastructure.

The modifications described in this Section may result in the system becoming singular and not conforming with general industry standards.

Potential Treatment

When there is a need for access to both hardware and operating systems for the user to carry out his or her required functions, the IT equipment/system may fall into Model 2 or Model 3.

4.4.5 Multiple operating system environments

On several occasions the study team was shown systems configured with multiple operating system environments. This commonly involved the use of more than one of Microsoft Win 3.1, Win 9x, NT and Linux in the same machine. This situation exists primarily to facilitate the use of PC equipment with specialist software that is sourced from differing suppliers and is used in data processing in the research environment. The object of the multi boot environment is to make the required environments available for a minimal hardware cost.

Potential Treatment

This requirement will have to be taken into account in developing the RFT. This requirement requires additional expertise on the part of the outsourcer, but there is no reason the need cannot be met. The use of multi boot machines is becoming common in areas outside of the science industry. Depending on the exact use of the equipment, the outsourcer could provide a fully supported machine with multiple operating systems installed and the equipment would fall into Model 1. To the extent regular modifications to the operating systems are also required, the equipment may fall into Model 2. The study team noted that other projects in the Initiative have required multiple boot configuration.

4.4.6 Network experimentation

The study team noted that some CSIRO research teams are involved in network related research. This raises the following issues for outsourcing.

In one case, a team is developing and proving modifications to the way in which the Internet Protocol is used. Although much of this work is being conducted over a logically separated portion of the network, a significant part of the testing process is dependant upon being carried out in a production working environment. This experimentation involves the generation by the research team of extremely high bandwidth loading of the network and has the potential to seriously affect overall network latency or even cause complete failure of the network.

Experimentation may also involve the development of intellectual property. CSIRO may develop the intellectual property for its own use or on behalf of a client. CSIRO has raised a concern that the use of an IT infrastructure service provider will create certain issues. Specifically, CSIRO is concerned that the outsourcer would have access to the intellectual property and may use it improperly. In addition, CSIRO raised the concern that post-outsourcing, its commercial partners will no longer want to engage CSIRO due to the perception that CSIRO no longer controls access to intellectual property and other confidential information.

An example of this situation is in the Telecommunications and Industrial Physics area of CSIRO and involves the MARSHNet LAN. MARSHNet connects four sites, Lindfield, Marsfield, North Ryde and a site at the Macquarie University. At the Marsfield site there is a sub network that has been constructed as an experimental site. This experimental site has implemented "virtual path configuration" by the creation of virtual switches within single ATM switches. The virtual path configuration is valuable commercial information. Because the outsourcer could be in the business of providing IT&T solutions, CSIRO is concerned that its information may be used improperly by the outsourcer.

Potential Treatment

The two issues raised by CSIRO are:

- the continuation of an Agencies' ability to access the IT&T environment with the potential for Agency induced outages; and

- the need to protect confidential information, including intellectual property generated by CSIRO for itself or on behalf of a client.

Agencies needs can be addressed through the use of the general exclusions in the service level schedule which excuse an outsourcer from service level obligations arising from outages caused by Agency personnel. The outsourcer remains obligated to restore the system to function. See section 3.1.2 for a complete description of this approach.

The protection of confidential information, including intellectual property, is discussed in section 4.7.4.

4.4.7 BOM applications support fault diagnosis

BOM has advised that it is the current practice for staff involved in applications support of operational systems such as AIFS, the message switch, satellite systems and real time databases to have root access to the machines that are supporting those applications. BOM views these applications as being critical to its operations. They are developed in-house, are complicated, make extensive use of system resources and require a high standard of support.

Applications support staff use root access to enable quick diagnosis of the causes of failure and to allow immediate application of remedial steps. Remedy commonly involves the need to make changes to system resources.

BOM operates 24 hours per day, seven days a week. Because these systems are critical to BOM's operations, BOM currently has applications development support staff on call 24 hours a day in the case of failure of the systems

Potential Treatment

The systems identified as supporting the BOM's operational applications have been described as consisting of off the shelf hardware configuration and operating system. As such these could be expected to fall into Model 1. However, the extent or frequency of a user's need to access the operating system may result in modified treatment.

There are two approaches that accommodate users' need to have access to the operating system. Flexibility to retain Agency access to operating systems are the same under both approaches, but the applicable service levels and the resulting incentives are different (see also Section 3.1.2).

The presumptive model is used in the first approach. The outsourcer is responsible for support of the system up to and including support and maintenance of the operating system. However, the Agency retains the right and the discretion to access system software, including the operating system, at any time. But, if the user's actions result in an outage in the system the outsourcer will be relieved of service level requirements only for that particular outage. Regardless of the cause of any outage, the outsourcer must restore the system following any outage, subject to service levels relating to problem resolution. The benefit of this approach is that the outsourcer is responsible for the performance of the entire IT&T environment and except for exclusions resulting from Agency actions, service levels are guaranteed.

In the second approach, the outsourcer is responsible for the procurement, maintenance and support of IT hardware and the procurement, installation and upgrading of operating systems (Model 2). The agency retains responsibility for support and maintenance of operating systems. A different service level regime operates under this approach. Service levels for system availability are treated as targets not guarantees because the outsourcer does not have control over the entire IT&T environment. Regardless of the cause of any outage, the outsourcer must restore the system following any outage, subject to service levels relating to problem resolution.

The model employed under these circumstances will depend on, among other facts, how frequently BOM personnel need access to the operating system, whether there are methods to control access and the desired service level/incentive regime. A risk exists in allowing the sharing of the root user password on these systems in that it is not possible to maintain a valid audit trail in relation to changes that are made to the system/s. Additionally uncontrolled use of root access provides those who do have these privileges with the opportunity to remove or alter any audit trails that do exist on the system to conceal use of the privileges. Software tools exist in the UNIX environment that enable the maintenance of suitable audit trails of the use of root or superuser powers. BOM advises that the SUDO product has been trialled without success, however this tool is in common use with other agencies within Group 9. Given the sensitivity of BOM to the reliability of their production operational systems and low tolerance to system down-time, the practice of sharing the root user password presents a serious risk exposure to operational integrity. BOM may want to explore with the ultimate vendor, whether there is an access control system that would meet its needs and reduce the level of risk resulting from multiple user access to the operating system. The approach BOM takes to operating system access will determine the Model that should be applied to these systems.

4.5 Third party equipment

4.5.1 Accommodation of visiting staff and equipment

Most Agencies are constantly hosting persons who are not formally part of the organisation, who bring IT infrastructure with them and who may require connection to the Agency network facilities. The persons involved provide their own, often specialised equipment and

for the period of their visit often require IT infrastructure support. Examples of such individuals are:

- Visiting scientists (often from international origin and may require systems operating on character sets other than the standard ASCII, for example the Japanese Katana character set);
- Graduate students; and
- Representatives of organisations involved in joint ventures or other collaborative efforts.

Some of the Agencies also have IT equipment that is provided by third parties for the conduct of research or experimentation. Again, this equipment may require connection to the Agency network facilities.

IT Infrastructure and instruments that are brought to Agencies by visiting scientists and students is supported in varying degrees by Agencies. The extent of Agency support required by these visitors can range from conventional support of a laptop with administrative/desktop functions to specialist support of scientific and research instrumentation and applications.

The length of stay this equipment may have at the Agency varies from several days to a year or more.

The connection and support of "visiting" IT equipment may present issues to a potential outsourcer in that the "visiting" equipment may be unfamiliar in terms of hardware, operating system and applications. This is no different than the current situation. However, potentially the outsourcer may have a greater ability to deal with "visiting" equipment through identifying the capability to deal with it in another area of its organisation.

Although not specifically identified to the study team as an issue, if equipment to be connected to the network is significantly different in form or use it may affect the performance of the network. Presumably such an occurrence would be unusual, but if it occurs it may relieve the outsourcer from service level requirements.

Potential Treatment

Generally, if requested, the outsourcer would be able to provide support of the visitor's IT equipment and facilitate and support any networking needs. This is contemplated in Model 4.

4.5.2 Collaborative arrangements

The ownership structure of IT infrastructure in Group 9 Agencies involved in collaborative ventures include:

- Full ownership of IT infrastructure by Agencies;
- Lease of IT infrastructure from third party vendors;
- Donated IT infrastructure, with ownership vesting in Agencies;

- 'In-kind' contribution from private or public sector partners as part of a Co-operative Research Centre (CRC), joint venture or contractual arrangement;
- IT infrastructure which are on loan for varying periods as part of a CRC, joint venture or contractual arrangement; and
- Joint ownership between the Agency and a third party of IT infrastructure.

Several of the Agencies visited are involved in CRCs. These are most commonly run in conjunction with commercial entities or with State Government bodies. Frequently IT infrastructure will be jointly owned and in many cases the IT infrastructure is provided as an "in kind" contribution for the furtherance of the research activity.

Frequently Agencies provide support services for the infrastructure as part of that Agency's contribution to the CRC, joint venture or contractual arrangement. The IT infrastructure which are part of the collaborative arrangements could be located on Agency premises, or at third party premises and the IT infrastructure support services would be provided at those locations.

Potential Treatment

In the cases where an Agency is providing IT infrastructure support services to a collaborative arrangement it would be expected that an outsourcer would provide those same services. In general, Model 1 would apply unless other considerations discussed in this Report apply.

4.6 Discussion of other significant equipment and systems

4.6.1 Supercomputing/processing

CSIRO and BOM are both users of machines commonly described as "supercomputers". The term is essentially colloquial and is generally taken to mean high-end machines that have a design emphasis upon high-speed numerical processing power. These machines exist in two main architectures being the "shared memory" model and the "distributed memory" or Beowulf Cluster model. Examples of the "shared memory" models seen were the, now outmoded, Cray computers that use the UNICOS operating system and the NEC supercomputers that use the SUPER-UX operating system. Examples of the "distributed memory" machines seen were either clustered high end PC machines (with clusters of up to 16 machines used in these Agencies) running on Linux or clustered Compaq Alpha machines running on the True 64 operating system. Each of these systems have operating requirements peculiar to the concept of supercomputing that requires sophisticated modification to operating systems and network connections between component machines to enable use of scheduling procedures to effectively utilise available CPU time thus maximising system throughput.

Currently all applications running in the supercomputing environment are developed in-house.

An observation made by the study team was that there is an apparent wide-spread need among the Agencies in Group 9 for increasing amounts of computing power to enable processing of large data models. This was obvious in the various areas dealing with Computational Fluid Dynamics, mining research and atmospheric studies. Whilst BOM and CSIRO have pooled resources in the operation of the NEC SX4 and NEC SX5 supercomputers, there would appear to be scope for further increasing available supercomputing resources to areas that currently could not support this cost on their own. It is possible this need could be addressed through the outsourcing process.

Possible Treatment

The NEC SX4 and NEC SX5 are complex machines and the existence of a viable market for operation and support of such machines in Australia cannot be determined unless the tender process is undertaken.

The most flexible approach to the tender process as it relates to the NEC SX4 and NEC SX5 would be to include the machines in scope under Model 1, subject to withdrawal if the technical solution and/or business case of the bids are not viable in the context of the entire project. The RFT could also be drafted to permit tenderers to submit a bid that will not be considered "non-compliant" if it does not provide support for the NEC SX4 and NEC SX5. This approach would ensure that the inclusion of support for a complex computing environment in the Group 9 business does not preclude a robust competition for the bulk of the Group 9 business.

The Beowulf Clusters are a different case. The modifications to the operating systems and network connections (used internally to the cluster) make the Beowulf clusters more akin to the systems discussed under infrastructure configuration modification (Section 4.4.4) than supercomputers. As a result, the Beowulf Clusters might be treated substantially in accordance with Model 1, 2 or 3, depending upon the level and frequency of user access to the hardware and systems software that is required.

4.6.2 AARNet, LAN and WAN

CSIRO is a member of the consortium that owns and operates the Australian Academic and Research Network (AARNet). AARNet provides internet services between eight state and territory based Regional Network Organisations (RNOs). The RNOs are unincorporated joint ventures whose participants are the AARNET members located in that particular region. The RNOs act as the hub for the AARNet members located in each region. Each participant in AARNet links to the network through the RNO in its region. CSIRO is located in every region and thus is linked to every RNO.

Ownership of AARNet is vested in the consortium and CSIRO is a one/thirty-eighth member of the consortium. CSIRO owns the LAN/WAN infrastructure located at its sites and the infrastructure that links CSIRO sites to the RNO. The connections to the RNOs are a mixture of microwave links, frame relay links, ISDN links and fibre optics links. The links connect to a "gateway" router that is owned by the RNO.

CSIRO uses AARNet to provide its WAN backbone. The LAN in each CSIRO site is linked to AARNet to create the data network for all CSIRO facilities.

AARNet is a research network and is also used for voice communication among the members of AARNET. The voice communication is provided through the use of voice over IP developed by CSIRO. CSIRO considers the voice over IP technology to be the intellectual property of CSIRO and that it is not available on the commercial market.

ANSTO is also commected to AARNet and uses its AARNet connection for Internet access. ANSTO may desire to use AARNet for its voice communications in the future.

The other Agencies in Group 9 are not members of AARNet and while ANSTO has signed the AARNet Access Agreement to obtain Internet access, AARNet does not constitute ANSTO's LAN or WAN facilities. As a result, there were no reasons presented for why the LAN or WAN of the other Group 9 Agencies require special treatment in the outsourcing process.

Potential Treatment

The ownership structure of AARNet dictates that AARNet cannot be outsourced under the Initiative. The study team considers that the point that the infrastructure changes from CSIRO owned infrastructure to AARNET or RNO owned infrastructure (the "gateway") is the point at which the CSIRO WAN/LAN becomes out of scope. From the gateway inward, the CSIRO LAN should be treated under Model 1, subject to the discussion of confidential information in Section 4.7.4.

Because the software used to provide voice over IP to AARNet is the intellectual property of CSIRO, the in scope portion of the LAN requires special treatment. The study team considers the use of voice over IP technology by AARNet is functionally equivalent to a software producer providing software subject to a licence. Presumably, CSIRO has already entered into some sort of arrangement that protects the use of its voice over IP technology by the other members of AARNet. The study team proposes that the same approach could apply in the situation where an outsourcer is responsible for the operation of the LAN. Strict constraints on the use of the voice over IP technology would be put on the outsourcer that would operate in a similar fashion to a software licence. The legal advisers should be tasked to ensure that the intellectual property provisions of the IT outsourcing contract provides adequate protection of CSIRO's intellectual property.

4.6.3 Large volume data repositories

All Agencies involved in Group 9 have vast accumulations of scientific data and continue to acquire data on a daily basis. Most of this data is required for future analysis and re-use and as such must be maintained in a manner that the data will remain accessible and its integrity maintained.

Some examples were shown to the study team where BOM data was re-analysed, after a twenty year time lapse, and using current technology, revealed valuable information that had gone undiscovered previously.

Different Agencies have taken differing approaches to archiving this data and in some cases the long term viability of the data concerned is at risk. Data stored on magnetic medium is prone to atrophy if it is not exercised on a regular basis. The exercising of large amounts of data stored on DAT tape, for example can be an expensive and time consuming task. Similarly data that is stored on tape can be difficult to access, particularly of there is a significantly large amount and the technology employed does not facilitate mass data retrieval.

AGSO advised the study team that it is interested to implement a new technology platform that encompassed PC based access to a central data repository.

Potential Treatment

Data repositories serving the mass data storage requirements of all Agencies should be pursued through the tender process under Model 1. This would ensure professional care was taken to maintain integrity and availability of the data when it is required. The study team noted that other projects under the Initiative have included similar mass storage requirements.

4.6.4 BOM mass data store

The study team was shown a StorageTek silo that is central to computer operations at BOM. This machine is critical to the successful processing of the operational data within BOM. It acts as a data buffer for output from the NEC Super computer and a general data repository for data generation on other BOM machines.

Potential Treatment

This machine is vendor standard and is supported by the vendor. An outsourcer would be able to support the machine with assistance of the vendor if required in accordance with the presumptive model.

4.6.5 Australian Telescope National Facility

CSIRO has the responsibility for the provision and management of the Australian Telescope National Facility. This facility consists of major radio telescope installations at Narabri and Parkes and minor telescope installations at Canberra and Mopra. A site at Marsfield in Sydney serves as headquarters.

Use of the facility is not exclusive to CSIRO and is made up of 40% use by scientists from overseas, 40% use by non CSIRO Australian scientists and 20% use by CSIRO staff. CSIRO staff currently provide IT support services to visiting scientists.

The facility operates 24 hours per day every day of the year. As a result, CSIRO have identified the need for IT support services at least on an on-call basis 24 hours a day.

Overall in the complete facility (including the Marsfield site) the facility uses the following infrastructure:

- 155 "WINTEL" workstations;
- 122 Unix/VMS workstations;
- 40 computers used in real-time instrument control; and
- networking infrastructure to support their operation and link the telescopes to the Marsfield headquarters.

A further breakdown of machines located at the Parkes and Narrabri sites are as follows:

Machine Type	**Parkes**	**Narrabri**	**Totals**
WINTEL	28	44	72
UNIX/VMS	25	24	49
Realtime Control	6	15	21
Totals	59	83	142

Most applications utilised both in the control of the telescopes and in the analysis of collected data are written and maintained in-house.

In this area scientists who are using UNIX based machines for data analysis and synthesis imaging processes commonly have office automation software installed on these machines to facilitate documentation and communication functions as well. Some of the machines are also used for software development and maintenance. The machines use vendor standard hardware and operating system configurations.

The facility, at Marsfield, includes an "Electronics and Receiver" group whose role is the development of experimental receivers and integrated circuit chips. This process involves the modification of IT hardware and operating systems and requires development staff to have routine access both to the hardware and to the operating system to allow modifications. The electronics group maintains a private network that is "bridged" to the main CSIRO network. Currently the electronics group performs its own IT support inside the "bridge".

Some additional issues identified by CSIRO in relation to the Telescope Facility infrastructure are:

- The need for computer support staff to have a good working knowledge of the radio astronomy process and operational safety issues associated with the large antennae and antenna arrays to be able to provide adequate support;
- The need for applications support personnel to have root/administrator access to machines supporting the applications;
- The need for networking and computing hardware to be specified with as low Radio Frequency Interference (RFI) as is procurable;

- The need for highly customised/specialised interface between the realtime control computers and the antennae. This interface utilises in-house developed chip technology; and
- Some image processing is carried out using on-line data received directly from the antennae. This is experimental involving the development of software. Staff involved in this exercise are required to have an intimate knowledge of the instrument, astronomical theory, and software techniques. Given the developmental nature of this work and the requirement for staff to have routine access to superuser privileges in relation to the machines involved these machines would be best catered for under Model 2.

Potential Treatment

Both the administrative desktop machines and the UNIX and VMS workstations used for the analysis of data and the synthesis of images are industry standard machines with industry standard operating systems even though they may support highly specialised applications. As such these machines would fall into outsourcing Model 1.

There are two approaches that accommodate users' need to have access to the operating system. Flexibility to retain Agency access to operating systems are the same under both approaches, but the applicable service levels and the resulting incentives are different (see also Section 3.1.2).

The presumptive model is used in the first approach. The outsourcer is responsible for support of the system up to and including support and maintenance of the operating system. However, the Agency retains the right and the discretion to access system software, including the operating system, at any time. But, if the user's actions result in an outage in the system, the outsourcer will be relieved of service level requirements only for that particular outage. Regardless of the cause of any outage, the outsourcer must restore the system following any outage, subject to service levels relating to problem resolution. The benefit of this approach is that the outsourcer is responsible for the performance of the entire IT&T environment and except for exclusions resulting from Agency actions, service levels are guaranteed.

In the second approach, the outsourcer is responsible for the procurement, maintenance and support of IT hardware and the procurement, installation and upgrading of operating systems (Model 2). The Agency retains responsibility for support and maintenance of operating systems. A different service level regime operates under this approach. Service levels for system availability are treated as targets not guarantees because the outsourcer does not have control over the entire IT&T environment. Regardless of the cause of any outage, the outsourcer must restore the system following any outage, subject to service levels relating to problem resolution.

The realtime control systems associated with the antennae present a different problem in that the hardware and communications interface to the antennae is customised and some additional skills appear necessary in relation to the safety of operation of the antennae. Additionally these machines are based on the PSOS real time operating system and use in

house developed and built interface boards and protocols to interface with antennae servo motors. It appears that Model 3 may provide the necessary flexibility for scientific staff to retain control of the operation of the antennae but to still have access to assistance from the outsourcer in support of the hardware and operating system on an as needed basis.

The use the Electronics and Receiver Group have for IT infrastructure places it in a similar situation to that found in the TIP electronics development area at Marsfield. Full support of equipment is currently provided from within the group without assistance from the computer support group. Currently the boundary for normal support has been defined to be the "bridge" machine used to connect the Electronics and Receiver Group sub network to the rest of the CSIRO LAN. If these machines were to be placed into Model 3 or 5 this arrangement could be continued with the added value that the Electronics and Receiver Group could seek assistance in support for hardware and operating systems on an as needed basis from the outsourcer.

4.7 Other relevant issues

4.7.1 Educational and other discounts

Agencies have advised the study team that they obtain significant academic and other discounts from IT&T vendors. Agencies believe these discounts may be put at risk if their IT infrastructure is outsourced. Examples of the advantageous pricing that Agencies have secured include:

- CSIRO Corporate has around 48 IT contracts, some have consortia or academic pricing. There is a concern that CSIRO may lose their academic status as a result of outsourcing which may result in higher costs.
- Some hardware and software products are supplied to CSIRO in return for joint research or the potential that CSIRO may eventually determine to purchase additional equipment. In some cases this relationship allows CSIRO to have input into the development of the products.
- BOM as a national meteorological organisation and as a contributing partner to the World Meteorological Organisation (WMO) obtain special pricing for software. BOM is also concerned that IT outsourcing may put at risk its status under the WMO and increase costs.
- ANSTO receive academic pricing on hardware and software from a number of suppliers.

Potential Treatment

Under the Initiative, the aggregation of Agencies IT requirements improves Agencies' ability to leverage the scale and volume of requirements beyond that which is normally available to a single Agency. In addition, irrespective of the size of any single Agency and its purchasing power, an IT outsourcer, particularly one with worldwide affiliations, will have greater purchasing power based on the aggregation of its global business requirements. As a result, discounts secured by Agencies for IT products may be able to be matched or exceeded by an outsourcer. However, in the event that an outsourcer cannot secure pricing as good as

that obtained by an Agency, the IT outsourcing contract provides for the following flexibilities.

IT&T hardware
Under the IT outsourcing contract, Group Agencies retain the freedom to source the supply of IT&T hardware from third party suppliers if pricing from the outsourcer is un-competitive.

Third Party Software
For previous IT outsourcing transactions, the outsourcing contract specifies various possible options for the treatment of third party software. These options permit the financial benefits of any current licensing arrangements to be maintained after outsourcing (if necessary by Agency retention of existing licenses). The appropriate option that would apply for each item of Agency third party software would be dependent on the economics of the outsourcer's proposal compared with the current contractual arrangements that Agencies have with software suppliers.

4.7.2 Early adopter positioning

In certain areas of the Agencies, the need to take advantage of leading edge or beta technology was emphasised to the study team. In some cases Agencies have arrangements with manufacturers to provide early release or pre-release of hardware or software. A discussion of one aspect of these arrangements is located in the Section on educational and other discounts (Section 4.7.1 above). The ability of an outsourcer to source equipment or software prior to its release may be explored during the tender process. It may well be the case that large IT infrastructure service providers have an equal or potentially greater access than Agencies to pre-release goods due to their size and influence on the industry. In a previous IT outsourcing transaction, tenderers offered Agencies access to early release or pre-release technology as part of the benefits of the contractual relationship. The larger outsourcing service providers active in the Australian market indicated in the context of previous projects that they have existing agreements with major software vendors for pre-release versions of software that they could make available to Group Agencies.

The contract for services is non-exclusive. To the extent an outsourcer is unable to obtain access to technology, Agencies will still be able to obtain leading edge or beta technology, whether through purchase or some other arrangement, e.g.. the provision of equipment in return for testing. The adoption of any such technology in the IT&T environment and any changes to IT infrastructure that may be required will need to be subject to a technical change control framework that will be developed between the Agencies and the outsourcer during the transition period. Individual Agencies may want to establish policies that govern the procurement of technology outside the outsourcing contract.

4.7.3 Service levels

Agencies impressed upon the study team the need to maintain current service levels. Issues were raised in connection with the requirement that system and network "uptime" be

guaranteed. Reasons given for the required service levels relate to the business cost of failure and the community service cost of failure.

Business cost of failure represents the cost in terms of time. In particular, Agencies highlighted areas that conduct research or development that requires prolonged computational processes. Some computational runs extend over a period of months. Examples include Fluid Dynamics research and research undertaken in relation to the study of Genetics. If system or network failure occurs during the computational process, the process has to be re-run. Most commonly these extremely long computations have a means to minimise time lost in the event of network failure, however, the time lost may still be significant.

BOM cited the possibility of community service cost of failure arising in relation to weather model processing and the need to provide timely weather information to the Australian aviation industry. To the extent systems are not functioning, BOM is unable to provide information to its customers. This may result in the failure to release an extreme weather warning or the failure to provide the aviation industry with the information it needs to operate. In the former case, life may be at risk and in the latter case commercial loss may be significant.

Agencies expressed uncertainty about the ability of contractual obligations or financial penalties to deliver high levels of performance.

Potential Treatment

OASITO considers that requirements for high levels of service performance is not an issue of scope, but relates more to the capability and experience of the outsourcer to deliver the services. Agencies' requirements for the levels and standards of service performance will be addressed in detail as part of the drafting of the RFT. Assessments regarding the capability of tenderers to perform the IT&T services required by Agencies will be a major aspect of the evaluation of tenders.

4.7.4 Protection of confidential information

All the Agencies expressed concern over the protection of confidential information. The types of confidential information identified to the study team includes data, intellectual property, software, hardware configurations, the fact that a particular type of research is going on and the names of clients. The confidential information may be Agency confidential information or it may be a client's confidential information. Confidential information will also change over time. Some specific examples include:

- projects at CTIP in which the development of hardware (specialised cards or other items) is central to the research being done (see also section 4.4.6 on network experimentation);

- projects at CMIS that involve the use of confidential client data in the development of data mining tools;

- confidential medical records relating to AAD staff serving in the Antarctic; and

- voice over IP used within AARNet to provide voice communications to AARNet members (see also section 4.6.2).

Potential Treatment

The study team does not consider the existence of Agency confidential information to be sufficient justification for Agency IT infrastructure to be excluded from the scope of the Group 9 IT outsourcing. The following measures can be taken.

The Services Agreement used by the Initiative deals with confidential information in several ways. At the most basic level, there are provisions that protect all confidential information. These provisions restrict the access of outsourcer employees to confidential information and prohibit the use of confidential information for any purpose other than the outsourcer's performance of its obligations under the agreement without the written consent of the Agency involved.

Overlaying the contractual provisions, the outsourcer is required to comply with the *Privacy Act 1988* (Cth) as if it applied to the outsourcer in the same manner it applies to Agencies. Further, the outsourcer is required to abide by the privacy provisions in any legislation that affects or is administered by the Group. In each case, the outsourcer must ensure that all of its personnel comply with the foregoing requirements.

In the case of intellectual property, there are contractual provisions in the Services Agreement that deal with the protection of intellectual property. The provisions are generally drafted in the context of Agency intellectual property that is incidental to the services (e.g. modifications to device drivers, desktop images, macros and similar items). The intellectual property in use or to be developed by the Group 9 Agencies is not simply incidental and the Services Agreement will need to be re-examined to ensure an adequate level of protection. In some cases, the use of intellectual property may be functionally equivalent to using software subject to a license, e.g. the use of voice over IP on AARNet (see also section 4.6.2). In such circumstances intellectual property could be protected by contractual constraints that are similar to those found in licensing arrangements.

CSIRO identified certain areas where its concerns about the protection of confidential information are heightened. These are the areas where the research being conducted is in the same line of business as a potential outsourcer. Although CSIRO and the potential outsourcer may be competitors in these areas, it does not change the fact that the outsourcer is bound by the contractual provisions described above.

OASITO considers that concerns regarding the protection of confidential information can be appropriately handled in the context of the Services Agreement. The combination of the

foregoing requirements means that the outsourcer, its personnel and sub-contractors cannot use any confidential information or intellectual property, in whatever form and of whatever nature, for any purpose other than the provision of services pursuant to the services agreement. IT outsourcers are in the business of handling information, and it is a business imperative for them that that information remain confidential to the client. The outsourcer's reputation depends on their ability to guarantee the integrity and security of client information.

Irrespective of the contractual provisions that protect confidential information, CSIRO believes that clients, or potential clients, may perceive that CSIRO is no longer able to control the security or access of confidential information. As a first step, CSIRO can educate clients as to the mechanisms in place to protect confidential information. IT outsourcing is becoming a standard business management tool, and many Australian and international companies (some of whom may be clients of CSIRO) outsource their IT infrastructure. If this practice is acceptable for the client's own business, then whether or not CSIRO outsources its IT infrastructure should not an issue.

Each case must be examined on an individual basis. In some cases, it may be necessary to take additional measures. If a client is concerned about its confidential information, it may be appropriate to quarantine the client-related activities and the IT&T infrastructure it uses from the normal range of services provided by the outsourcer, with support and pricing modifications as negotiated at the time. The quarantine would apply for the period of the project.

The Agency would be responsible for the support and maintenance of the infrastructure for the duration of the quarantined activity. After this period, the quarantined infrastructure would revert to the full control and responsibility of the outsourcer. Alternatively, the services agreement would permit the Agency to remove affected equipment and services from scope when the conflict arises.

For new IT infrastructure which is required specifically for the quarantined activity, Agencies have a number of options. These range from:

- acquiring the new IT infrastructure and support from a third party;

- requiring the outsourcer to procure the IT infrastructure and own and manage the asset, with no additional support services from the outsourcer. The Agency would pay only for the rental of the equipment. This is similar to the arrangement for existing infrastructure; and

- the Agency taking responsibility for procuring, managing the asset, and supporting the IT infrastructure. At the conclusion of the quarantined activity, the infrastructure could be retained by the Agency and deployed to other functions, be sold to the outsourcer, or disposed of entirely.

The boundaries created by quarantining a project or activity would have to be determined on a case by case basis.

CSIRO has expressed that quarantine of such equipment and systems may have some undesirable side effects. The separation of equipment and systems may lead to some level of duplication of equipment as a result of running the quarantined area separately. CSIRO also feels that quarantine may limit the free flow of information that currently occurs. Despite the fact that CSIRO personnel will not be restricted from the exchange of ideas, CSIRO believes the procedures that would need to be put in place to guard against outsourcer personnel coming in contact with quarantined information would have a dampening effect on the sharing of information. CSIRO believes that if the size of the area quarantined is large enough (e.g.. site or building within CSIRO) the issue is lessened.

Most of the concerns relating to the protection of confidential information and intellectual property stem from a lack of trust on the part of the Agencies with a potential outsourcer. In the evaluation phase of the tender process, Agencies will have the opportunity to assess tenderers' technical and business capability to meet Agency requirements.

4.7.5 Maintenance of expertise

A concern voiced by each Agency is the potential loss of expertise. The concern is that when the maintenance and support of IT infrastructure is outsourced, and a corresponding reduction in personnel results, there will be a lack of expertise available within the Agencies to deal with issues relating to IT infrastructure that arise in the course of their activities. Among others, this situation could occur in the software development area when an applications developer would like the assistance or input of an IT infrastructure specialist to assist in determining the solution to a particular issue that arises as a result of the interaction of the software and the hardware.

The availability of IT infrastructure expertise will not necessarily be diminished, however, it will take a different form. In the first instance, expertise will be rendered by the outsourcer. Technical support of application development efforts including direct developer access to outsourcer technical support personnel (without going through the Helpdesk or any outsourcer 'filter' is included in the Services to be provided. Incidental, ad hoc support (in person, by telephone, or by attendance at meetings) is included in Service Charges. Only dedicated technical support of a development project would incur additional costs.

Depending on the needs of the Agency involved, the option of retaining some of the expertise in the form of Agency personnel may be available. Such personnel would no longer be responsible for the maintenance and support of the IT infrastructure, but the fact that an individual's current duties are in-scope does not oblige the Agency to declare that individual surplus to requirements upon outsourcing.

Although recognising that the Agencies could adopt this approach, a further concern arises. If Agency personnel do not engage in the maintenance and support of the IT infrastructure on a daily basis, their skills and knowledge of the IT system will gradually diminish.

4.7.6 Continuing flexibility to restructure divisions

Certain of the Agencies expressed a need to have the flexibility to restructure the operating units within the Agency and raised concerns over how changes in Government portfolios may be handled in an outsourced scenario. The needs expressed included the observation that certain of the Agencies may engage in joint ventures, cooperative research centres (CRCs), other collaborative ventures or even spin off operating units.

The contract for services, as developed by OASITO and its advisers, anticipates changes in the scope or volume of services provided. The contract permits Agencies to increase or decrease services to meet their changing needs. In addition to general provisions relating to such changes, the contract specifically states that Agencies may notify the outsourcer of changes including amalgamation with other Agencies, restructure of an Agency by the Commonwealth, movement of one Agency into another, changes in functions of an Agency, the performance of functions for another Agency and privatisation of an Agency or any part of an Agency. The object of the provision setting out the foregoing situations is to reflect the changing nature of Commonwealth Agencies and highlight particular situations that may be quite different from providing services to a private sector client. Irrespective of whether the change results from the foregoing causes, the Agencies have the right to adjust the nature of the services delivered.

The contractual provisions contemplate that where additional services are requested, they will be priced in accordance with an existing pricing mechanism or matrix. If one does not exist, pricing will be determined with regard to prevailing prices available in the market for similar services to like customers. The provisions allow the Agencies to ask for documentary proof that the pricing meets this criteria and also ensure that they reflect any cost savings resulting from any changes to the outsourcer's then current arrangements or operations. The exact content of the provisions in any particular contract will be subject to negotiation.

In the case of removal of services, the provisions tend to be the subject of greater negotiation thus causing the final outcomes to vary. However, the basic concept is that Agencies have the flexibility to remove any services and service charges will be reduced accordingly.

The pricing bands applicable to each service will be broad enough to accommodate most changes. However, to the extent an Agency is restructured, either to remove it from the group or result in a significant decrease in size, the change volume of services may be so large as to result in a change in the price of the services involved. For example, if the restructuring of an Agency results in an 50% decrease in the supply of services on desktop computers, the price of support services per desktop may increase by a designated amount.

In practice, these provisions provide sufficient flexibility for the circumstances that the Agencies brought to the attention of the study team. To the extent that an Agency is removed from Group 9, there would be a corresponding reduction in services and service

charges would be adjusted. If it exceeds any specified upper limit (as described in the preceding paragraph), the outsourcer may be entitled to some compensation. The same mechanism would apply to any other reduction in services required including if it results from a spin-off or other arrangement that would move functions performed by the Agency to a third party.

APPENDIX A – LOCATIONS VISITED BY STUDY TEAM

Agencies visited in the course of the Study were:

Location	**Agency**
Geelong	CSIRO Australian Animal Health Laboratories.
Parkes	CSIRO Australian Telescope National Facility.
Canberra	AGSO
Sydney	CSIRO Telecommunications & Industrial Physics Division,
Sydney	ANSTO
Brisbane	CSIRO Exploration & Mining, Pinjarra Hills; CSIRO Food Science, Cannon Hills
Cape Grim	BOM/CSIRO joint facility
Hobart	AAD
Hobart	CSIRO Marine Division AAD Aurora Australis
Sydney	BOM Sydney regional office
Canberra	CSIRO Entomology CSIRO Plant Industries
Canberra	CSIRO Corporate CSIRO Mathematics & Information Sciences
Melbourne	BOM head office
Melbourne	CSIRO Minerals Division, Clayton; CSIRO Manufacturing Sciences & Technology, Clayton
Melbourne	CSIRO Atmospheric Research, Aspendale; CSIRO Building Construction & Engineering, Hyatt
Cribb Point	BOM Satellite Ground Station
Wagga Wagga	BOM Remote Site Visit.
Canberra	CSIRO to discuss issues at Divisions not visited

APPENDIX B – IDENTIFIED ISSUES

Appendix B

Identified Issues

Discussion with scientific and research personnel in the areas visited resulted in the following list of issues arising from the Group's use of IT infrastructure that should be considered in implementing the decision to outsource under the Initiative (illustrative examples are meant to highlight these issues and are not an exhaustive list):

- Systems located in hazardous environments.
  ANSTO (Radio Pharmaceuticals, Reactor areas)
  CSIRO (Animal Health Lab, Plant & Industry and Entomology Quarantine Labs, Mining Operations)

- Systems located in remote areas.
  AIMS (Main Office)
  AGSO (Seismic Observatories and Geomagnetic observatories)
  AAD (Antarctic Stations further complicated by limited ability to travel to and between stations)
  CSIRO Radio (Astronomy Observatories)
  BOM/CSIRO (Cape Grim Atmospheric Observatory)
  BOM (Weather observation sites)

- Systems located in environments hostile to IT infrastructure.
  CSIRO/AAD/AIMS (machines required to operate onboard ship exposed to sea spray and sudden movement from ship's motion on rough seas.)
  CSIRO (Machines exposed to dust and jarring when deployed in mine environments).
  CSIRO (Plant and Industry and Entomology machines used in field work).
  CSIRO (Atmospheric research where machines are used in an airborne environment subject to jarring from the aircraft motion).
  AGSO (ANSIR equipment used in seismic field studies)

- System supports scientific instrument and is specified and coupled to the instrument and supported by the supplier.
  CSIRO (Electron Microscopes, Mass Spectrometers),
  AGSO/CSIRO (Mass Spectrometers, Mass Selective Detector),

- Interface with Scientific Instrument is such that outmoded hardware is required to support instrument.
  All Agencies have examples where scientific instrument is expensive and old and upgrade of interface is costly and time consuming. Outmoded hardware and operating systems are maintained to support such instruments.

  All Agencies where speed of current microchips is too great to support data acquisition interface hardware.

- The need to maintain outmoded operating systems to support outmoded hardware and applications.
  AGSO Black Mountain Paleomagnetic Laboratories.

- The need to access or process data created/stored in outmoded formats using outmoded information systems.

  ANSTO AUSANS machines where outmoded computers are retained to access data stored using outmoded applications.
  AGSO tape devices to read outmoded seismic data tapes.

- The need to retain outmoded hardware as a source of spares for outmoded equipment in use.

- Interface with Scientific Instrument is such that esoteric operating system is mandated
  CSIRO Entomology where several operating systems are maintained to support scientific instrumentation including Mac, NT, OS/2, OS9, Linux.

- Nature of scientific activity dictates "real time" data acquisition e.g.. LynxOS, and operating systems such as Win9X and NT do not have adequate system clock integration.
  AGSO QNX devices for geomagnetic observatories.
  CSIRO Robotics experimentation.

- Nature of Scientific activity dictates a particular mother-board and hardware configuration as a result of interface card interoperability or required system performance.

- The need for access to system internals for hardware, operating system and software modification for research, experimentation and application development and problem diagnostics and correction.
  CSIRO Mathematics and Information Systems (CMIS) software development and testing
  CSIRO Exploration and Mining group (Equipment Automation Group) development of robotic machinery.
  BOM AIFS & CMSS applications utilise X25 technology that requires superuser access for fault diagnosis and correction.

- The need to move machines from location to location.
  AGSO ("Bigfoot" seismic survey activity)
  AAD (Antarctic expedition activity)
  AAD (Ocean Research and data acquisition activity)
  AIMS (Ocean Research and data acquisition activity)
  BOM (Field PCs used in short term forecasting in Fire Weather conditions)
  CSIRO (Mines and other industrial research, Ocean Research and data acquisition activity)
  CSIRO (Atmospheric research where machines are placed in aircraft for research activity).

- "Visiting" machines
  AAD (Short term staff joining Antarctic Expeditions)
  Most Agencies host scientific gatherings and conventions and must support visiting IT infrastructure.
  Most Agencies host Post Graduate and Phd Students
  Cooperative ventures with private enterprise or other Governments and Agencies
  International Co-Operation

- Use of specialised and infrequently used operating systems.
  CSIRO Mining Robotics Research (LynxOS)
  Most Agencies have the need to modify and recompile operating system kernels thus creating non standard operating systems.

- The need for the availability of multiple operating systems in the same environment
  ANSTO/AAD/CSIRO have occasion to use Win3.1, Win9X, NT and Linux on single machines in multi-boot environment.

- The need for Researchers to be able to reconfigure machines with different operating systems and with differing versions of operating systems to match their client environments. Particularly noted in the case of:
  CSIRO (Mathematics and Information Science Division).

- The need for freedom for researchers to experiment in a production network environment.
  CSIRO (Telecommunications research MARSHNet)

- The need for network support to recognise real-time usage where ANY outage may have a significant impact upon the business process:
  AGSO(Earthquake and nuclear explosion monitoring network).
  ANSTO (Network Is an integral part of environment monitoring for HIFAR reactor which must be shut down if network fails).
  BOM (transference of met observations that has a short shelf life, e.g. data from Doppler Radar).
  BOM (Delivery of forecast warnings of severe weather conditions)
  BOM (Possible loss of data for climate archive)
  CSIRO (transference of data that is supporting complex processing that if stopped could represent the loss of significant time in recommencing the process).
  AAD (Communications and data transfer between Antarctic bases and Kingston particularly in the case of medical emergency)

- Equipment is used is part of Cooperative Research Centre or Joint Venture activity where ownership is not exclusively vested in the Commonwealth.
  CSIRO/AAD are supporting activity where hardware and or software are provided by sponsors of the particular research effort.

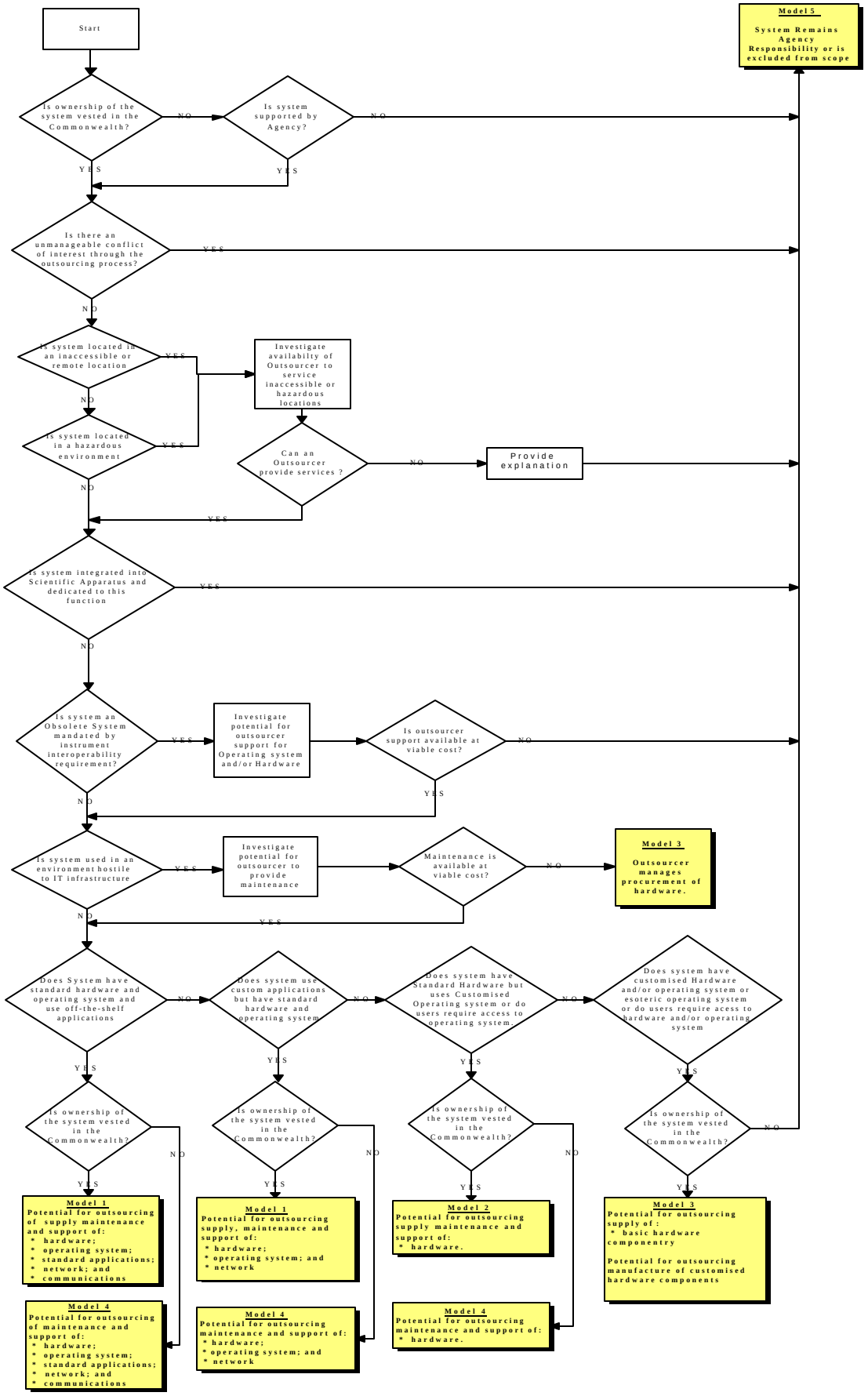
- The need to protect intellectual property concerning hardware, networking and software.
  CSIRO This concern is greatest where work is being carried out on a commercial basis for sponsors in private enterprise. An emergent property in relation to this issue is the potential for client loss as a result of perceived risk of intellectual property loss should the IT outsourcing process result on a competitor being contracted to provide IT infrastructure support.

- The need to protect confidentiality of data stored on systems in deference to commercial clients. In many cases this data exists in flat file format that cannot be intrinsically secured from system administrators.
  CSIRO (Mathematics and Information Science Division).

- The need to protect confidentiality of configuration of network hardware, software and firmwear where these are the subject of developmental research.

CSIRO (Telecommunications and Industrial Physics, Marsfield)

APPENDIX C – LOGICAL SCOPING SCHEMA


Start
Model 5
System Remains Agency Responsibility or is excluded from scope
Is ownership of the system vested in the Commonwealth?
NO
Is system supported by Agency?
NO
YES
YES
Is there an unmanageable conflict of interest through the outsourcing process?
YES
NO
Is system located in an inaccessible or remote location
YES
Investigate availability of Outsourcer to service inaccessible or hazardous locations
NO
Is system located in a hazardous environment
YES
Can an Outsourcer provide services ?
NO
Provide explanation
NO
YES
Is system integrated into Scientific Apparatus and dedicated to this function
YES
NO
Is system an Obsolete System mandated by instrument interoperability requirement?
YES
Investigate potential for outsourcer support for Operating system and/or Hardware
Is outsourcer support available at viable cost?
NO
YES
NO
Is system used in an environment hostile to IT infrastructure
YES
Investigate potential for outsourcer to provide maintenance
Maintenance is available at viable cost?
NO
Model 3
Outsourcer manages procurement of hardware.
NO
YES
Does System have standard hardware and operating system and use off-the-shelf applications
NO
Does system use custom applications but have standard hardware and operating system
NO
Does system have Standard Hardware but uses Customised Operating system or do users require access to operating system.
NO
Does system have customised Hardware and/or operating system or esoteric operating system or do users require acess to hardware and/or operating system
YES
YES
YES
YES
Is ownership of the system vested in the Commonwealth?
NO
Is ownership of the system vested in the Commonwealth?
NO
Is ownership of the system vested in the Commonwealth?
NO
Is ownership of the system vested in the Commonwealth?
NO
YES
YES
YES
YES
Model 1
Potential for outsourcing of supply maintenance and support of:
* hardware;
* operating system;
* standard applications;
* network; and
* communications
Model 1
Potential for outsourcing supply, maintenance and support of:
* hardware;
* operating system; and
* network
Model 2
Potential for outsourcing supply maintenance and support of:
* hardware.
Model 3
Potential for outsourcing supply of:
* basic hardware componentry
Potential for outsourcing manufacture of customised hardware components
Model 4
Potential for outsourcing of maintenance and support of:
* hardware;
* operating system;
* standard applications;
* network; and
* communications
Model 4
Potential for outsourcing maintenance and support of:
* hardware;
* operating system; and
* network
Model 4
Potential for outsourcing maintenance and support of:
* hardware.

APPENDIX D – OUTSOURCING MODELS.

Group 9 IT Outsourcing Models

Model 1 Fully outsourced IT infrastructure including desktop applications	Model 2 Feed & Care of IT Infrastructure	Model 3 IT Infrastructure procurement and management	Model 4 IT Infrastructure hardware support	Model 5 IT Infrastructure Agency responsibility
Procure/Maintain/ Support: • Custom applications	Procure/Maintain/ Support: • Custom applications • Operating systems	Procure/Maintain/ Support: • Custom applications • Operating systems	Procure/Maintain/ Support: • Custom applications • Operating systems	Procure/Maintain/ Support: • Custom applications • Operating systems
Procure/Maintain/ Support: • Custom applications	Procure/Maintain/ Support: Custom applications			
Procure/Maintain/ Support: • Desktop applications suites • Applications development software tools & other off-the-shelf applications	Support: • Operating systems for Agency caused outages			
Maintain/Support: • Operating systems, databases & associated middleware	Procure, install and upgrade: • Operating systems	Install/Maintain/Support: • Operating systems, databases & associated middleware	Support: • Operating systems & D/top Applications	
Maintain/Support: • IT hardware • Network (cables, routers, firmware/software) • Telecommunications carriage • Helpdesk advisory services • Hard & soft MACs	Maintain/Support: • IT hardware • Network (cables, routers, firmware/software) • Telecommunications carriage • Helpdesk advisory services • Hard & soft MACs	Support: • IT hardware • Network (cables, routers, firmware/software) • Telecommunications carriage • Helpdesk advisory services • Hard & soft MACs	Maintain: • IT hardware	Maintain/Support: • IT hardware • Network (cables, routers, firmware/software) • Telecommunications carriage
		Maintain: • IT hardware • Network (cables, routers, firmware/software) • Telecommunications carriage • Helpdesk advisory services Hard & soft MACs	Support: • IT hardware Provide network & telecommunications access	
Procure: • Operating systems	Procure: • Operating systems	Procure: Operating systems		
Own/Procure: • IT hardware • Network (routers, firmware/software) • Telecommunications carriage	Own/Procure: • IT hardware • Network (routers, firmware/software) • Telecommunications carriage	Procure: • IT hardware (incl installed SOE) • Network (cables, routers, firmware/software) • Telecommunications carriage		Own/Procure: • IT hardware • Network (cables, routers, firmware/software) • Telecommunications carriage
Asset Management	Asset Management	Asset Management		Asset Management

APPENDIX E – CLASSIFICATION OF EQUIPMENT

Appendix E records the current analysis undertaken by the study team of the IT equipment and systems observed by the study team in Group 9 Agencies other than CSIRO. While the study team has attempted to categorise IT equipment and systems in Agencies other than CSIRO, this analysis might change when an analysis of the volumes and dispersion of the IT infrastructure for CSIRO is complete.

The equipment/systems listed below are divided under headings that correspond with the discussion in Section 3 of the Scoping Study Report. The classifications are based upon the information received by the study team in the course of conducting the Scoping Study. The listing is not an exhaustive list of the equipment and systems located at each Agency. The intent is to illustrate the applicability of the model and its variations by classifying the IT equipment/systems that the study team observed.

The Agencies were asked to identify to the study team equipment and systems that may present justification for modifications to the outsourcing model used by the Initiative to date. As such, administrative or other systems that run off-the-shelf software or standard office automation suites were not considered and are not included in this listing and are presumptively included in Model 1. Each Agency presented equipment and systems that are indicative of the complexity of IT usage with the Agency concerned. As a result, this listing should be representative of the types of issues faced by the Agencies and the equipment and systems listed can be used as illustrative examples for the treatment of equipment and systems that were not seen by the study team.

The first section of the listing represents IT equipment and systems that can be outsourced in accordance with the presumptive outsourcing model. The presumptive model provides for variations that address many of the issues presented by the Agencies to the study team. However, certain of the IT equipment and systems present issues that may justify modifications to the presumptive model, which are represented in the Scoping Study Report as Models 2, 3, 4 and 5.

The presumptive IT&T outsourcing model (Model 1)

AAD

Network monitoring and management including Antarctic bases where LAN would be managed remotely if technically and economically feasible. Hard MACs in the field would be carried out by Agency technicians as is current practice.

Marine Science NT servers when located in Australia. These systems have standard operating systems but do not operate off-the-shelf applications or standard office automation packages. If technically and economically feasible, these servers could be remotely supported by the outsourcer. However hard MAC support in the field would be AAD's responsibility.

Network infrastructure including routers, switches and printers.

Installation of LAN infrastructure on Aurora Australis and support whilst vessel is in port. There may be requirements that dictate the use of marine qualified cablers.

LAN hardware for ship based systems, including provision, installation, and removal of equipment. Accommodation on board ship is restricted and as a result specialist IT support is not feasible when the vessel is away from port. These items become the Agency's responsibility to support while the vessel is at sea.

Ship based NT server systems - Accommodation on board ship is restricted and as a result specialist IT support is not feasible when ship is away from port. These items become the Agency's responsibility to support while the vessel is at sea.

Ship based office automation system - support only to be provided whilst ship is in Hobart. Accommodation on board ship is restricted and as a result specialist IT support is not feasible when vessel is away from port. These items become the Agency's responsibility to support while the vessel is at sea.

Sun servers for administrative systems (Midas, resource navigator). No off-the-shelf applications operate on these servers. Applications are in-house developed and applications support staff require routine access to the superuser (root) password. There are two ways to treat the need for root access. System failure that results from the actions of an application administrator would result in an exclusion from the outsourcer's obligation to provide designated levels of service. At all other times the outsourcer would be required to maintain service levels. This treatment would occur in the presumptive model. The alternative is to treat the system in accordance with "care and feed". In that case, the outsourcer would only support the system up to, and not including, the operating system. A separate service levels regime will operate.[1]

AGSO

Geomagnetic system used for polling remote observatories. These are standard PC configurations. Some of the applications running on the systems are supportable by an outsourcer.

IMB mapping facility - This includes some UNIX workstations and Windows NT computers. There are some specialised graphical plotting peripherals associated with these computers. They are currently maintained by the vendor of the peripherals by means of a maintenance agreement. The contractor could step into the shoes of AGSO to oversee the continuing maintenance by the vendor of these systems.

Laptops that go into the field or travel with AGSO employees. The laptops run standard software and sometimes in-house applications. Generally the laptops will be fully supported by the outsourcer. When the laptops go out into the field or elsewhere, the outsourcer will

1

continue to remotely support the end user through the Helpdesk, with back to base support when necessary.

UNIX server used for field seismic data processing. The UNIX server will be fully supported by the outsourcer until it goes into the field. When the server is in the field, support by the outsourcer through the Helpdesk would be available with back to base support when necessary.

Network infrastructure including routers, switches and printers.

The bridge PC and hosts connected to the GCM Autospec mass spectrometer systems. This PC is connected to the instrument sub-network and connects as a bridge to the main AGSO data network. This PC may run some off-the-shelf applications that may be supported.

PC connected to Hewlett Packard MSD (mass selective detector) used to make data available on the AGSO data network. This PC may run some off-the-shelf applications that may be supported.[1]

Network connections for remote geomagnetic and seismic observatories**.**

GCM Autospec mass spectrometer systems. The system includes an instrument sub-network of VAX/VMS systems. There are two servers and a number of workstations in the network.

Varian gas chromatograph. The chromatograph is connected to a outmoded Osborne 486 running Windows 3.1. It is connected to the instrument through a proprietary interface.

ANSTO

Mainpac system - The system runs on standard hardware using standard operating systems. Mainpac is an off-the-shelf software and is customised for the user. Confidentiality of data in this system is important and this issue would need to be addressed in any outsourcing contract. It is an Agency option to have the outsourcer support the Mainpac application. *Note: ANSTO may replace the Mainpac system with a new BIS which would be outsourced in accordance with Model 1.*

[1] IT&T infrastructure which is associated with a scientific instrument is considered in scope unless its sole function is to operate and support an instrument. To the extent that any IT&T infrastructure that operates and supports an instrument performs additional functions (eg a PC also collects, analyse and distribute data) that PC is considered to be within the scope of the Initiative.

PC connected to dosimeter - There are some custom applications on the PC which operates to facilitate control and data acquisition from the dosimeter[1]. The PC is used solely to collect and store data from the dosimeter and to transmit the data over the network. There is a support contract with Gamasonics that covers hardward and software support. Management of the support contract could be assumed by the outsourcer for the length of the contract. ANSTO would like to determine the timing of technology upgrades based upon the requirements of the dosimeter manufacturer, so the PC will not be on a standard refresh cycle. However, this will not affect the support provided by the outsourcer. The PC also runs standard desktop software used for administrative purposes.

Sun server and data base relating to the dosimeter - Standard Sun server and operating system. Ingres data base is a standard data base package, albeit customised for its particular use. The data base may be redeveloped, however this dedevelopment should not affect the services provided by an outsourcer.

Environmental Sciences computers – There is a variety of equipment and systems within the Environmental Sciences area. End users would like the availability of differing operating systems in a multi-boot environment. The machines themselves are standard and the operating systems are not modified. The computers also run standard applications that the outsourcer can support in addition to customised in-house applications. The use of more than one operating system needs to be specified in the Statement of Work, but there is no reason the outsourcer could not support them. Environmental Sciences also has PCs connected to scientific instruments that may fall into Model 3 or 5.

Laptops used for monitoring - To the extent the laptops are running standard applications they would fall into this category. The laptops themselves are standard and the operating systems have not been modified. When these laptops go out into the field, support from the outsourcer would be provided through the help desk with back to base support when necessary.

Network infrastructure including routers, switches and printers.

DEC Ultrix machines that are kept to retain old data from the AUSANS instrument and its accessibility. The machines are kept purely for the purpose of accessing historical data. They use standard operating system and in-house applications, albeit on outmoded machines. ANSTO intends to transfer the data on these machines prior to handover, in which case outsourcer support will no longer be necessary.

SIMS Sun SparcStation - the machine is confined to a particular release of Solaris and supporting platform, but the operating system has not been modified and is supportable. Although it is connected to an instrument, it appears to perform other functions[1].

The Radio-pharmaceuticals area has a variety of equipment. The desktops and servers located in this area are fully supportable by an outsourcer. As mentioned in conjunction with the Mainpac system, a portion of the IT infrastructure may be converted to a new BIS prior to handover. This area maintains a private LAN. Also located within this environment are outmoded machines running DOS based applications. Support of the LAN and certain of these machines could be carried out by an outsourcer observing safety procedures currently in force. However, to the extent the outmoded machines running DOS based applications are used solely to drive scientific instrumentation, they may fall into Model 3 or 5.

BOM

LAN facilities in regional offices.

Laptops that scientists take into the field - When these laptops go out into the field, support by the outsourcer could be provided through the help desk with back to base servicing when required.

Desktops used in forecasting offices - For the most part, while these machines have high end display and run custom applications, the machines are standard with standard operating systems.
HP mid range machines - These machines use "standard" HP hardware and operating systems with in-house developed applications. They are currently supported by HP under a warranty/maintenance contract. The contract could be novated to the outsourcer.

SGI mid range machines - These machines use "standard" SGI hardware and operating systems with in-house developed applications. They are currently supported by SGI under a warranty/maintenance contract. The contract could be novated to the outsourcer.

IBM mid range machines - These machines use "standard" IBM hardware and operating systems with in-house developed applications. They are currently supported by IBM under a warranty/maintenance contract. The contract could be novated to the outsourcer.

Laptops used by observers are standard laptops that run custom applications. Generally the laptops will be fully supported by the outsourcer. When the laptops go out into the field or elsewhere, the outsourcer will continue to support the laptops through the Helpdesk with back to base support when necessary.

Silicon Graphics workstation connected to WeatherWatch radar and SGI or HP terminals connected to radars - The workstations runs custom applications only, but they do not require modification of operating systems or hardware. These workstations are connected to the network. BOM staff would continue to support the interface between the SGI machines, the radar and the custom applications.

Pentium machines linked to spectrometers - No modification of hardware or operating system. If these machines perform functions other than to control or support the spectrometer, they would be outsourced in accordance with the presumptive model. If their

sole function is to control or support the spectrometer, they would remain the responsibility of the agency[1].

Automatic Weather Station data collection systems at the head/regional office level - System designed to collect information through use of modems. They are standard hardware and operating systems with custom applications.

Flood warning data collection systems in BOM head and regional offices - System designed to collect information through use of modems. The equipment used are outmoded standard equipment and standard operating systems with in-house developed applications.

Network infrastructure including routers, switches and printers.

NEC and Cray Super computers - These machines use "standard" hardware and operating systems with in-house developed applications. The NEC SX4 and SX5 are currently supported by NEC under warranty/contract. The contract can be managed by an outsourcer. As discussed in the Scoping Study Report, whether a viable market for support of these machines exists will have to be determined through the tender process (see Section 4.6.1).

Mass data store – StorageTek silos - These silos are standard equipment.

Feed and care (Model 2)

Some of the equipment and systems listed above may be treated in accordance with the feed and care variation. As indicated in connection with several of the equipment and/or systems listed above, the feed and care variation is an alternative approach available in circumstances in which users need access and control over the operating system in the normal course of their business. In the feed and care approach, the Agency remains responsible for the support and maintenance of the operating system. The presumptive model may be preferable, in that the outsourcer would still have some responsibility for the support and maintenance of the operating system. Users are still able to access the operating system, subject to internal policies of Agencies that govern access. In cases where the actions of the Agency users resulted in failure of the system, the outsourcer would be able to rely on an exclusion from service levels that excuses the outsourcer for the failure. However, the outsourcer would remain responsible for getting the system back up and running. This approach passes more of the burden for system availability to the outsourcer without limiting the flexibility of the Agencies.

Satellite systems - Mainly HP-UX based ingesters running in-house applications. Hardware and operating system are standard whereas applications are in-house developed and supported. Support of the platforms and operating system could be outsourced.

UNIX systems running AIFS - There is no modification to the hardware or operating systems. BOM emphasises that applications support personnel require routine root access for timely application trouble shooting and rectification. There are two ways to treat the need for root access. System failure that results from the actions of a administrator access would result in an exclusion from the outsourcer's obligation to provide designated levels of service. At all other times the outsourcer would be required to maintain service levels. This treatment would occur in the presumptive model. The alternative is to treat the system in accordance with "care and feed". In that case, the outsourcer would only support the system up to, and not including, the operating system. A separate service levels regime will operate.

IT Infrastructure Procurement only (Model 3)

AAD

WAN hardware infrastructure required for installation at Antarctic Bases. This would include ground stations, racks, power supplies, hubs, switches, cold temperature cabling, NT servers, desktops, frame relay devices. Network monitoring equipment, Web cameras.

PABX hardware and remote support, cold temperature telephone cabling, handsets.
PC hardware and operating system for Building Management Systems (BMS) for Antarctic Stations support of applications and system will remain AAD responsibility.

AGSO

Geomagnetism PC used for development purposes. - This PC is used for the development of the geomagnetic observatories.

Geomagnetic observatories and seismic observatories. The instrument is home built by the AGSO engineering department. The integration of the IT infrastructure and the other components of the stations is tight. The parts may be procured through an outsourcer, but an outsourcer would probably have no interest in ownership of the final product which is basically a scientific instrument with some stripped down PCs attached. The network connections, however, will be provided and supported by the outsourcer.

Support only (Model 4)

AAD

Equipment accompanying visiting research staff.
Equipment supplied by joint venturers or as part of a CRC.

AGSO

Equipment accompanying visiting research staff.
Equipment supplied by joint venturers or as part of a CRC.

ANSTO

Equipment accompanying visiting research staff.
Equipment supplied by joint venturers or as part of a CRC.

BOM

Equipment accompanying visiting research staff.
Equipment supplied by joint venturers or as part of a CRC.

IT infrastructure remains agency responsibility (Model 5)

AAD

Environment control systems installed at Antarctic Stations.

Lidar. Is supported by several networked PC machines and a DEC VMS machine.. All software is in-house developed. Peripheral drivers are in-house developed and routine access is required to operating systems. Routine access is required to hardware components. This is an integrated operating unit that will be permanently based in Antarctica.

AGSO

The IT infrastructure associated with the following instruments are not running any standard applications, they are stand-alone machines that are not connected to the network:

> Hewlett Packard MSD (mass selective detector). This is a combined PC and instrument supplied by HP. The MSD PC runs Windows NT v4.0. To date AGSO has avoided "interference" in the support of the PC to avoid issues with the vendor in relation to performance of the instrument.
>
> GEO-X system used for field seismic data. This system is really one instrument. IT is tightly integrated. It serves no purpose other than to service the instrument.
>
> Geomagnetic calibrations facility. This facility is not owned by AGSO and they do not provide any support for the IT infrastructure.

ANSTO

Waste management PCs. PCs have vendor standard hardware but run specialised third party software. The operating systems are not modified. They are stand-alone machines that are dedicated to the gamma scanner and barcode reader.

Sun machine connected to AUSANS instrument. This runs in-house applications and special SCSI driver to allow interface with instrument. The SCSI driver is in-house developed. The machine is used only to support the instrument.

Certain of the equipment located in radio-pharmaceuticals are connected to and used solely to drive instrumentation. One example is the label-maker. This equipment would remain the responsibility of the agency.

Both the Silicon process System and the Reactor SCADA are located within the reactor building. They are purpose built systems that have sole suppliers. There is no market for these systems. Both systems are currently supported and maintained by the system vendors Yokogawa and Foxboro respectively. It may possible for an outsourcer to step into the shoes of ANSTO and oversee the arrangements with the suppliers but it is not practical for the following reasons. In order for outside maintenance personnel to enter the reactor building, they must be accompanied by specified ANSTO personnel. The potentially hazardous nature of working in the reactor building is a further complicating factor. The liability resulting from a failure of these systems is high and would not be insurable.

Tandem accelerator system. Supported by outmoded hardware and software. Primary systems are VME bus rack-mounted interfacing to DEC-Ultrix PCs. Interfaces to instrument dictate the operating system used. These are used only to drive the tandem accelerator system.

BOM

At remote sites WeatherWatch radar connected to 80386 DOS based workstations running in-house developed applications. Exclusively used to receive information from the radar.

Ozone data measurers. These are outmoded systems, however they are standard hardware and operating systems. The applications running on them are all custom built. These are dedicate machines used solely for the collection of ozone data.

Mass Spectrometers. Currently supported by HP. The HP equipment is only used to drive the mass spectrometers.

Automatic Weather Station (AWS). These are devices placed in remote locations that automatically measure rainfall and temperature information. These store the information until it is accessed by dialup link from BOM headquarters. IT infrastructure in these devices is a cut down industrial PC tightly integrated in to the device by BOM. There is no other supplier of this technology.

WeatherWatch radar. These are radar devices that feed data into supporting workstation devices. These are SGI machines that run BOM developed software. The hardware interface to the radar equipment from the workstations was also developed by BOM technicians.

Floating buoys used to measure wave height. These devices contain some IT components but are unrecognisable as such and are used solely for measurement purposes. There may be some ability to procure parts through the outsourcer but this is not likely.

586 based machines that release upper air measurement systems. Processor and software provided and supported by the vendor. These are purpose built industrial devices that are dedicated to the function of filling and releasing upper atmosphere balloons.

Expendable IT componentry included in Ozone sensing devices such as radio sondes.

Floodwarning data acquisition units. To the extent these are owned by BOM they may want to procure parts through the outsourcer. However, these are basically instruments, not IT infrastructure, so that may be impractical.