National Office for the Information Economy:
Submission to the Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

Introduction

The National Office for the Information Economy (NOIE) welcomes the Committee's invitation to make a submission to this Inquiry into the Management and Integrity of Electronic Information in the Commonwealth. Trust – privacy, security and authentication - is a critical online enabler to engender confidence about the use of the electronic and online mediums to store data and conduct transactions.

It is recognised that the Commonwealth Government has a special role in engendering trust and confidence in the information economy. Some Commonwealth agencies have powers to compel individuals and organisations to provide information; others may exercise a virtual compulsion where information must be provided in order for the agency to grant a benefit, service or licence. In these circumstances the public must trust the Government to protect its holdings of and the way it uses personal, commercial and other sensitive information.

The trust that the public places in private sector organisations is fundamentally different to that it places in government agencies, primarily because there is choice and competition in the private sector. Citizens can take their business elsewhere if they are not satisfied. This is not the case with government agencies. Because they must trust government agencies to protect their information, individuals and organisations expect agencies to be worthy of their trust.

NOIE is working with a range of departments and agencies to build public trust and confidence in the electronic and online environment. This submission first briefly describes NOIE's role and activities, and then addresses the Terms of Reference.

NOIE's Role in the Information Economy

The National Office for the Information Economy:

- provides strategic advice to the Government on the key factors driving the information economy;
- coordinates the application of new technologies to government administration, information and service provision (including assistance to public sector bodies to deliver services online);
- Promotes the benefits of, and Australia's position in, the information economy; and
- Undertakes such other tasks related to the above functions as the Minister may require from time to time.

NOIE's key priorities in 2002 are to:

- develop strategic advice on the demand drivers for Broadband and provide the secretariat for the Australian Broadband Advisory Group;
- encourage economic transformation through better information and communications technology (ICT) use across the Australian economy;
- transform Australian government information services and administration through the application of ICT;
- map the long term uptake of e-business and e-procurement by small to medium business enterprises (SMEs) and
- promote e-security, facilitating implementation of a coordinated national e-security agenda.

To further the 3rd key priority (transforming Australian government information services and administration through the application of ICT), the *Better Services, Better Government* e-government strategy was launched by the Minister for Communications, Information Technology and the Arts, Senator the Hon Richard Alston, on 11 November 2002. This document can be accessed from:

http://www.noie.gov.au/publications/NOIE/better_services-better_gov/index.htm

Better Services, Better Government continues the emphasis on building user trust and confidence for government information and services held electronically and for electronic service delivery. This emphasis includes the importance of practical and effective arrangements, which respect existing privacy legislation in Australia, for ensuring the identity of individuals.

Concepts relevant to e-security, authentication and identification

E-security

E-Security is concerned with three main areas:

- Confidentiality - information should only be available to those who rightfully have access to it;
- Integrity - information should be modified only by those who are authorised to do so; and
- Availability - information should be accessible to those who need it when they need it.

Attacks on ICT systems (also called exploits) can be understood in reference to their effect on these three areas. For example, Denial of Service (DOS) attacks seek to make a service unavailable by disabling the relevant servers.

Defacement attacks on websites, while also being attacks on the availability of the organisation's publicly available information, may also be attacks on the integrity of this information. Other attacks on integrity may include the destruction of information and attempts to alter records. Trojan horses, viruses and other maleficent code may be used to attack the integrity of information.

Attacks on confidentiality involve the disclosure of information to parties who don't have rightful access to it. Trojan horses can be used to provide a hacker with remote control of infected computer and access to the information stored therein. Similarly recent virus attacks have taken control of the address list of e-mail applications and used these addresses to further promulgate the virus. These can be seen as attacks on the confidentiality of the user's address list.

Authentication

Authentication is a crucial aspect of information system management. Only users with legitimate access should be authenticated to a network or server.

Networks are held together by authentication protocols. Most users are familiar with logons and passwords. These access controls are commonly used to authenticate users to a network. Other access controls include one-time passwords, challenge and response systems, cookies, biometrics and PKI.

The NOIE Online Authentication Guide provides information for agencies on the range of access controls and authentication techniques and provides a framework for matching these to types of transactions.

Identification

Authentication is the process whereby a user can obtain rightful access to services or information. This process may not necessarily require the identification of the user but for high assurance transactions identification is usually required.

A face to face Evidence of Identity (EOI) process is usually required for the issue of digital certificates to individuals. Agencies currently employ a variety of EOI processes (often based on the 100 point check from the Financial Transaction and Reporting Act) to identify their clients. It is important that online authentication processes employed by agencies are based on robust EOI processes. There is a serious risk that, if this is not the case, personal information may be disclosed to the wrong person.

The most well known exploits around authentication and identification are known as identity fraud and identity theft. The former is the appropriation of an individual's identity in order to commit fraud. The latter often also incorporates fraud but also involves the impersonation of the individual in a number of contexts. In September 2001 the Attorney General released a public version of a report on Identity Fraud Risks in Commonwealth Agencies, entitled *Scoping Identity Fraud.* This report estimates the cost to Australia from identity related fraud to be in excess of $4 billion per annum. The report also points to high rates of forged identity documents. For example a study by Westpac and the NSW Registry of Births, Deaths and Marriages found 13% of birth certificates to be false.

Identity fraud and the authentication of agency clients are priority issues for the work of the Information Management Steering Committee.

Government Policy relevant to the Committee's Terms of Reference

The Commonwealth Government has a framework of policies in place to enhance the privacy, security and integrity of information stored, managed and transmitted by Commonwealth agencies. Key elements include:

1. The Protective Security Manual

The Commonwealth's Protective Security Manual (PSM) is issued by the Protective Security Coordination Centre (PSCC) within the Attorney-General's Department. It is the principal means for disseminating Commonwealth protective security policies, principles, standards and procedures to be followed by all Commonwealth agencies for the protection of official resources.

The recently revised PSM provides minimum common standards in protective security for all Commonwealth agencies and contractors and their employees performing services for and on behalf of the Commonwealth. These minimum standards ensure that there is a consistent approach to protective security within and between agencies.

The PSM has been widely distributed to agencies and compliance is required.

2. The Australian Communications-Electronic Security Instructions (ACSI) 33 guidelines.

ACSI 33 provides the formal basis for agencies to develop and implement effective IT and web site security practices. Compliance with ACSI 33 is mandatory for Commonwealth agencies.

3. Privacy Act

Commonwealth Government agencies must comply with 11 Information Privacy Principles which are set out at section 14 of the Privacy Act. These are based on the 1980 OECD guidelines governing the protection of privacy and transborder flows of personal data. The Privacy Commissioner has also issued a set of four guidelines about how to comply with the Information Privacy Principles in the online environment, and compliance with these guidelines was mandated by the Government as part of the Government Online strategy. The Guidelines are available at

http://www.privacy.gov.au/internet/web/index.html.

In addition, specific legislation imposes obligations in relation to tax file numbers, spent convictions, data-matching, and Medicare and Pharmaceutical Benefits Program information. Agencies are also bound by other specific legislation, such as secrecy provisions in their own legislation.

4. Gatekeeper Strategy

Gatekeeper is the Commonwealth Government's strategy for the use of Public Key Infrastructure (PKI) and a key enabler for the delivery of Government online services and e-commerce. Gatekeeper incorporates an accreditation regime for PKI service providers.

PKI is not a mandated technology – in fact NOIE's Online Authentication Guide for government agency managers surveys a range of authentication options and matches them to transaction types requiring different levels of assurance.

However, where an agency choses to use PKI for transactions with business or individuals it must be Gatekeeper accredited and any technology provider it uses must also be Gatekeeper accredited. To date eight organisations have been granted Gatekeeper Accreditation.

5. The Australian Business Number–Digital Signature Certificate

The Australian Business Number–Digital Signature Certificate (ABN-DSC) is a digital certificate linked to an entity's ABN. It provides the opportunity for Australian businesses to simplify their identity requirements when dealing online with government, as it enables any business entity to maintain a single electronic identity that will be accepted by Government agencies. Where a Commonwealth Government agency seeks to authenticate a business using a digital certificate, it must use an ABN-DSC.

More generally, the ABN-DSC will facilitate online service delivery and foster the use of digital certificates and e-commerce among Australian businesses. For example, the four major Australian banks have expressed an interest in having their digital certificates recognised as ABN-DSCs. The Government has agreed to this recognition, subject to the Commonwealth's framework requirements being met.

6. FedLink

FedLink is an innovative and cost-effective solution for enabling secure communications between Government agencies. It is a Virtual Private Network that provides secure and trusted communications across the Internet. The FedLink architectural framework provides:

- secure communications between Departments, Agencies, the Parliament and Ministerial offices, and
- an evolutionary path to e-business transactions, a knowledge-based environment and full multi-media applications.

Fedlink is fully implemented, making access available to all Commonwealth agencies. Thirteen agencies are currently using Fedlink More information on can be found at

http://www.fedlink.gov.au

NOIE's activities on e-security and authentication

NOIE plays a key role in the implementation of the policy framework around security and authentication. NOIE has a general policy role in defining standards and frameworks around Government use of online technologies, including online security. NOIE also has a role in managing Australia's broad interests in protecting the national information infrastructure.

In this capacity, NOIE chairs the peak Commonwealth e-security body, the Electronic Security Co-ordination Group (ESCG)**.** Other key members include the Attorney General’s Department, Department of Defence, Defence Signals Directorate, Australian Federal Police, Australian Security Intelligence Organisation, Department of Prime Minister and Cabinet, and the Department of Foreign Affairs and Trade.

The current work program for the ESCG includes:

- implementation of low cost information program targeted at small to medium enterprises and home-users;
- sponsoring initiatives to improve the IT security skills levels and increase research and development in e-security;
- improving the culture of security within Commonwealth Government agencies; and
- maintaining effective relationships with industry, State and Territory Governments and coordinating international activities.

A sub-committee of the ESCG, the Critical Infrastructure Protection Group (CIPG), chaired by the Attorney-General’s Department, is tasked with the responsibility of identifying and providing advice on the protection of Australia’s information infrastructure where information technology incidents may be defined as critical.

Through its website, NOIE publishes a large amount of material relating to these activities, which may be of interest to the Committee. A list of relevant activities of NOIE and other agencies, together with a brief description and the relevant URL, is at Attachment 1.

The building of a trusted information and communication technology environment for commonwealth agencies has been identified as a key priority of the newly-established Information Management Strategy Committee (IMSC), and its subsidiary body, the Chief Information Officer Committee (CIOC). The IMSC is the peak forum for considering the Commonwealth government’s information and communication technology strategies. It was established following consideration of the *Australian Government Use of Information and Communications Technology: A New Governance and Investment Framework* report, released by the Management Advisory Committee (MAC) on 15 October 2002.

Important agenda items for this new committee are secure business systems and the authentication of clients. NOIE provides support functions for the IMSC and the Chief Information Officer Committee (CIOC).

The Terms of Reference

The privacy, confidentiality and integrity of the Commonwealth's electronic data.

The policy framework outlined above is directed at ensuring the privacy and confidentiality of Commonwealth-held electronic data. Under the Privacy Act, the Financial Management and Accountability Act (FMA Act) and the PSM, the protection of information assets is the responsibility of each department and agency.

NOIE's role is to promulgate guidance and standards, to assist agencies and to facilitate synergetic cooperation between agencies and other parties. NOIE encourages agencies to employ risk management processes in line with the PSM to assess and manage their risks and threats.

The information that is available on the privacy, confidentiality and integrity of the Commonwealth's electronic data is limited. Please see Attachment 1 for information on the Online Surveys conducted by NOIE. These surveys, conducted by NOIE, were based on agency self-assessment. Agency advice was accepted. The last survey, Round 4, is over a year old.

Other information that may be relevant includes the Privacy Commissioner's Privacy Compliance Audit of Commonwealth Government Web Sites, (see http://www.privacy.gov.au/publications/wsr01.html) and the ANAO's Audit Report No. 13 on Internet Security within Commonwealth Government Agencies. While both of these are third party audits, their scope was mainly limited to website privacy and security.

The management and security of electronic information transmitted by Commonwealth agencies.

The transmission of electronic information by Commonwealth agencies includes information transmitted within agencies, between agencies and that transmitted from agencies to other parties. Major vectors of transmission are by websites and e-mail. Both these can pass over the public network (the Internet) or over private networks. Whether the Internet or a private network is used as the transmission medium is significant in terms of security. Fedlink has been designed and implemented to address the issues raised by the transmission of information between agencies over the Internet.

Many agencies now employ Intranets to make information available to their staff and a great deal of internal communication is taking place via e-mail within agency networks. Such internal networks and intranets are sequestered from the Internet by gateways employing firewalls and other security applications.

Both the Privacy Commissioner and the Defence Signals Directorate (DSD) provide guidance for public facing websites. These are Privacy Commissioner's Guidelines for Federal and ACT Government Websites which can be accessed from http://www.privacy.gov.au/internet/web/index.html, and DSD's Handbook 10 on Web Security which is part of ACSI 33. This can be accessed from the URL below.

http://www.dsd.gov.au/infosec/acsi33/HB10.html

Compliance with both the Privacy Commissioner's Guidelines and ACSI 33 was mandated by the Online Government Strategy and agencies were required to comply with them by the end of 2001.

The roles of the IMSC and the CIO Council are shown in Appendices 1 and 2 of the MAC report. Identified tasks from the Secure Business Systems Working Group are shown in Appendix 3 of the MAC report (*Australian Government Use of Information and Communications Technology: A New Governance and Investment Framework)*. This report can be seen at

http://www.noie.gov.au/publications/NOIE/MAC/MAC_NOIE_No21.pdf

The management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks.

Security and authentication are important issues for both centralised and distributed IT systems. Variations in network topology and configuration can have security implications but these can be managed within an overarching policy framework. Similar general security policies and principles will apply irrespective of the network topology employed.

DSD provides advice to agencies on technical issues around security and would be in a better position than NOIE to advise the Committee on any technical issues relating to this question.

The adequacy of the current legislative and guidance framework

Elements of the legislative and guidance framework undergo periodic review in order to maintain adequacy. For example, recent amendments to the Privacy Act strengthened the provisions relating to the outsourcing of applications where personal information may be passed by agencies to contractors. A review of the Privacy Act is scheduled to take place late in 2003.

The last issue of the PSM was in 2000 and it is currently undergoing revision. ACSI 33 is also periodically updated by DSD.

Assessment of the adequacy of the current legislative and guidance framework will be part of the work of the IMSC and CIO Council. Important agenda items for the IMSC are secure business systems and the authentication of clients.

NOIE's role in respect to this issue is to provide appropriate guidance, through seminars, publications and working groups, to help agencies understand and implement current legislative and guidance frameworks.

Attachment 1

NOIE's Activities around e-security and authentication

The NOIE Confidence, Trust and Security web page

This is a good starting point as it broadly sets out NOIE's activities in these areas.
http://www.noie.gov.au/projects/confidence/index.htm

Advancing Australia - The Information Economy Progress Report 2002

This report was launched by Senator Alston on 22nd November 2002. The Minister's Media release can be accessed at
http://www.noie.gov.au/publications/media_releases/2002/Nov2002/adv_aust.htm

The full report can be accessed from the URL below.
http://www.noie.gov.au/publications/NOIE/progress_report/start.htm

In the Introduction of the Progress Report is noted that "…e-security issues have risen up the agenda of governments world-wide in the wake of the September 11 terrorist attacks."

Chapter 5 of the Progress Report is entitled "A Framework for Trust and Security" and provides an overview of NOIE's activities around e-security and authentication.
http://www.noie.gov.au/publications/NOIE/progress_report/chap_5.htm

National E-security agenda.

In September 2002 the Commonwealth government announced measures to create a secure and trusted electronic operating environment for Australia. This is the National E-security agenda. Please see
http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm

The agenda encompasses the National Information Infrastructure (NII) which includes both the private and public sectors but it also specifically addresses Commonwealth Government issues. Please see
http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm#Government

Roles and responsibilities of NOIE and other agencies

NOIE has a general policy role in defining standards and frameworks around Government use of online technologies, including online security NOIE also has a role in managing Australia's broad interests in protecting the national information infrastructure. In this capacity, NOIE chairs the peak Commonwealth e-security body, the Electronic Security Co-ordination Group. The Defence Signals Directorate (DSD), the Attorney Generals Department and the Privacy Commissioner also have important roles. These roles are set out at the URL below.

http://www.noie.gov.au/projects/confidence/index.htm#cwealth

E-security R&D

In September 2001 NOIE published a *Report on E-security R&D in Australia, An Initial Assessment.* Key findings in respect to the Commonwealth were that The Defence Science and Technical Organisation (DSTO) and the Defence Signals Directorate (DSD) are the only Commonwealth organisation with a substantial e-security R&D program in place and that DSTO and DSD would like to increase the their links with Australian industry and academia. The full report can be accessed at http://www.noie.gov.au/projects/confidence/Protecting/RD_scoping_paper14-09-01.pdf

E-security Standards and guidelines

Commonwealth agencies are required to comply with a range of online security mandates and guidelines. These include the *Privacy Act 1988* and the Privacy Commissioner's Guidelines for Federal and ACT Government Websites, The Protective Security Manual (issued by the Attorney General's Department) and ACSI 33 (issued by DSD). In March 2000 the Commonwealth government mandated Commonwealth agency compliance with existing Commonwealth standards for information security and privacy and in November 2000 the government decided on an additional range of online security measures to apply in agencies. These included a more active coordination role for NOIE and increased agency reporting requirements on online security issues. More information can be found at http://www.noie.gov.au/projects/confidence/Securing/security.htm

Government Online Surveys

During 2000 and 2001 NOIE conducted a series of surveys of Commonwealth agencies to assess progress against the objectives of the April 2000 Government Online Strategy. The final survey was in October 2001. Some significant findings from the Round 4 Survey are:

- The most common impediments to using authentication and encryption were lack of resources (17%) and financial constraints (14%). Other impediments mentioned by 5% or more of agencies were difficulties with service providers, software, uptake and agency size.
- 40% of agencies state that they are fully compliant with the PSM and the ACSI-33 standard. This represents an increase from 31% in Round 3. Of those agencies not fully compliant, over half (54%) reported that they expect to fully comply by the end of 2001. Furthermore, two thirds (67%) of agencies using outsourced online service providers report that those providers are fully complying with appropriate security standards or practices, and of those not currently reporting full compliance, over half (60%) anticipate meeting the target by the end of 2001 – which will bring the total to 83% of agencies in full compliance.

- Agencies were asked to report how the Privacy Commissioner rated them in their most recent audit of compliance with the Commissioner's Guidelines for websites. Over 75% of agencies indicated that they met all four guidelines.

Most agencies reported that they expected to fully comply with the relevant standards by the end of 2001.

http://www.noie.gov.au/projects/egovernment/archive/online%5Fsurvey/r4%5Fresults/rd4-section%201.htm

The OECD Guidelines for the Security of Information Systems

The Organisation for Economic Co-operation and Development has released a new set of Information Security Guidelines to replace those previously made in 1992. The Australian Government, represented by officers from the Attorney-General's Department participated in the development of these Guidelines The new guidelines act as an important policy framework for the formation of e-security policies and practices for both private and public sectors within the OECD and aim to develop a "Culture of Security" within OECD economies. The full Guidelines can be accessed from the URL below.

http://www.oecd.org/pdf/M00034000/M00034292.pdf

A summary of the Guidelines can be accessed from

http://www.noie.gov.au/projects/confidence/Protecting/OECDPress_Release2.pdf

and Questions and Answers on the Guidelines from

http://www.noie.gov.au/projects/confidence/Protecting/Q&Arevised_Guidelines2.pdf

APEC Telecommunications Working Group

Australia currently holds the chair of this Group. The interests of this Group include Internet and e-commerce issues. Participation in this group is managed by DCITA and DFAT but NOIE provides input on e-commerce issues. The working Group website is at

http://www.apectel.com/apec/main.html

E-security Seminar

As part of the Government's e-security national agenda, NOIE and the DSD presented the 'E-security in Government' seminar. The seminar was held at the Australian Institute of Sport on September 11, 2002. Mr John Rimmer, CEO of NOIE delivered the opening address and Mr Stewart Skelt, Assistant Secretary, Department of Defence, delivered the Keynote address on 'The E-security Framework for the Commonwealth'. During the seminar, expert speakers also provided case study material and practical demonstrations of some of the information security dangers facing Commonwealth agencies. The agenda is at the URL below.

http://www.noie.gov.au/publications/presentations/esecurity/Agenda_11Sep02.pdf

The presentations given at the seminar can be accessed from the URL below.

http://www.noie.gov.au/projects/confidence/Protecting/index.htm

Online Authentication Guide

In July 2002 Senator Alston released this guide. It provides agencies with advice and guidance on key issues to consider when implementing authentication solutions in their e-business strategies. The Guide can be accessed at http://www.noie.gov.au/publications/NOIE/online_authentication/index.htm

This guide recently received favourable comment in the Spring 2002 edition of the CIO magazine. In an article entitled *Road Trip* by Andrea Di Maio the Guide was described in the following terms.

"…NOIE's recent document on authentication approaches is a comprehensive, down-to-earth, piece of guidance for all agencies, getting away from the more prescriptive (and restrictive) approach that other countries are promoting and stimulating a scalable, stepwise approach to this complex matter."

This article can be found at the following URL.

http://www.cio.com.au/idg2.nsf/AllCIO/EE0B1830A164EFE3CA256C7C00069E05!OpenDocument&NavArea=Topic+Centres&SelectedCategoryName=E-Strategies

The Guide provides advice on matching authentication levels to transaction types. This is an important consideration for online transactions as it provides a flexible approach to authentication for agencies implementing online transactions.

Trusting the Internet

Trusting the Internet is a publications that helps small business owners and operators understand e-security issues. This was launched by the Senator Alston on July 16 2002. This document can be accessed at

http://www.noie.gov.au/publications/NOIE/trust/index.htm

Gatekeeper

Gatekeeper is the Commonwealth Government's strategy for the use of Public Key Infrastructure (PKI) and a key enabler for the delivery of Government Online and e-commerce. Gatekeeper incorporates an accreditation regime for PKI service providers. The accreditation criteria include

- compliance with Commonwealth Government procurement policy;
- security policy and planning;
- physical security;
- technology evaluation;
- Certification Authority policy and administration;
- personnel vetting;
- legal issues; and
- privacy considerations.

To date eight organisations have been granted Gatekeeper Accreditation. These are SecureNet, PricewaterhouseCoopers (beTRUSTed), Australia Post Telstra Corporation Limited, eSign Australia Limited, Health eSignature Authority Pty Ltd, Baltimore Certificates Australia Pty Ltd (CAPL) and the Australian Taxation Office. For further information on Gatekeeper please see

http://www.noie.gov.au/projects/confidence/Securing/Gatekeeper.htm

The Australian Business Number Digital Signature Certificate (ABN-DSC)

The ABN-DSC is a digital certificate linked to an entity's ABN. It will facilitate online service delivery and foster the use of digital certificates and e-commerce among Australian businesses. It simplifies the identity requirements for Australian businesses when dealing online. It also enables any business entity to maintain a single electronic that will be accepted by all Government agencies. For further information see

http://www.noie.gov.au/projects/confidence/Improving/abn-dsc.htm

Project Angus

This project involves Gatekeeper recognition of Australian banks that have received accreditation under the Identrus PKI scheme. On 22 March 2001 Senator Alston announced that digital signature certificates issued by the Australian banks to businesses will be accepted by government agencies. These digital certificates will be regarded as ABN-DSC digital certificates. E-commerce in Australia will be simplified by allowing businesses to use one digital certificate to carry out online transactions with banks, trading partners and government agencies. For further information see the Frequently Asked questions at

http://www.noie.gov.au/projects/confidence/Improving/abn-dsc-angus.htm

The National Authentication Technology Framework

In May 2002 NOIE released a discussion paper on the potential for a National Authentication Technology Framework. The paper broadly looked at the trends in relation to authentication technologies (PINS, passwords, PKI, SSL, biometrics), and considers the possible future of the Gatekeeper accreditation framework, and NOIE's role in relation to authentication technologies (PKI and biometrics in particular). The consultation paper can be found at

http://www.noie.gov.au/publications/NOIE/Authentication/NATF_Discussion_paper_July2002.pdf

NOIE hosted discussion fora of interested stakeholders in Canberra, Sydney, Melbourne and Adelaide. The results of these consultations can be found at

http://www.noie.gov.au/publications/NOIE/Authentication/NATF_Discussion_paper_July2002.pdf

Further consultations with the key players are planned for December 2002.

The Business Authentication Framework (BAF)

The Business Authentication Framework (BAF) is intended to provide easy to use and cost-effective validation services and common use signing interface between e-commerce partners and participating Commonwealth, State and Local Government agencies. The BAF is a Commonwealth Government initiative undertaken by the Commonwealth Department of Employment and Workplace Relations (DEWR), the Australian Taxation Office (ATO) and the Business Entry Point in consultation with the National Office for the Information Economy. Trials of the framework are planned with major applications at DEWR and ATO. Further information can be accessed from the BAF website below.

http://www.BAF.gov.au

The Information Management Steering Committee (IMSC)

The Information Management Strategy Committee (IMSC) is the peak Commonwealth information technology strategy body. It was established as a result of a recommendation outlined in the *Australian Government Use of Information and Communications Technology: A New Governance and Investment Framework* report. This was released as a Management Advisory Committee (MAC) report on 15 October 2002. One of the IMSC's activities will be facilitating the building of a trusted ICT environment. Important agenda items for this new committee are secure business systems and the authentication of clients. For more information please see the IMSC website below.

http://www.IMSC.gov.au

NOIE provides support for the IMSC and the Chief Information Officer Committee (CIOC). The CIOC is a sub-committee of the IMSC which is a sub-committee of the Management Advisory Committee (MAC).