An Agreement to a National Identity Security Strategy

AN AGREEMENT

Between

The COMMONWEALTH OF AUSTRALIA and

The STATE OF NEW SOUTH WALES;

The STATE OF VICTORIA;

The STATE OF QUEENSLAND;

The STATE OF WESTERN AUSTRALIA;

The STATE OF SOUTH AUSTRALIA;

The STATE OF TASMANIA;

The AUSTRALIAN CAPITAL TERRITORY; and

The NORTHERN TERRITORY OF AUSTRALIA

April 2007

An Agreement to a National Identity Security Strategy

This Agreement is entered into by the Commonwealth of Australia, the States of New South Wales, Victoria, Queensland, Western Australia, South Australia, and Tasmania, the Australian Capital Territory and the Northern Territory ('the Parties').

Recitals

1. On 14 April 2005, the Commonwealth Government announced plans to develop a national strategy to combat identity theft and the fraudulent use of stolen and assumed identities as a matter of national priority.

2. The Commonwealth Government noted that the national strategy would be developed in partnership with State and Territory Governments, recognising their joint responsibility for the issuing of documents that are widely accepted in the community as evidence of a person's identity.

3. At its Special Meeting on Counter-Terrorism on 27 September 2005, the Council of Australian Governments (COAG) agreed that the preservation and protection of a person's identity is a key concern and a right of all Australians. COAG agreed to the development and implementation of a national identity security strategy to better protect the identities of Australians. The strategy will enhance identification and verification processes and develop other measures to combat identity crime, and will be underpinned by an inter-governmental agreement.

4. COAG also agreed to:

   (a) develop and implement a national document verification service to combat the misuse of false and stolen identities, and

   (b) investigate the means by which reliable, consistent and nationally interoperable biometric security measures could be adopted by all jurisdictions.

5. ***DEFINITIONS***

In this Agreement, unless a contrary intention is apparent:

"Agreement" means this document and includes the Attachment

"Commonwealth" means the Commonwealth of Australia

"Government agencies" means Commonwealth, State and Territory agencies

"**Identity crime**" is a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of crime

"**Identity fraud**" is the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity

"**Identity theft**" is the theft or assumption of a pre-existing identity (or a significant part thereof), with or without consent, and whether, in the case of an individual, the person is living or deceased

"Jurisdiction" means the Government jurisdiction of any of the Parties

"State(s) and Territory(ies)" means the State and Territory Governments.

The Strategy

6. This Agreement outlines the elements of a National Identity Security Strategy (NISS) including undertakings to further develop and implement the NISS to give effect to the COAG commitments. The NISS will provide a framework for inter-governmental cooperation to strengthen Australia's personal identification processes.

7. The Parties agree to work together to develop and implement the NISS comprised of the following elements:

7.1 registration and enrolment standards for use by agencies which enrol individuals to issue government documents that also may function as key documents for proof of identity purposes;

7.2 security standards for such documents to reduce the possibility of forgery or unauthorised alteration of documents;

7.3 improved ability for Government agencies across jurisdictions to verify information on such documents;

7.4 standards in the processing and recording of identity data to improve the accuracy of existing records (where appropriate) and to prevent the creation of inaccurate identity records in future;

7.5 standards for Government agencies to apply where they provide services to a person whose identity needs to be verified and there are significant risks associated with the wrong person getting access to a service; and

7.6 measures to enhance the national interoperability of biometric identity security measures.

The *Work Program* at **Attachment A** provides further detail to the elements of the NISS, and must be considered as a work-in-progress requiring further consideration.

8. The Parties agree to develop and implement the NISS by:

8.1 identifying possible common approaches in the field of identity security in Australia, based on an understanding of deficiencies, problems, challenges and risks;

8.2 taking into account the needs of Commonwealth, State and Territory Governments and their agencies in considering common approaches;

8.3 ensuring that approaches devised to improve identity security processes are sufficiently flexible to take account of emerging technologies, are proportionate to the risk involved and achieve their objectives;

8.4 balancing the privacy, civil liberties and broader community interests in the development and implementation of robust identity security (where possible, identity security initiatives will be implemented in a privacy-enhancing manner); and

8.5 designing programs and procedures to implement the NISS, including the development of a national document verification service, and measures to enhance the national interoperability of biometric identity security measures.

Working Arrangements

9. The Parties agree to:

9.1. work collaboratively and cooperatively to strengthen identity security for the Australian community;

9.2. consult with each other on matters of shared interest and benefit;

9.3. work together to raise community awareness of the risks of identity theft and identity fraud, so that citizens are better equipped to protect their identities;

9.4. engage with the private sector in developing elements of the NISS to take into account business practice and make best possible use of private sector expertise; and

9.5. consider the privacy impacts for their jurisdictions of national identity security initiatives.

Governance

10. The Parties agree:

10.1 that the National Identity Security Coordination Group ("the Coordination Group") will be the primary vehicle for developing the details of the NISS and will be required to report back to COAG within 12 months from the commencement of this IGA and annually thereafter;

10.2 that the Coordination Group have representation from First Minister Departments of the Commonwealth, State and Territory Governments and/or their designated representatives, the Council of Australasian Registrars for Births, Deaths and Marriages, the lead agency for the Certificate Validation Service, Austroads and the Federal Privacy Commissioner;

10.3 that the representatives on the Coordination Group provide a central point of coordination for consultation with stakeholders and representation of stakeholder interests from their respective jurisdictions;

10.4 that the Coordination Group establish working groups with representation from Commonwealth, State and Territory Governments to develop proposals for its consideration, with Chairs to be determined by the Coordination Group; and

10.5. to review the role of the working groups and disband or establish groups as requirements change.

Commencement

11. This Agreement commences immediately upon its execution by the Parties.

Review of the Agreement

12. The Parties agree to review this Agreement after three years of operation to assess the circumstances and the necessity for this Agreement to continue.

Variation, Withdrawal and Termination of the Agreement

13. Amendments to this Agreement may only be made with the written consent of all Parties.

14. This Agreement may be terminated at any time by agreement in writing by all the Parties and under any terms and conditions as agreed by all the Parties.

15. A Party may withdraw from this Agreement by giving not less than three months notice, in writing, to each of the other Parties.

16. If a Party withdraws from this Agreement, this Agreement will remain in force in relation to the remaining Parties.

Signed for and on behalf of each of the Parties by:

The Hon John Howard, MP)
Prime Minister of Australia)

The Hon Morris Iemma, MP)
Premier of New South Wales)

The Hon Stephen Bracks, MP)
Premier of Victoria)

The Hon Peter Beattie, MP)
Premier of Queensland)

The Hon Alan Carpenter, MLA)
Premier of Western Australia)

The Hon Michael Rann, MP)
Premier of South Australia)

The Hon Paul Lennon, MHA)
Premier of Tasmania)

Jon Stanhope, MLA)
Chief Minister of the Australian Capital Territory)

The Hon Clare Martin, MLA)
Chief Minister of the Northern Territory)

ATTACHMENT A

WORK PROGRAM

ELEMENTS OF THE NATIONAL IDENTITY SECURITY STRATEGY

Identity security is a critical concern to Commonwealth, State and Territory governments which have responsibility for Australia's national security, revenue protection and law enforcement. False identities underpin some terrorist and criminal activity and undermine border and citizenship controls and efforts to combat terrorist financing and financial crime. Identity theft is also a major invasion of privacy and a serious concern to the Australian community. It is essential to Australia's security and economic interests that the identities of persons accessing government or commercial services, benefits, official documents and positions of trust, can be accurately verified.

Identity security is a whole-of-government cross-jurisdictional issue. Developing and implementing the National Identity Security Strategy (the Strategy) will require a comprehensive and collaborative effort between and within jurisdictions.

The National Identity Security Coordination Group (the Coordination Group) has worked collaboratively as a whole-of-government body and has given significant consideration to responses which will achieve the elements of this Agreement. The Coordination Group has mapped out six elements, as described below. The elements will provide a framework for strengthening national arrangements at each point along the identity security continuum.

Substantial work has been completed by working groups, which report to the Coordination Group, on the six elements. Jurisdictions recognise the value of the work done to date, and the scope for jurisdictions which so choose to make use of this work in the further refinement of their own identity security frameworks. It is noted that the working groups will continue to develop a work program to finalise elements in accordance with this Agreement.

The items of work elaborated in this document are intended to be used to enhance identity security standards and procedures in accordance with relevant policy priorities, security risk assessments and legislative requirements. The Coordination Group will present these elements for consideration by COAG.

The six elements of the Strategy being developed in accordance with the Agreement are:

Registration and Enrolment Framework
It is intended that this element (*Clause 7.1 of Agreement*) will be a common set of standards for use by agencies which enrol individuals for the purpose of issuing high integrity government documents that also may function as key documents for proof of identity purposes. It will form the basis for, and operate in conjunction with, other elements of the Strategy;

Security Standards for Proof of Identity Documents
It is intended that this element (*Clause 7.2 of Agreement*) will provide minimum security standards for key proof of identity documents, with the aim of reducing the risk of forgery or unauthorised alteration of documents.

The work will also devise a system of categorisation for proof of identity documents based on assessed risk and levels of confidence required, and recommend appropriate technical security features suitable for each category of document to meet those standards;

Document Verification Service (DVS)
Development and implementation of a national DVS was specifically agreed to by COAG in September 2005. A pivotal component of any identity security architecture is the ability to verify the documents presented as proof of an individual's identity were in fact issued by the issuing agency.

The Coordination Group will be responsible for the development and implementation of a fully-fledged national DVS (*Clause 7.3 of Agreement*) which will enable agencies across jurisdictions to verify the bona fides of documents presented by applicants as proof of identity. The design and specification of the DVS will require the collaboration and active participation of all jurisdictions, taking into account the current operating environment and systems, to verify data on key proof of identity documents submitted by clients registering for services.

The DVS will provide an enhanced on-line service to allow key proof of identity documents that have been presented to be verified by agencies which issue such documents.

The DVS would be an important contribution to an enhanced identity security regime;

Integrity of Identity Data
Variations in the processing and recording of identity data between agencies, and changes over time, can result in excess, redundant or incorrect identity records. Inaccurate identity records undermine governments' ability to properly allocate entitlements, collect revenue, provide services effectively and efficiently, and comply with privacy obligations.

Improving the integrity of agency identity data holdings is a key element of the Strategy (*Clause 7.4 of Agreement*). In particular, improvements to the integrity of agency identity data holdings are necessary to ensure the effective operation of the national DVS.

It is intended that this stream of work will devise standards that will provide guidance on improving the accuracy of personal identity information held on government agencies' databases, including correcting existing records (where appropriate) and ensuring that personal information is collected and held in accordance with relevant privacy legislation;

Authentication Standards

It is proposed that this element (*Clause 7.5 of Agreement*) will describe standards that Government agencies could apply where:-

(a) they authenticate identity electronically for the purpose of providing service; and

(b) there are significant consequences if the wrong person gets access to a service (that is, there is a high level of risk associated with the transaction); and

Biometric Interoperability

Traditionally, identity verification has relied on "something you know", such as a password or personal identification number, or on "something you have", such as a smart card or access device.

Biometrics offer the advantage of being based on the unique physical characteristics of an individual - "something you are". They can provide the missing link between these traditional 'credentials' and their authorised users. They can also be used to link the appearances of otherwise unknown individuals.

Biometrics also have the capacity to be both privacy enhancing and privacy invasive depending on the uses to which they are put.

This element (*Clause 7.6 of Agreement*) will outline types of biometric systems, issues about standardisation and interoperability and community acceptance. It will consider the means by which reliable, consistent and nationally interoperable biometric identity security measures could be adopted by all jurisdictions to reduce the risk and incidence of identity forgery, taking into account potential community concerns.