



AUSTRALIAN

GOVERNMENT USE

OF INFORMATION

AND COMMUNICATION

TECHNOLOGY

MANAGEMENT  
ADVISORY  
COMMITTEE

2

A NEW GOVERNANCE AND INVESTMENT FRAMEWORK >> >>



A U S T R A L I A N

G O V E R N M E N T U S E

O F I N F O R M A T I O N

A N D C O M M U N I C A T I O N

T E C H N O L O G Y

MANAGEMENT  
ADVISORY  
COMMITTEE

2

A N E W G O V E R N A N C E A N D I N V E S T M E N T F R A M E W O R K >> >>

© Commonwealth of Australia 2002

ISBN 0 642 54356 9

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without permission from AusInfo. Requests and enquiries concerning reproduction and rights should be addressed to the Manager, Legislative Services, AusInfo, GPO Box 84, Canberra ACT 2601.

# CONTENTS

---

<b>EXECUTIVE SUMMARY</b> .....	<b>2</b>
ISSUES .....	2
AGREED APPROACH .....	3
<b>INTRODUCTION</b> .....	<b>6</b>
<b>THE ISSUES</b> .....	<b>10</b>
MAINSTREAMING ONLINE SERVICE DELIVERY.....	10
INVESTMENT .....	10
GOVERNANCE.....	11
SHARED AND COLLABORATIVE APPROACHES.....	11
<b>PRINCIPLES OF ICT GOVERNANCE TO OPTIMISE COMMONWEALTH OUTCOMES</b> .....	<b>12</b>
<b>BUSINESS DRIVERS</b> .....	<b>12</b>
IMPROVED VALUE FOR MONEY .....	13
SECURITY AND PRIVACY .....	13
INFORMATION RE-USE.....	14
DEVELOPMENT OF THE AUSTRALIAN INFORMATION ECONOMY .....	14
<b>OPERATIONAL FRAMEWORK, ROLES AND RESPONSIBILITIES</b> .....	<b>16</b>
NOIE .....	17
IMSC .....	17
CIO COMMITTEE .....	17
WORKING GROUPS .....	18
<b>INVESTMENT</b> .....	<b>18</b>
<b>ARCHITECTURE PRINCIPLES AND STANDARDS</b> .....	<b>18</b>
STANDARDS.....	20
TECHNICAL ARCHITECTURE .....	20
NETWORK ARCHITECTURE.....	20
OPERATING ENVIRONMENT.....	21
<b>INITIAL PRIORITIES</b> .....	<b>21</b>
SECURITY .....	21
NEW AND SECOND GENERATION ICT SOURCING MODELS.....	22
THE HUMAN ISSUES .....	22
<b>AGREED APPROACH</b> .....	<b>24</b>

<b>APPENDIX 1 - ROLE OF THE INFORMATION MANAGEMENT STRATEGY COMMITTEE (IMSC)</b> .....	26
<b>APPENDIX 2 - ROLE OF THE CHIEF INFORMATION OFFICER (CIO) COMMITTEE</b> .....	27
<b>APPENDIX 3 - SECURE BUSINESS SYSTEMS WORKING GROUP</b> .....	29
<b>APPENDIX 4 - INTEGRATED SERVICE DELIVERY WORKING GROUP</b> .....	32
<b>APPENDIX 5 - AUTHENTICATION OF EXTERNAL CLIENTS WORKING GROUP</b> .....	35

## EXECUTIVE SUMMARY

---

## **EXECUTIVE SUMMARY**

---

Government is committed to providing the best possible services to the community. Achieving this goal is dependent on maximising the effectiveness of policy development and program delivery, planning and budgetary arrangements, decision-making processes, organisational structures, workplace relations and people management.

Much reform has been undertaken in these areas and significant gains in performance have been achieved. Increasingly, information and communications technology (ICT) plays an important role in determining the quality and accessibility of services. The development of effective whole-of-government approaches to ICT is critical to achieving further significant gains in the delivery of government services.

The move towards e-Government—more responsive, comprehensive and integrated government operations and service delivery—requires a transformation of business processes to adopt and respond to new technologies. In this environment, the business case for a whole-of-government approach to ICT investment and governance is strengthened.

This report outlines an appropriate framework to guide Commonwealth departments and agencies (referred to as agencies in this report) through this transformation and into the next stage of delivering better government. The report reflects the work of the IT Architecture and Governance (ITAG) Sub-Committee of the Management Advisory Committee (MAC). The recommendations of the report were endorsed at the 20 August 2002 meeting of the MAC.

## **ISSUES**

There is an increasing demand for government to provide more integrated and interactive information and services. To provide a seamless and consistent service across government, agencies must work together to ensure that their individual systems are compatible and can be linked.

Decisions about ICT investment and governance are currently made at agency level. A 'big picture' approach is necessary when considering these issues, so that decisions support the whole-of-government business case, and investments are made with a view to the return across government, not to individual agencies alone.

There is an opportunity for increased collaboration on ICT procurement and re-use of valuable intellectual property across the federal government. In addition, shared approaches to standards, infrastructure, security, collaboration in procurement and the best use of government intellectual property can deliver better value for money.

This report has identified the initial priorities as security, second generation ICT sourcing, IT management skills and contract management.

To support this whole-of-government or 'federated' approach, this report recommends a review of ICT standards, interoperability and investment and governance of shared infrastructure, as well as management and operational practices.

## **AGREED APPROACH**

After considering the report of the ITAG Sub-Committee, the MAC agreed:

- The Governance Principles set out on page 12 as guiding principles for federal government agencies, noting that:
  - agencies will continue to manage their own information technology strategy, development, implementation and support; and
  - a federated approach to ICT governance in the Commonwealth is warranted where whole-of-government interoperability is an issue or a whole-of-government approach may be beneficial.
- The establishment of a new structure consisting of a two tiered peak level Information Management Strategy Committee (IMSC), supported by a Chief Information Officer (CIO) Committee. (The roles of these groups are outlined in Appendix 1 and 2.)
- The Architectural Principles set out on page 18 as guiding principles for federal government agencies.
- That the IMSC will approve a work plan for the CIO Committee that may include working groups to investigate specific areas of interest and operate for defined periods.
- An initial agenda for future strategic work, to include:
  - identification of significant issues related to investment in, and governance of, shared ICT infrastructure;
  - development of a model for architecture, governance and investment for the secure business systems of the Commonwealth;
  - development of a proposal for a new action plan for integrated service delivery (ISD), built on the work of ISD working group, with an action and investment plan, for consideration by government;
  - identifying the key lessons learned which would assist agencies entering into new and 'second generation' ICT sourcing agreements; and
  - authentication of clients.



## INTRODUCTION

---

## INTRODUCTION

---

*Another challenge is the capacity of departments to successfully interact with each other in pursuit of whole of government goals and more broadly, for the entire Service to work in partnership with other bureaucracies, with business and with community groups as resources and responsibility are devolved closer to where problems or opportunities exist.*

The Hon. John Howard MP  
Prime Minister  
Centenary of the APS Oration, June 2001

Government is committed to providing the best possible services to the community. Achieving this goal is dependent on maximising the effectiveness of policy development and program delivery, planning and budgetary arrangements, decision-making processes, organisational structures, workplace relations and people management.

Much reform has been undertaken in these areas and significant gains in performance have been achieved. Governments and the private sector are saving time and money by automating business processes. Developments in ICT have opened the door for even greater efficiencies and improved service delivery to the public through integrated processes. The strong business case for this approach is driving the transformations necessary to take advantage of the full potential of ICT.

Investment in ICT is paying off across the economy, introducing new products and services, enhancing existing products and services, and achieving efficiencies. There are opportunities for even greater gains as public and private sector organisations transform their existing processes by the strategic application of ICT. For individual organisations and government agencies, the most significant gains are achieved when ICT decisions are business-driven. Shared arrangements in the private sector have demonstrated significant benefits—for example, the banking sector’s credit card arrangements and the travel industry’s booking facilities. Shared arrangements also offer significant opportunities to improve efficiency and service delivery in the public sector.

The strategic use of ICT enables departments and agencies to improve existing program models and introduce new ways of delivering government information and services. The use of this technology will also allow a greater outward focus and provide more efficient access to government services by citizens and business.

The Commonwealth Government spends around \$3.5 billion annually on ICT (an estimated \$2.1 billion<sup>1</sup> recurrent and up to \$1.4 billion capital). Government’s significant and rapidly growing investment in electronic information management and service delivery is driven by citizens’ demands for higher levels of service delivery, and by government’s anticipated efficiency gains through electronic information and service delivery.

---

<sup>1</sup> Extrapolated from *Australian Bureau of Statistics 8119.0 Government Use of Information Technology, Australia*.

Australia is among world leaders in applying new technologies to government administration and service delivery—now commonly referred to as ‘e-Government’. Like Canada, the United States and the United Kingdom, Australia is moving beyond single-agency IT installations and unrelated Internet web sites. In a trend mirroring the private sector, the Australian Government is entering the complex phase of providing integrated service delivery both online and through other channels.

Common issues that all these leading countries are facing include:

- linking disparate back-end systems to provide electronic transactions which cross agency boundaries;
- reconciling technical and financial imperatives to move towards shared standards, where appropriate;
- defining the architectural framework and standards needed for effective infrastructure investment and interoperable systems; and
- establishing a Commonwealth-wide investment strategy to facilitate the development of ICT capability that benefits multiple agencies.

Increasingly, government policies and programs are being jointly developed and delivered across more than two agencies. This often requires systems to operate across agency boundaries and to be interoperable with other systems. Issues associated with the effective operation of such systems, including governance, architecture and investment, are becoming priorities for management.

Established government policy and program models are changing. New models, while enhancing program outcomes, create more complex ICT support systems and demand higher levels of capability and security. As a result, there is an increase in costs of the technology infrastructure on which improvements in overall program efficiency depend. There is also growing awareness that the pace of technological change is requiring policy makers and legislators to consider the balance between protecting information and privacy and the growing community desire for better service delivery and greater access to information.

A range of policies, regulations and legislation combine to form the existing governance and financial framework for ICT acquisition, development and management. These include the Protective Security Manual, the Telecommunications Act, the Privacy Act, the Financial Management and Accountability Act, the Public Service Act and outsourcing policy. In this changing policy and program environment, there is a case for a more coherent framework across government.

Federal government agencies have made substantial progress in improving the efficiency of their program delivery. This has been based on a devolved approach to ICT investment and innovative program design. In order to achieve the type of whole-of-government outcomes based on partnerships outlined by the Prime Minister, the current approach will need to be augmented by new systems and processes that better align resources between agencies, where appropriate, while recognising the existence of departmental or jurisdictional boundaries.

In a devolved management system where the cost of enablers like ICT is increasing, a ‘federated’ governance approach is desirable. A federated governance system is one in which independent agencies work together to achieve an optimal outcome for each

other and government as a whole. This approach will facilitate shared investments and standards, where appropriate, to achieve better value for money and to support lead agencies in the development of innovative business systems that can be re-used by other agencies. It also allows a more coordinated approach to shared policy challenges like security and privacy.

### **Information Technology Architecture and Governance Sub-Committee**

At its meeting of 5 September 2001, the MAC established the ITAG Sub-Committee. The Sub-Committee's task was to investigate and make recommendations on an appropriate governance and investment framework for the Australian Government's use of ICT. Its terms of reference were:

- Consider and, if appropriate, oversee the development of a governance and investment framework for the development and management of inter-agency ICT infrastructure.
- In particular, consider the justification for, and membership and terms of reference of, an ongoing CIO Committee.
- Identify issues that may most appropriately be handled at the whole-of-government level to optimise outcomes from a whole-of-government perspective.
- Propose priorities and make recommendations to the MAC, as appropriate, on ICT matters that affect government.

The outcomes expected by the MAC were:

- an effective framework for governance of ICT architecture, standards and investment choices which affect more than one agency;
- clear accountability consistent with the overall management and accountability framework;
- more cost effective investment outcomes; and
- efficient and effective ICT enabled operations.

## THE ISSUES

---

## THE ISSUES

---

There is a global trend for companies and governments to improve the efficiency of their business processes and service delivery by moving information and services online. In 1997 the Prime Minister set a target for federal government agencies to have all appropriate services online by 2001. This target has been met. Experience with the Internet has created an expectation of electronic information and service delivery—it is no longer regarded as something special.

Moving information online and automating processes has involved significant investment. The next stage of transforming business processes will require an even greater investment. It will provide greater rewards through increased efficiencies within government and improved service delivery. It is likely, however, that small and medium-sized agencies will find it difficult to meet the costs of sophisticated online services.

Some components of the federal government's online operations are best addressed at a whole-of-government level, rather than by individual agencies. These include government secure business systems—for example, the budget system—and the standards and protocols that underlie integrated service delivery.

### **Mainstreaming online services delivery**

The Commonwealth's initial approach to online service delivery was a simple and direct translation of existing activities that lend themselves to the online medium. However, online delivery of programs, services and information is now becoming 'mainstream'.

It is no longer enough for online service delivery to be an add-on or after-thought or simply to be 'overlayed' on existing service delivery channels. The online channel is not merely for information and service delivery. It drives new approaches to information management that enable the integration of information and services. An online information management system provides access to information that is easy to update. It promotes consistency through all service channels. Put simply, a telephone hotline operator, an official responding to a letter or a citizen seeking information online can obtain the same data from a single, integrated Internet-enabled source.

Government and private sector organisations are starting to offer integrated service delivery channels, to provide ease of access for customers and in the interest of efficiency. This is creating a rising customer expectation that higher quality integrated services are only a click or two away. Reviewing existing business models and process re-engineering is essential for the benefits of new online approaches to be realised.

### **Investment**

Agencies have indicated that more sophisticated service delivery will be difficult to progress without a coherent cross-agency investment strategy. Some agencies believe more sophisticated online services can be funded through the expected business gains and efficiencies that can be achieved by replacing traditional service delivery channels, or through re-engineered back-end systems. However, the sources of such

business gains are often uncertain and return on investment may be delayed. The costs and benefits may also fall unevenly across different sponsors and recipients.

Investing up-front in innovative or higher-risk projects and funding cross-agency networks can be difficult under the existing budgetary system. In the current environment it is difficult to allocate funding for whole-of-government infrastructure projects.

The Commonwealth's *Government Online* Strategy had multiple objectives that encompassed both single agencies and whole-of-government. Encouraging uptake of online services in the wider community and showing leadership in this area are both whole-of-government objectives. Other countries, such as the United Kingdom and United States, have developed and implemented investments to address these higher-level objectives.

## **Governance**

Governance may be described as the people, policies and processes that provide the framework within which managers make decisions and take actions to optimise outcomes related to their spheres of responsibility.

Existing Commonwealth governance arrangements focus primarily on single agency responsibility. For example, the Financial Management and Accountability Act requires a chief executive to manage the affairs of the agency in a way that promotes proper use of the Commonwealth resources for which the chief executive is responsible. This results in decisions about resources based on internal agency considerations. While this is designed to deliver solutions that meet an individual agency's requirements, the outcome may not be the best one from a whole-of-government perspective.

Where program delivery requires inter-relating of information, business processes and ICT systems across different agencies, single agency governance arrangements will need supplementation.

The increasing trend towards cross-agency responsibilities, together with increasing demand for whole-of-government systems, has created a need to review existing arrangements. This includes reviewing ICT standards, interoperability and investment decisions as well as management and operations.

## **Shared and collaborative approaches**

As policy development that crosses agency boundaries is increasing, a governance framework for the 'shared' elements of systems becomes critical. These elements range from ownership of shared business systems, to information ownership, infrastructure, and standards.

Agencies already co-operate when developing policies and standards. Similarly, opportunities will continue to be taken to collaborate on ICT procurement both by leveraging government's collective buying power and by increasingly re-using valuable intellectual property across the Commonwealth.

## **PRINCIPLES OF ICT GOVERNANCE TO OPTIMISE COMMONWEALTH OUTCOMES**

---

A federated system of governance for ICT will promote optimal outcomes across the federal government, in terms of those government programs and services that are supported by ICT. Agencies will continue to manage their own information technology strategy, development, implementation and support, but there are areas in which these federated principles should apply.

The following principles will support such a federated system:

- Agencies will continue to manage their own information and communications technology in terms of strategy, development, implementation and support.
- Agency management of ICT will be enhanced if there is improved information and knowledge sharing across government including 'better practice'.
- Guidelines and shared processes are important to optimise the business returns to government from ICT investment. These should:
  - be developed and managed through a cooperative governance model that is responsive to government priorities and policies;
  - promote interoperability and re-use of software or systems, to maximise future opportunities for improving government programs and services, and to promote better value for money; and
  - address public confidence and trust in the overall framework of ICT being used by the government.
- The premise that information content may at some time be transferred across agency boundaries should underpin decisions when agencies are designing new systems.
- Security and privacy is essential to ICT supported business processes.
- A strategic focus on business outcomes and efficiency gains is required for funding Commonwealth ICT.
- Investment and funding models must accommodate the development of shared approaches to system development and Intellectual Property (IP).
- The integrity of shared architecture and systems should be protected by an agreed Quality Assurance process.

## **BUSINESS DRIVERS**

---

There are both individual agency and whole-of-government business drivers for this new architecture, governance and investment framework. Individual agency drivers may differ but the whole-of-government ones are expected to also be applicable to most agencies.

## **Government transformation**

The appropriate use of ICT enables transformation in the policy, administration and program delivery processes of government. The pace of change can be accelerated to improve efficiency and effectiveness in government. Agencies can now take a more flexible and dynamic approach to policy and program delivery.

Citizens and businesses will come to expect government bodies to remember the services already provided and the information already gathered. These expectations apply to all channels of service delivery.

## **Multiple service delivery channels**

Program delivery routinely takes place through multiple channels (counter, mail, telephone, Internet). ICT enables the same information infrastructure to service every channel. The result is more consistent government decision-making and service delivery, leading to greater efficiency. Additionally, citizens experience greater convenience and more streamlined and integrated services.

## **Improved value for money**

Today all public and private sector organisations are aware that buying and installing ICT of itself does not produce benefits. ICT investments must be actively planned and managed to deliver specified benefits. Maximising benefits of business transformation and ICT investment across the Commonwealth requires attention to the impact of one agency's investment on others.

In a devolved environment for management of ICT, shared standards, infrastructure, security, collaboration in procurement and exploitation of government IP can deliver better value for money.

## **Security and privacy**

The balance between security and privacy is a key consideration as public policy develops in this area. Increased awareness about security following the terrorist attacks on the United States in September 2001 focused attention on the Commonwealth's security drivers. Further, the Privacy Act has raised the profile of individual privacy.

In September 2001 the federal government established new arrangements for protecting critical infrastructure, including information infrastructure, and enhancing e-security across the government and private sectors. The Critical Infrastructure Protection Group (CIPG), chaired by the Attorney-General's Department and reporting to the Secretaries Committee on National Security, is the forum for handling serious actual and potential information security incidents affecting the Commonwealth and critical industry sectors. The E-Security Co-ordination Group (ESCG), which is chaired by the National Office for the Information Economy (NOIE), deals with broader e-security issues. The ESCG has established a government E-Security Working Group that is jointly chaired by Defence Signals Directorate and NOIE.

Public sensitivity and awareness of the potential to aggregate electronic data collected by government is growing. Already, federal agencies are working to develop stronger authentication of individuals with access to this private data.

### **Information re-use**

Subject to appropriate privacy and security treatment, information sharing can improve the efficiency of business processes within government and streamline government service delivery to citizens and businesses. ICT is the key enabler of this process.

There is evidence that individuals and businesses dealing with government expect some knowledge of previous contacts on a particular issue. Data linking between agencies, with appropriate safeguards, will increasingly be required since the principle of 'enter once, use many times' can improve government efficiency and the service provided to citizens.

### **Development of the Australian information economy**

The Commonwealth acts as a powerful agent for the innovative use of technology. The problems faced by governments have much in common with those in the private sector. Effective government application of ICT both learns from and influences private sector development. This gives impetus to the development of the Australian information economy, including development of Australian capabilities in technology, software and services.

## **OPERATIONAL FRAMEWORK, ROLES AND RESPONSIBILITIES**

---

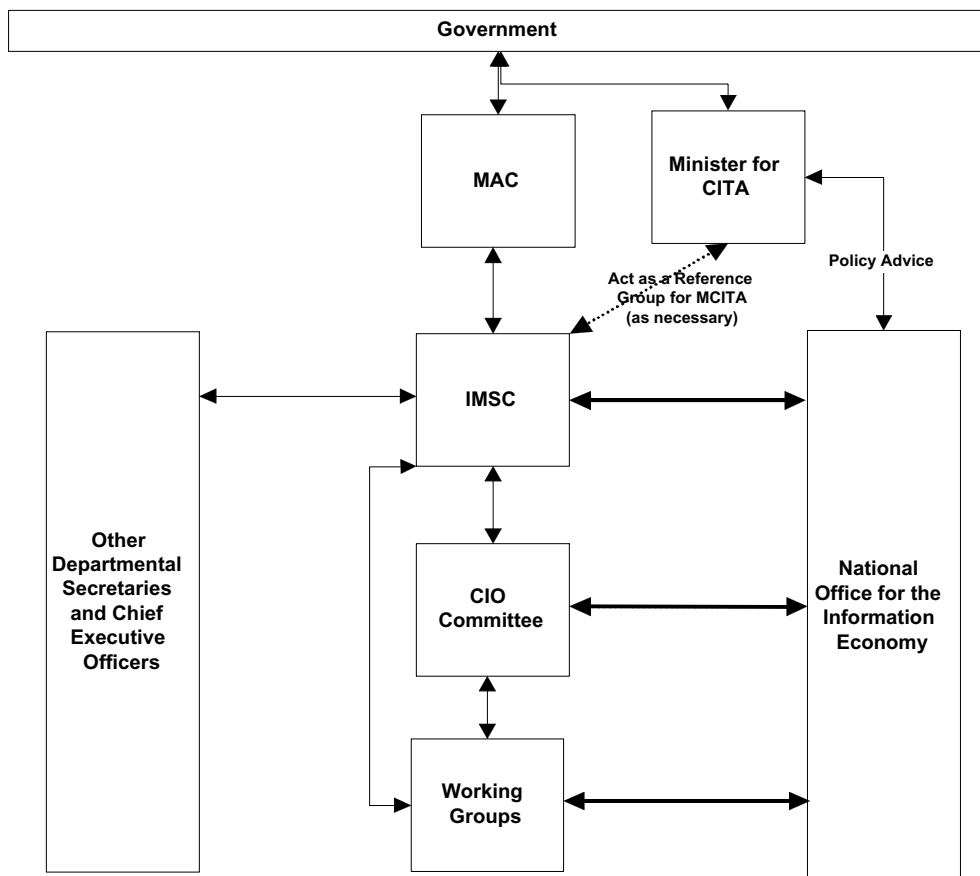
## OPERATIONAL FRAMEWORK, ROLES AND RESPONSIBILITIES

To address the issues and emerging business drivers related to government ICT use, a new governance model, building on existing management arrangements, will be adopted.

The existing arrangement is that Secretaries are responsible for agency-level strategic decisions on business processes and ICT investment. NOIE is responsible for the coordination of the application of new technologies to government administration, information and service provision.

A senior advisory group—the Information Management Strategy Committee (IMSC)—will be established to provide leadership and advice to the Australian Public Service (APS) on ICT strategic and governance issues. The IMSC will be supported by key business strategy and support decision makers—the Chief Information Officer (CIO) Committee—and, where appropriate, working groups to address specific matters.

The framework for this approach is represented in the diagram below.



## **NOIE**

The charter of the National Office for the Information Economy (NOIE) is to provide strategic advice to the federal government on the key factors driving the information economy and coordination of the application of new technologies to government administration, information and service provision. Within these parameters, NOIE will support the IMSC by facilitating the consideration of ICT issues affecting more than one agency, developing options and, where appropriate, providing shared or collective ICT solutions required by the IMSC. NOIE will also provide secretariat support for the IMSC, the CIO Committee and, where appropriate, working groups.

## **IMSC**

The IMSC will provide shared leadership on multi-agency and whole-of-government information management strategies. It will oversee the development of policies, standards, specifications and guidelines for ICT, to support future interoperability as well as individual business solutions for agencies. As a leadership group, the IMSC will use its influence to leverage support for its approaches.

No formal or statutory powers are proposed for the IMSC. However, if formal authority is required to achieve desired outcomes, the IMSC will advise the MAC and, where appropriate, the Minister for Communications, Information Technology and the Arts.

The IMSC will comprise the Secretary of the Department of Communications, Information Technology and the Arts as Chair and five to eight members at Secretary or CEO level, appointed by the MAC. Membership will be drawn from agencies that have key central roles or major responsibility for delivering services online. The CEO of NOIE will be the Chair of the CIO Committee and will also be a member of the IMSC. Given the lead times for significant projects, the IMSC will be established for three to five years.

The role of the IMSC is outlined at Appendix 1.

## **CIO Committee**

Reporting to the IMSC, the CIO Committee will identify strategic issues, address issues referred by IMSC and develop options for adoption and implementation of ICT at agency or whole-of-government level. This will include developing strategic architectures, standards and proposals for shared services. Through working groups, it will address specific issues and promote research and development, and knowledge sharing. For example, in consultation with the Australian Public Service Commission, the CIO Committee may consider human resource issues in the government ICT arena.

CIO Committee members will be drawn from key central agencies and agencies that are high users of ICT. There will be fourteen members, of whom ten will be ongoing members and four appointed by the IMSC for a set period. These four non-permanent members may represent small agencies with particular areas of expertise. Broadly, permanent membership of the Committee will comprise:

- the National Office for the Information Economy (Chair);
- the Australian Public Service Commission;

- the Department of Finance and Administration;
- six other agencies (central agencies and high ICT users); and
- a small agency providing the perspective of other small agencies.

Non-permanent membership will be co-opted by the permanent members. It may include agencies undertaking or planning a major information infrastructure project or agencies whose CIO has specific skills, interest or connections required by the IMSC.

Members will normally be drawn from the agency's executive management group and have responsibility for the nexus between business strategy and ICT strategy.

The role of the CIO Committee is outlined at Appendix 2.

### **Working groups**

Working groups will be created to address specific matters identified by the IMSC and CIO Committee. Membership will be determined by the CIO Committee and by the willingness of agency heads to contribute resources. Membership of working groups could be drawn from any interested agency.

## **INVESTMENT**

---

A key inhibitor of a government-wide ICT infrastructure is that funding for technology is currently provided on an agency-by-agency basis and for overall proposals that rarely identify ICT-specific components. Investment for common or shared infrastructure requires a different approach. The return on such investment does not always accrue to the spending agency. In other words, costs and benefits are not always aligned with the investor, and the timeframe for the return may be different. In these circumstances, agency heads may be reluctant to commit their agency funds to shared infrastructure.

The MAC Budgeting and Resources Management Sub-Committee has reviewed these issues in terms of shared outcomes and outputs. However, an ICT investment strategy would benefit from some new work addressing shared investment.

## **ARCHITECTURE PRINCIPLES AND STANDARDS**

---

A federated approach to government ICT governance, architecture and investment is appropriate in the Australian environment. This means that, when ICT investments are considered, the onus is on decision-makers to consider convergence of existing and planned systems and service channels. A federated approach will provide the Commonwealth with the level of desired flexibility to deliver its programs and services in ways that achieve government objectives and meet the needs and circumstances of citizens.

For a federated approach to work, sound architecture principles are crucial. Principles and standards should encourage, not inhibit, the use of ICT to support business processes. A formal change management process should be used if significant modifications to agreed principles and standards are required. The following table lists the identified architecture principles for Commonwealth ICT.

<b>Architecture Principle 1:</b> <i>Reduce Integration Complexity</i>	The federated architecture must promote reduced complexity and enable integration and interoperability.
<b>Architecture Principle 2:</b> <i>Holistic Approach</i>	Information is a government asset. Its value is enhanced when it can be accessed and applied to accelerate and improve decision-making within and across agencies, within the bounds of legislation, security and privacy.
<b>Architecture Principle 3:</b> <i>Business Event-Driven Systems</i>	Systems must be designed to be business event-driven. This principle applies to manual, process and application systems.
<b>Architecture Principle 4:</b> <i>Defined Authoritative Sources</i>	All information must have defined 'authoritative sources'. These sources will act as 'information stewards'. Authorised data must be accessible and available for re-use by any entitled system and/or business process.
<b>Architecture Principle 5:</b> <i>Security, Confidentiality, Privacy &amp; Protection of Information</i>	ICT systems must be implemented in compliance with government security, confidentiality and privacy policies and laws. Information must be protected against unauthorised access, denial of service and both intentional and accidental modification.
<b>Architecture Principle 6:</b> <i>Proven Standards and Technologies</i>	ICT solutions must, wherever possible, use commercially viable standards-based technologies. The customising of purchased software should be avoided wherever possible. Priority should be given to products adhering to industry standards and open architecture.
<b>Architecture Principle 7:</b> <i>Total Cost of Ownership (TCO)</i>	Total Cost of Ownership, including consideration of costs and benefits across government, for applications and technologies (hardware and software) must balance development, support, disaster recovery and retirement costs along with the costs of flexibility, scalability, ease of use/support over the life-cycle of the technology or application.
<b>Architecture Principle 8:</b> <i>Adopt Formal Methods of Engineering</i>	Government must employ formal practices, methods, and tools for architecture and engineering for all stages of these disciplines in ICT, from design to construction and implementation.
<b>Architecture Principle 9:</b> <i>Extended Information &amp; Services Environment</i>	To the maximum extent possible, the integration of the ICT infrastructure should enable and enhance the provision of government information and services to citizens, businesses, other Commonwealth agencies and other governments.
<b>Architecture Principle 10:</b> <i>Multiple Delivery Channels</i>	ICT should support client delivery channel preferences in accessing government services.
<b>Architecture Principle 11:</b> <i>Accessible Government</i>	To be responsive to the increasing diversity of Australian society, the Government must be accessible to all citizens.

<b>Architecture Principle</b> <i>12: Robustness</i>	Implemented infrastructure must be robust, responsive and reliable, with appropriate redundancy to protect against system failure.
--	--

## Standards

Standards are an integral part of information management. In print, many standards, such as the conventions used in publishing, have been virtually invisible. In other areas, such as records management, agencies operate within broad government-wide parameters but can also use standards they develop themselves.

With the growth of automated document handling systems and networking, effective information management is becoming increasingly dependent on adopting standards and protocols that support inter-agency and agency-client interoperability. Full interoperability consists not only of technical interoperability, but also functional interoperability—enabling people to use different systems but experience a familiar interface. With services and information increasingly delivered online, this focus is a critical element of architectural principles and strategies. It is also essential that standards encourage, rather than inhibit, the use of the online medium.

Recent experience selecting office automation and similar products suggests that the Commonwealth may need to accept that many of its information management standards will be driven by the wider global marketplace, primarily dominated by Europe, Japan and the United States. As a result, when adopting standards the Commonwealth needs to balance the risk of moving too quickly and selecting standards that do not find market favour, and being too late to prevent agencies from adopting incompatible approaches.

There may need to be a two-tiered approach to selecting standards, covering both existing and emerging standards. Although led by the market, the Commonwealth, in a small number of cases, may need to influence the development of standards that are particularly significant for, or unique to, government information management.

## Technical architecture

Technical architecture standards should provide a clear link between information technology projects and business practices. Simplification of agency collaboration on projects could provide savings through increased IT purchasing power and reduced training costs. Uniform architectural specifications should also reduce the complexity of some ICT tenders making it easier for companies to do business with the Commonwealth.

## Network architecture

The standards that are set as part of the network architecture will define the technologies to enable connections between government agencies and out to citizens and business. They may consist of facility designs, communication network components and protocols.

## **Operating environment**

A core set of business applications across the Commonwealth could reduce downtime when staff move from one agency to another. Agencies will have a requirement for their agency specific applications to meet individual business needs. Applications may already exist elsewhere in the APS to address these needs.

Agencies can design, acquire, develop, or enhance applications to share data and integrate processes with appropriate stakeholders. A total cost of ownership model for new applications will balance the costs of development, support, training, disaster recovery and retirement against the costs of flexibility, scalability, ease of use, and reduction of integration complexity. Applicable security, accessibility, confidentiality, and privacy policies also need to be included in systems development.

When designing applications or components of applications, agencies should consider flexibility and their underlying technology infrastructure. Applications should be scalable in size, capacity, and functionality to meet changing business and technical requirements.

## **INITIAL PRIORITIES**

---

The ITAG Sub-Committee created three working groups to examine three priorities common to all agencies: a) authentication of external clients; b) integration of service delivery; and c) government secure business systems. A summary of the working group reports, including suggested ongoing task lists, are at Appendix 3, 4 and 5. In addition to these working group priorities, the following three areas, which require immediate investigation, have been identified on the basis of the ITAG Sub-Committee's work.

### **Security**

The security framework for the federal government's use of ICT limits access to systems and processes. It comprises the technical structures, procedures, processes and intellectual capital, and is broad enough to cover the risks agencies face. A risk management approach can ensure a standard 'one size fits all' solution is not attempted. Security issues include authorisation, data integrity, authentication and confidentiality as well as technical elements such as firewall management, 'tunnelling'—for example, Fedlink—and protection of infrastructure.

The ITAG Secure Business Systems Working Group has been considering the Commonwealth's needs for secure inter-agency data communication and has identified a series of tasks to help move toward secure business capability (Appendix 3). The group is expected to provide a plan for a more coordinated approach to implementing inter-agency shared secure business processes, in consultation with the Defence Signals Directorate and the Australian Public Service Commission.

In the new era of e-Government, citizens' demands for services are a major driver for the nature and delivery mechanism of services provided by agencies. This requires many more sophisticated online services with transactional capability. It also requires associated services to be integrated wherever possible to provide clients with a more complete package of linked services.

Promoting public confidence in these services, including the need to authenticate users of government services, will remain a priority. The Authentication of External Clients working group has been looking at ways of achieving trust and confidence as well as ways to provide consistency of experience for users across government services (Appendix 5). It is expected that this working group will continue to develop proposals to realise these benefits.

### **New and second generation ICT sourcing models**

Some early outsourcing contracts for government ICT services are nearing completion and agencies need appropriate information to assist them in considering future arrangements. Many of the lessons learnt can benefit all agencies. An example is service level agreements regarding security, which were not as prescriptive as they might have been. The CIO Committee will facilitate learning and information exchange among agencies. The IMSC may decide that a working group is required to investigate this issue and develop templates to assist agencies considering second generation ICT sourcing.

There is a requirement for improving contract management skills within the Commonwealth. Agencies could work together to develop contract management templates that draw on the experiences of the Commonwealth in general and incorporate work completed by the Australian National Audit Office.

### **The human issues**

The success of ICT service delivery within the Commonwealth relies on staff having the knowledge and skills necessary to meet agencies' business requirements. Contract management is a key skill. The current competitiveness of the IT sector makes it difficult for agencies to retain the qualified staff they have. In addition, there is a perceived lack of suitably qualified or experienced employees in Australia. Recent experiences with government IT outsourcing have also encouraged staff to move to the private sector, further reducing the ICT skill pool across the Australian Public Service. The IMSC may decide it appropriate for a working group to consider these 'human issues' in regard to strong ICT management and support in the Commonwealth.

## AGREED APPROACH

---

## AGREED APPROACH

---

After considering the report of the ITAG Sub-Committee, the MAC agreed:

- The Governance Principles set out on page 12 as guiding principles for federal government agencies, noting that:
  - agencies will continue to manage their own information technology strategy, development, implementation and support; and
  - a federated approach to ICT governance in the Commonwealth is warranted where whole-of-government interoperability is an issue or a whole-of-government approach may be beneficial.
- The establishment of a new structure consisting of a two tiered peak level Information Management Strategy Committee (IMSC), supported by a Chief Information Officer (CIO) Committee. (The roles of these groups are outlined in Appendix 1 and 2.)
- The Architectural Principles set out on page 18 as guiding principles for federal government agencies.
- That the IMSC will approve a work plan for the CIO Committee that may include working groups to investigate specific areas of interest and operate for defined periods.
- An initial agenda for future strategic work, to include:
  - identification of significant issues related to investment in, and governance of, shared ICT infrastructure;
  - development of a model for architecture, governance and investment for the secure business systems of the Commonwealth;
  - development of a proposal for a new action plan for integrated service delivery (ISD), built on the work of ISD working group, with an action and investment plan, for consideration by government;
  - identifying the key lessons learned which would assist agencies entering into new and 'second generation' ICT sourcing agreements; and
  - authentication of clients.

## APPENDIXES

---

---

## **APPENDIX 1 - ROLE OF THE INFORMATION MANAGEMENT STRATEGY COMMITTEE (IMSC)**

---

### **Role:**

- To direct the CIO Committee work plan and to consider its proposals.
- To provide shared leadership on whole-of-government information management strategies.
- Within the governance principles, to develop policies, standards, specifications and guidelines for ICT that support business solutions for agencies as well as future interoperability.
- To identify and consider strategic information management approaches aimed at delivering whole-of-government benefits, and optimising potential gains.
- To promote ICT investment, architecture and governance arrangements for strategic projects that support innovative business solutions.
- To initiate research and development into matters affecting whole-of-government ICT activities.
- To sponsor key strategic issues for ministerial consideration.

### **Responsibilities and management:**

- The IMSC will be responsible to the MAC, act as a reference group for the Minister for Communications, Information Technology and the Arts (where appropriate) and draw on agencies with key central roles or major responsibility for delivering services online.
- The IMSC will also include representatives of the primary agencies involved in delivering programs and implementing policies that use ICT as an enabler.
- It will be chaired by the Secretary of the Department of Communications, Information Technology and the Arts.
- It will be serviced by NOIE and supported by the CIO Committee.

### **Membership:**

The IMSC will comprise a Chair and five to eight members at Secretary or CEO level, appointed by the MAC. The Chair of the CIO Committee (the CEO of NOIE) will be a member of the IMSC.

---

## **APPENDIX 2 - ROLE OF THE CHIEF INFORMATION OFFICER (CIO) COMMITTEE**

---

CIO Committee members will be drawn from both key central agencies and agencies that are high users of ICT. Members would normally be drawn from the agency's executive, and have responsibility for the nexus between business strategy and ICT strategy.

### **Role:**

- To develop and distribute policies, standards, specifications, and guidelines for ICT that will support business solutions for agencies while facilitating capacity for future interoperability.
- To develop guidance to agencies on information and information technology plans, drawing on best practice and highlighting issues relating to potential future interoperability, including appropriate monitoring of ICT procurement intentions to identify impediments to information policies, interoperability and standards.
- To consider across-government strategic projects referred by IMSC, and advise on appropriate ICT investment, architecture and governance arrangements that support innovative business solutions.
- To oversee research and development projects into matters affecting whole-of-government ICT activities identified by the IMSC.
- To establish working groups to assist the Committee, where appropriate.
- To work with appropriate agencies to ensure development of suitable information technology security and authentication policies.
- To facilitate and provide expert advice on plans for shared and common ICT-enabled business processes and respective budget requests, and recommend priorities to the IMSC.
- To promote the sharing of lessons learnt by agencies.

### **Responsibilities and management:**

- The CIO Committee will be chaired by the CEO of NOIE and supported by NOIE.
- It will be responsible to the IMSC.
- It will meet as required, and make use of working groups of Committee members and seconded agencies as required.

**Membership:**

There will be fourteen members, including ten permanent members and four non-permanent members appointed by the IMSC for set periods. The four non-permanent members may represent small agencies with areas of expertise in particular fields.

---

## **APPENDIX 3 - SECURE BUSINESS SYSTEMS WORKING GROUP**

---

### **IDENTIFIED WORK TASKS**

The working group categorised four significant risk areas:

#### **1. THE CULTURE OF SECURITY**

It is not possible to impose a security culture on agencies. Successful development and effective maintenance relies on active and willing cooperation of all staff in all areas.

##### **Suggested actions**

- Agencies should ensure that staff and management know and meet their obligations in relation to security as set out in the Australian Public Service Code of Conduct, the Protective Security Manual (PSM) and associated Australian Electronic Communications Security Instructions (ACSIIs) issued by the Defence Signals Directorate.
- Each agency needs to undertake a proactive role in creating a culture of security in relation to its operations, by learning from and using the skills found throughout the government. To reduce the cost for small agencies, there are opportunities for similar sized agencies or those with similar functions to collaborate with each other or create strategic partnerships with larger agencies.
- Agencies need support for the creation and delivery of security training modules as part of general staff training. This applies to all new starters as well as those moving into new roles with specific security requirements. These modules can be developed centrally. The 'probity culture' existing in agencies can, in part, be attributed to awareness of the requirement to comply with the Australian Public Service Code of Conduct.
- Senior management must take responsibility for implementing and monitoring security requirements at an agency level. The risks associated with inadvertent or malicious breaches of security need to be articulated and made available to decision makers.
- The Australian National Audit Office should review agencies' efforts to create cultures of compliance. Such audits would raise awareness about the importance of people and process issues as well as the physical, system and software measures necessary to create a secure environment.

## **2. EMAIL**

Email now represents the preferred method of communication; however, there is a gap in security standards, processes and systems for email.

### **Suggested actions**

- Investigate the development of non system-specific standards for the use of email services.
- Determine whether existing standards apply to the creation, storage and distribution of electronic documents. Alternatively, investigate the feasibility of reviewing 'traditional' registry standards to apply to electronic records and documents.
- Consider mandating the use of 'endorsed' email systems and web browsers for use by all agencies.
- Investigate development of a whole-of-government pricing regime that could assist smaller agencies.
- Encourage the use of Fedlink to manage security on inter-agency communication services.

## **3. 'APPLICATION TO APPLICATION' TRAFFIC**

The escalating pace of Government business and use of advances in technology has increased electronic transfer of data between different applications in separate agencies. In general, this type of traffic occurs on a point-to-point basis through leased lines. However, there is evidence of traffic occurring on public infrastructure, such as the Internet, and potential for this to increase.

### **Suggested action**

- Consider an ACSI-type instruction relating to applications development that would require data classification and secure storage issues to be identified and addressed effectively in the design stage. Where communication with another agency is envisaged, inter-agency secure communications should be fully implemented.

## **4. GOVERNANCE**

A robust governance arrangement will ensure that staff, agencies and government have certainty in their decisions about activities in the security environment.

## **Suggested actions**

- Conduct a benchmarking exercise to determine the level of security compliance in agencies. This would identify the size of the problem and provide a point against which to assess progress.
- Investigate ways and means of improving the process for the Evaluated Products List (EPL), which may include a more proactive approach to endorsement to lower the costs and length of time involved in getting products evaluated and on the EPL.
- Establish a best practice and assistance group, drawn from agency staff, to assist smaller agencies achieve compliance with PSM, ACSIs and other mandatory security directions.
- Establish whether security, governance and compliance could be strengthened through greater involvement by central agencies like the Attorney-General's Department, Defence Signals Directorate and Australian National Audit Office.

---

## **APPENDIX 4 - INTEGRATED SERVICE DELIVERY WORKING GROUP**

---

### **IDENTIFIED WORK TASKS**

The working group identified the following issues:

#### **1. DISCOVERY**

There are various ways of discovering government resources. IT-based ways include agency web sites, fed.gov, australia.gov, portals, metadata, and commercial search engines (Yahoo, Google etc).

#### **Suggested actions**

- Establish a high level board, comprising agency representatives, to set strategies for the management of operational issues for whole-of-government discovery infrastructures such as fed.gov and australia.gov. This board would support and extend the work of the current More Accessible Government Group (MAG).
- Strengthen the existing approach to implementing metadata to further support agency efforts to ensure that material is discoverable.
- In consultation with users, pursue new discovery mechanisms such as drop down menus of available service types. These might be adapted from service definitions contained in metadata.
- Continue engagement with commercial portals to improve discovery of government resources.
- Research how customers want to discover information/services online.

#### **2. CONTENT MANAGEMENT**

To help users find greater value from online services, a customer focus, rather than an agency-centric approach is required. The quality of material provided online is paramount. Agencies must understand who their customers are and what their customers find most useful. This includes design, structure, language, ease-of-use, and other issues. The development of architectural and governance principles will help deliver on the promise of easier access to government information and services, but the basic content should be of the highest quality at the outset.

#### **Suggested actions**

- Identify and test the specific requirements and expectations of customers.

- Implement a trial of solutions to meet these requirements through the portals framework.
- Evaluate and disseminate the results of the trial and use this knowledge to develop a Commonwealth framework for content management.
- Consider developing a Content Management Policy with guidelines covering the integrity, currency, reliability, useability, availability, security, privacy, ownership, recovery, storage, agility, maintenance and integration of digital information for the Commonwealth.

### **3. CHANNEL MANAGEMENT**

Service delivery channels include: call (telephony, including inbound and outbound); web (online) and email (interactive, personalised/tailored); visit (Commonwealth officers visiting clients at their premises); access (customers visiting Commonwealth premises); and paper (publishing, forms and processing, correspondence). Current agency channel management differs from agency to agency. There is no overarching government strategy for channel management and no consistent approach across government.

#### **Suggested actions**

- Undertake a stocktake/gap analysis of priority areas to map the various channels and uses by agencies of those channels.
- Engage with directory service providers to develop services akin to an online ‘Yellow Pages’ of government services.
- Develop a framework for management across different delivery channels.

### **4. DATA/PROCESS INTEGRATION**

Data/process integration is in its infancy. Some agencies share data for internal purposes and some Government initiatives are making process at a more customer-focused level. For example, the Business Entry Point’s Transaction Manager, which allows users to find, complete and manage online transactions with Commonwealth, State/Territory and Local Government agencies, and the Trials of Innovative Government Electronic Regional Services (TIGERS), which has demonstrated some different approaches. Suitable governance and investment structures for whole-of-government approaches are key enablers in the current highly devolved environment. An architectural framework should comprise: standards for security/privacy/authentication; protocols and standards for data exchange and integration; protocols and standards for business processes integration (eg. web services); system templates; and an overarching interoperability framework (see below).

### **Suggested actions**

- Develop a whole-of-government interoperability framework.
- Examine the appropriateness of developing an ongoing governance model.
- Examine funding options.
- Identify appropriate transactions to trial approaches to data/process integration.

## **5. INTEROPERABILITY FRAMEWORK FOR THE COMMONWEALTH GOVERNMENT**

The ITAG Sub-Committee meeting of 14 February 2002 noted that NOIE, in conjunction with the major Commonwealth service delivery agencies, is developing an interoperability framework for government electronic service delivery. Members noted that the draft framework would be an agenda item at the next meeting once the Integrated Service Delivery working group considered it.

The working group reviewed the framework at its March 2002 meeting and decided it was a good initiative. The framework has been further developed through extensive consultation at officer level and is now ready for more senior review.

### **Suggested actions**

- Circulate the attached consultation draft *Interoperability Framework for the Commonwealth Government* to all Commonwealth Chief Information Officers or equivalent, for comment.
- Commence the process of seeking ongoing commitment to implementing and making best use of the framework.
- Enrich the framework with appropriate standards, business or process rules, template agreements and instruments to improve interoperability between agencies. Agencies should cooperatively determine the scope and extent of these, taking into account developments in the private sector, in other jurisdictions and internationally.

---

## APPENDIX 5 - AUTHENTICATION OF EXTERNAL CLIENTS WORKING GROUP

---

### IDENTIFIED WORK TASKS

The working group identified the following key task areas:

#### 1. AUTHENTICATION OF INDIVIDUALS

There is no whole-of-government approach to the authentication of individuals, who must undertake different processes with different agencies when identifying themselves to access government services. The working group agreed that the integrity of the initial identification process is crucial to effective authentication in the online environment. Shortcomings in identity management were identified in the Attorney-General's Department (AGD) report, *Scoping Identity Fraud*.

#### Suggested actions

- Develop a framework for authentication requirements across government services that ensures consistency of experience for the customer, with consistent levels of authentication requirements linked to transaction types.
- Continue the strong link between the working group's activities and the Attorney-General's Department Memorandum to Cabinet on controlling and managing identity fraud. The working group's discussion paper on the management of individual authentication highlights options for providing consumers with greater control over their identity through smartcards. However, it also raises the sensitive issue of a single trusted identity management authority. These are complex issues that need further investigation across Government.
- Further investigate the need for individuals to provide common primary identity documents when registering with different government agencies. Achieving commonality across Government will help deliver consistency of experience for customers.
- Further investigate with State and Territory authorities possibilities for a national online identity document validation framework, particularly through births, deaths and marriages, and transport departments.

#### 2. AUTHENTICATION OF BUSINESSES

Business authentication is significantly more developed than individual authentication due to initiatives such as the Australian Business Number, Australian Business Number-Digital Signature Certificate (ABN-DSC) and the Business Authentication Framework. A key feature of these initiatives is their independent development by individual agencies rather than using a whole-of-government investment approach. Further work needs to be undertaken to increase take-up and penetration of the ABN-

DSC so that the whole information economy benefits through wider confidence in e-business transactions.

### **Suggested actions**

- Develop a cross-agency approach to implement a critical mass of transactions requiring an ABN-DSC through discussions of primary agency service providers to business, such as the Australian Tax Office and Customs.
- Work with ABN-DSC providers to develop a consistent liability approach for certificates so that they are accepted by all Commonwealth agencies.
- Monitor consideration by ABN-DSC providers of potential future charges to agencies for certificate validation processes.
- Encourage the further development of 'cross recognition' policies and processes with overseas authentication processes.

### **3. OTHER ACTIVITIES**

The working group reviewed the *Authentication Guide for Public Sector Managers* drafted by NOIE. The guide was finalised after extensive input from working group members. It was released by the Minister for Communications, Information Technology and the Arts, Senator the Hon Richard Alston in July 2002, in conjunction with a complementary guide for consumers and SMEs, *Trusting the Internet*.

### **Suggested actions**

- Continue to investigate non-repudiation possibilities with varying authentication technologies, as it will be a key issue in the validity of online transactions.



AUSTRALIAN  
PUBLIC SERVICE  
COMMISSION