

The Auditor-General  
Audit Report No.29 2009–10  
Performance Audit

**Attorney-General's Department  
Arrangements for the National Identity  
Security Strategy**

Australian National Audit Office

© Commonwealth  
of Australia 2010

ISSN 1036-7632

ISBN 0 642 81119 9

## **COPYRIGHT INFORMATION**

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth.

Requests and inquiries concerning reproduction and rights should be addressed to:

Commonwealth Copyright  
Administration  
Attorney-General's Department  
3-5 National Circuit  
Barton ACT 2600

<http://www.ag.gov.au/cca>



Canberra ACT  
21 April 2010

Dear Mr President  
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the Attorney-General's Department in accordance with the authority contained in the *Auditor-General Act 1997*.

Pursuant to *Senate Standing Order 166* relating to the presentation of documents when the Senate is not sitting, I present the report of this audit and the accompanying brochure. The report is titled *Attorney-General's Department Arrangements for the National Identity Security Strategy*.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—<http://www.anao.gov.au>.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Ian McPhee', is positioned above the printed name.

Ian McPhee  
Auditor-General

The Honourable the President of the Senate  
The Honourable the Speaker of the House of Representatives  
Parliament House  
Canberra ACT

## AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:  
**The Publications Manager**  
**Australian National Audit Office**  
**GPO Box 707**  
**Canberra ACT 2601**

**Telephone:** (02) 6203 7505  
**Fax:** (02) 6203 7519  
**Email:** [webmaster@anao.gov.au](mailto:webmaster@anao.gov.au)

ANAO audit reports and information about the ANAO are available at our internet address:

<http://www.anao.gov.au>

---

**Audit Team**  
Charles Higgins  
Amanda Hall  
Tom Clarke

# Contents

Abbreviations.....	7
<b>Summary and Recommendations .....</b>	<b>9</b>
Summary .....	11
Introduction .....	11
Audit objectives and scope .....	13
Overall conclusion.....	13
Key findings by chapter.....	15
Summary of agency response .....	18
Recommendations .....	19
<b>Audit Findings and Conclusions .....</b>	<b>21</b>
1. Background and context .....	23
Introduction .....	23
The National Identity Security Strategy.....	27
Audit approach .....	31
2. Governance.....	33
Introduction .....	33
Overview of NISS governance bodies .....	33
Specification of roles and responsibilities in relation to developing and implementing the NISS .....	37
3. Progress against the NISS elements .....	40
Introduction .....	40
Progress achieved against the elements of the NISS .....	40
Contribution of each element to the overall NISS objective.....	50
4. Departmental arrangements for developing the NISS .....	51
Introduction .....	51
Planning framework .....	51
Monitoring and reporting of performance.....	55
Project resourcing and management.....	57
<b>Appendices .....</b>	<b>59</b>
Appendix 1: Formal comments on the proposed report .....	61
Appendix 2: Other Australian Government initiatives and international approaches to identity security.....	66
Appendix 3: List of POI document types .....	68
Appendix 4: POI framework.....	71
Appendix 5: Progress of the NISS elements (nDVS excluded).....	72
Series Titles.....	76
Current Better Practice Guides .....	79

## Tables

Table 1	NISS six elements .....	12
Table 1.1	Commonly used POI documents.....	26
Table 1.2	NISS six elements and associated work program.....	29
Table 1.3	Key milestones in the development and implementation of the NISS .....	31
Table 3.1	List of MOUs for the nDVS .....	45
Table 4.1	nDVS funding and expenditure by AGD (\$m) .....	57
Table A 1	List of commonly accepted Proof of Identity (POI) document types .....	68
Table A 2	POI framework as presented in the Report to Council of Australian Governments, April 2007.....	71

## Figures

Figure 1.1	Examples of acceptable POI documents .....	25
Figure 2.1	National Identity Security Strategy group structure.....	34
Figure 2.2	NISCG working groups.....	35
Figure 3.1	Information flows of nDVS.....	43
Figure 3.2	Number of nDVS responses.....	49

# Abbreviations

---

AGD	Attorney-General's Department
ANAO	Australian National Audit Office
BDM	Births, Deaths and Marriages registry
CIU	Cabinet Implementation Unit
COAG	Council of Australian Governments
CRG	Commonwealth Reference Group
CVS	Certificate Validation Service
DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
GSEF	Gold Standard Enrolment Framework
GSAR	Gold Standard e-Authentication Requirements
IGA	Intergovernmental Agreement
nDVS	national Document Verification Service
NeAF	National e-Authentication Framework
NISCG	National Identity Security Coordination Group
NISS	National Identity Security Strategy
pDVS	prototype Document Verification Service
POI	Proof of Identity
RTA	Roads and Traffic Authority
SS for POI	Security Standards for Proof of Identity documents





# **Summary and Recommendations**



# Summary

---

## Introduction

1. The misuse of false or stolen identities—commonly referred to as identity crime—poses significant threats, both in terms of national security and crime more generally. Recent estimates suggest that identity theft, a subset of identity crime, is a problem that costs the Australian economy approximately AUD\$1 billion per year.<sup>1</sup> In turn, identity security is becoming increasingly central to Australia’s national security, law enforcement and economic interests, and those of the global community generally.<sup>2</sup>

2. Identity security relates to the use and holdings of personal information. Credentials containing personal information are used extensively by individuals in interactions with the government and private sector. In the absence of a uniform national identity document, Australia relies on a range of credentials, issued for primarily operational purposes, which are routinely used by agencies, business and individuals as de-facto proof of identity (POI) documents. The current range of identity-related credentials are of variable quality and accuracy, which exposes individuals, business and government to many risks from not being able to verify that a person is who they claim to be. Within Australia, being able to verify with confidence an individual’s identity is balanced against privacy considerations and broader community interests.

3. Over the last decade, the differing standards and inherent risks within Australia’s identity security framework has resulted in the Australian Government intensifying its focus on identity security. In 2005, the Australian Government announced the need for a National Identity Security Strategy (NISS) to combat identity crime and the fraudulent use of stolen and assumed identities as a matter of national priority. Subsequently, the Council of Australian Government (COAG) agreed that the preservation and protection of a person’s identity is a key concern and a right of all Australians. In 2007,

---

<sup>1</sup> OECD Committee on Consumer Policy, *Online Identity Theft*, February 2009, p. 37.

<sup>2</sup> *ibid.* See also: Securities Industry Research Centre, *Identity Fraud in Australia: an Evaluation of its Nature, Cost and Extent*, 2003, ANAO Audit Report No. 24 2007-08, *DIAC’s Management of the Introduction of Biometric Technologies*, p. 34, and ANAO Better Practice Guide, *Fraud Control in Australian Government Agencies*, August 2004, Canberra.

COAG agreed to the development and implementation of the National Identity Security Strategy (NISS) to better protect the identities of Australians.

4. The first public articulation of the NISS was through an Intergovernmental Agreement (IGA) signed by all signatories to COAG in 2007. The NISS represents the current articulation of Australian, state and territory government policy. The NISS IGA contains a collective commitment from all governments to develop and implement the NISS and states that ‘the NISS will provide a framework for intergovernmental cooperation to strengthen Australia’s personal identification processes.’<sup>3</sup> To support the objective of the NISS, there are six distinct elements represented in Table 1.

**Table 1**

**NISS six elements**

NISS element	Element description
1. Registration and enrolment standards	Registration and enrolment standards for use by agencies which enrol individuals to issue government documents that may also function as key documents for proof of identity purposes.
2. Security standards for proof of identity documents	Security standards for such documents to reduce the possibility of forgery or unauthorised alteration of documents.
3. Document verification service	Improved ability for government agencies across jurisdictions to verify information on such documents.
4. Standards in the processing and recording of identity data	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.
5. Authentication standards	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.
6. Biometric interoperability	Measures to enhance the national interoperability of biometric identity security measures.

Source: COAG, *An Agreement to a National Identity Security Strategy*, 2007.

5. The six interdependent elements of the NISS have varying requirements from developing standards through to the building of information systems. Certain elements (for example, security standards and an improved ability to verify key documents) rely on other elements (registration and enrolment standards for such key documents). The six elements of the NISS are closely linked, may operate in close conjunction with one another, and are mutually enforcing.

<sup>3</sup> COAG, *An Agreement to a National Identity Security Strategy*, 2007.

6. The NISS IGA establishes the overarching governance of the NISS including the National Identity Security Coordination Group (NISCG), which incorporates broad representation from Australian, state and territory agencies. The NISCG is also 'the primary vehicle for developing the details of the NISS'.<sup>4</sup> The NISS IGA establishes an internal review mechanism whereby all parties have agreed to assess the circumstances of, and the necessity for, the agreement to continue from April 2010.

7. The Attorney-General's Department (AGD), through its mandate to 'coordinate federal criminal justice, security and emergency management activity, for a safer Australia'<sup>5</sup>, and Ministerial direction, is the lead Australian Government agency for identity security issues, including coordinating the development of the NISS.

## Audit objectives and scope

8. The objective of the audit was to assess the effectiveness of AGD's arrangements for coordinating the development of the National Identity Security Strategy.

9. ANAO's assessment was based on the following criteria:

- governance arrangements for the NISS;
- progress, to date, of the six NISS elements; and
- AGD's administrative arrangements for developing the NISS.

## Overall conclusion

10. Australia has a system of diverse personal identification credentials, issued for primarily operational purposes, which are routinely used by Australian Government agencies, business and individuals as de-facto identity documents. The current patchwork of identity-related credentials are of variable quality and accuracy, which exposes government, business and individuals to a variety of risks from not being able to verify a person is who they claim to be.

---

<sup>4</sup> COAG, *op. cit.*, p.3.

<sup>5</sup> Commonwealth of Australia, *Portfolio Budget Statements, Attorney Generals Portfolio 2009–10*, p. 2.

11. In 2007, the Australian, state and territory governments, as part of a COAG initiative, agreed through an Intergovernmental Agreement (IGA) to the National Identity Security Strategy (NISS). The NISS, when developed and implemented, was intended to provide a framework for intergovernmental cooperation to strengthen Australia's personal identification processes. The NISS is a body of work dependant on complementary actions by different agencies, the majority of which are located in Australia's states and territories. For the Australian Government, AGD is the lead agency for identity security issues and has lead responsibility for coordinating the development of the NISS. Overall, the ANAO concluded that there has been progress in the development of the NISS and its six elements but it is apparent that there are opportunities for AGD to build on the work achieved to date to strengthen the integrity of Australia's personal identification processes.

12. The department has established some of the foundation elements necessary to develop a whole-of-government initiative, such as: interdepartmental committees; development of the necessary infrastructure for the national Document Verification Service (nDVS); and a consultation process that has involved a diverse range of stakeholders. However, under the current governance arrangements, no agency is in a position to accept accountability for the implementation of the NISS elements. Clear identification of the key parties to the NISS and their roles and responsibilities with regards to implementation of the NISS elements would bring the NISS into line with other more recent IGA's and enhance the accountability for key NISS elements. Given its role in coordinating the development of the NISS, AGD is well placed to lead a process to clarify the governance arrangements for the strategy.

13. Progress in implementing the elements of the NISS by the parties to the IGA, as originally intended, has been limited. A range of activities tied to the six NISS elements has been undertaken which, in many cases, does not align with the original intended outcomes. The one budget funded element of the NISS, the nDVS, has been built and a range of document issuing agencies have been connected to the system, albeit more slowly than expected. However, the system is rarely used and presently, it is making little contribution to the NISS objective of strengthening Australia's personal identification processes. The passage of time and the lessons learned from the NISS related activities indicate that it is appropriate to revisit the rationale for, and appropriateness of, the NISS and its specific elements in a structured way by AGD and the NISCG.

14. The AGD's administrative arrangements to support the NISS include the planning for, and managing of, progress and specific project resourcing. Project management principles have only been applied to one element of the NISS, the nDVS, and in practice key project risks that were identified, have materialised and remediation strategies have taken longer than expected to come into effect. A more robust approach to planning and managing the implementation would have likely assisted in providing greater discipline to progress specific NISS elements, through the articulation of a shared understanding of the intended outcomes and monitoring of progress.

15. The ANAO made three recommendations aimed at improving AGD's co-ordination of this whole-of-government initiative.

## Key findings by chapter

### Governance (Chapter 2)

16. The governance framework for implementing the NISS was established by the NISS IGA, signed in April 2007. The NISS IGA establishes the National Identity Security Coordination Group (NISCAG) that is the key oversight body responsible for reporting to COAG. AGD has also established a Commonwealth Reference Group (CRG) to coordinate Australian Government involvement for identity security related matters. The specific role and consequences of actions of the CRG, however, is unclear as there are no terms of reference or clear mandate.

17. To support the NISCAG, AGD has established various working groups that are aligned to the six NISS elements. AGD has also facilitated new working groups to coordinate the development of the whole-of-government responses to emerging risks, such as the 2009 Victorian bushfires. Overall, the framework of the working groups under the NISCAG has allowed the convergence of various stakeholders in a structured forum to share experiences and work towards implementing proposals for improved disaster management and recovery operations.

18. The NISS IGA outlines the six elements and includes 'undertakings to further develop and implement the NISS to give effect to COAG commitments'.<sup>6</sup> Notwithstanding the text of the NISS IGA, AGD advised

---

<sup>6</sup> COAG, op. cit., p. 3.

ANAO that the department did not consider 'that the NISS IGA provides a mandate for the *implementation* of measures'. AGD's approach in relation to NISS has been consistent with this perspective. While implementation of particular standards related to NISS elements will be a matter for each jurisdiction, a consequence of this approach is that no agency is in a position to accept accountability for the implementation of the NISS elements. In the case of AGD, the Australian Government 'lead agency' considers it has limited leadership authority and no responsibility in relation to the implementation of the initiatives, excluding the nDVS. In these circumstances, there would be benefit in the parties to the NISS articulating their roles and responsibilities as far as implementation of the NISS elements is concerned, with AGD performing a leadership role in this process.

### **Progress against the six NISS elements (Chapter 3)**

19. The ANAO reviewed progress of each NISS element. In the majority of elements, there had been activity but it often did not align with the specific actions set out in the work program attached to the NISS IGA. For example, four of the six NISS elements<sup>7</sup> were about the development and implementation of standards. However, the ongoing development of all four 'standards' has been to develop 'better practice guides' which has resulted in a variance from the original intent of the NISS IGA. Two of these standards (drafted as better practice guides)<sup>8</sup> have been agreed to pursuant to the NISS, however, the extent of their adoption and implementation has been limited. Thus, while some action has been undertaken in relation to these four elements, they have not been completed as originally intended and the extent of adoption of the amended approaches is uncertain.

20. In relation to the NISS element, biometric interoperability, there have been a range of activities, primarily coordinated outside the formal NISS framework, that complement the intentions of the NISS. The NISS working groups has used these activities as a basis to focus current and future work on legal and policy issues for biometric interoperability.

---

<sup>7</sup> Registration and enrolment standards, security standards for proof of identity documents, standards in the processing and recording of identity data, and authentication standards.

<sup>8</sup> The Gold Standard e-Authentication Requirements (GSAR) and the Security Standards for Proof of Identity Documents.



21. The remaining NISS element (improved ability to verify information) required the development of the nDVS. While the nDVS has been built, implementation of the nDVS is at least 18 months behind the original four year project plan implementation dates. Widespread use relies upon the nDVS being connected to the agencies that issue documents used in establishing one's identity. Further uptake will, in part, be determined by the convenience, speed and reliability of the nDVS, when compared to other means of document verification. Notwithstanding a prototype Document Verification Service funded in 2005–06 and over two years of implementation of the nDVS, the project has presented significant problems for user acceptance and, consequently, it is rarely used. While AGD has had some recent success in getting more agencies connected to the nDVS, this has not translated into increased use. Remedial strategies for the nDVS may include changes to the nDVS, assisting with changes to user's systems and work practices, or considering the future of the nDVS itself. The current, very limited, use of the nDVS indicates that it is unlikely in the immediate future that use of the nDVS will significantly contribute to strengthening Australia's personal identification processes.

#### **AGD's administrative arrangement for implementing the NISS (Chapter 4)**

22. AGD relied on the higher level groups, such as the NISCG to establish the work program for the NISS. As a consequence, for the NISS elements other than the nDVS, there was neither planning documentation nor a project methodology for implementation of the elements. As such, AGD did not: develop documented goals or objectives for the various NISS elements; articulate how implementation of the various elements would contribute to the NISS objective; or rank or prioritise the elements under the NISS. For the nDVS, planning documentation was finalised following an external request and, while potential impediments to implementation were identified, the significance was not well understood.

23. While AGD was able to identify and assess various risks to the nDVS, the absence of robust, implemented treatment options has meant that potential risks have materialised and have not been well managed. This has impacted on the ability of the nDVS to achieve the full project objectives. AGD has implemented a series of revised strategies that have had some success in progressing the nDVS. A revised project management framework within AGD provides a framework for policy and program implementation which, if

implemented well, would assist AGD to fulfil its role in relation to coordinating the development of the NISS.

24. To date, public reporting of progress regarding the NISS has been limited. Further, irregular and inaccurate management reporting of the nDVS has restricted the information to which the respective governing bodies could undertake thorough and systematic assessments of the relevant issues relating to implementation. In August 2009, a revised nDVS team structure was agreed to by the relevant agencies, supplemented by the establishment of the DVS Advisory Board that reports directly to NISCG. The new structure provides an opportunity for AGD to establish a monitoring and reporting regime that better supports the DVS Advisory Board in making informed decisions.

25. Since 2005, the Australian Government has allocated \$30.8 million to AGD towards identity related security measures, including \$24.8 million towards the nDVS. There has been an underspend of the available funding across the financial years due to lack of progress and some of the funds allocated for the nDVS have been used for related tasks.

## Summary of agency response

26. The Attorney-General's Department (AGD) welcomes the Report of the ANAO's performance audit of the Department's arrangements for the National Identity Security Strategy (the Strategy). AGD accepts the ANAO's recommendations and has commenced work to implement them.

27. Development of the Strategy takes place in a complex, multi-jurisdictional environment; an environment that has evolved since the Council of Australian Governments first agreed to develop the Strategy. Work to develop and implement the Strategy since 2005 has achieved some important outcomes and addressed vulnerabilities to Australia's identity security. The progress that has been achieved to date provides a firm foundation for taking the Strategy forward.

28. The review of the Intergovernmental Agreement that underpins the Strategy (the NISS IGA)—commencing from April 2010—provides an excellent opportunity to address issues identified in the ANAO report. The review of the NISS IGA also provides an opportunity to reshape and refresh the work agenda, ensuring that the Strategy remains relevant to addressing current and future challenges to identity management.

29. AGD's full response to the report and the recommendations are set out in Appendix 1.

# Recommendations

---

## **Recommendation No.1**

### **Para 2.18**

The ANAO recommends that, to assist in the implementation of the National Identity and Security Strategy (NISS), the Attorney-General's Department, in consultation with the National Identity Security Coordination Group, formalise the specific responsibilities of key agencies of the NISS.

**AGD response:** *Agreed*

## **Recommendation No.2**

### **Para 3.24**

To more closely align the deliverables of the six National Identity Security Strategy (NISS) elements to the NISS objective, the ANAO recommends that the Attorney-General's Department, in consultation with the National Identity Security Coordination Group, assess the current objectives and appropriateness of the six NISS elements.

**AGD response:** *Agreed*

## **Recommendation No.3**

### **Para 4.14**

To improve program effectiveness, the ANAO recommends the Attorney-General's Department adopts a structured planning approach for all elements of the National Identity Security Strategy, against which progress and achievement can be measured and reported.

**AGD response:** *Agreed*



## **Audit Findings and Conclusions**



# 1. Background and context

---

*This chapter provides an overview of identity security, and Australian Government action on identity security, including the National Identity Security Strategy. It also provides information on the conduct of this audit.*

## Introduction

**1.1** The misuse of false or stolen identities—commonly referred to as identity crime—poses significant threats, both in terms of national security and crime more generally. Recent estimates suggest that identity theft, a subset of identity crime, is an issue that costs the Australian economy approximately AUD\$1 billion per year.<sup>9</sup> In turn, identity security is becoming increasingly central to Australia’s national security, law enforcement and economic interests, and the interests of the global community generally.<sup>10</sup>

**1.2** Identity security relates to the use and holdings of personal information. Credentials containing personal information are used extensively by individuals in interactions with the government and private sector. Examples of the use of personal information include: access to government benefits (social security payments), regulation of an activity (driver’s licence), or interaction with the private sector (opening a bank account). The personal information relied upon is generally based on fixed and variable attributes, which are officially provided by individuals and are registered by public agencies. These attributes can include an individual’s gender, first and last name, date and place of birth and place of residence. The various attributes are kept and recorded for different legislative purposes by Australian, state and territory government agencies.

**1.3** In the absence of a uniform national identity document, Australia relies on a range of credentials containing personal information, issued for primarily operational purposes, which are routinely used by agencies, business and individuals as de-facto identity documents. A state or territory issued driver’s

---

<sup>9</sup> OECD Committee on Consumer Policy, *Online Identity Theft* (February 2009), p. 37, and Cuganesan, S and Lacey D, *Identify fraud in Australia: An Evaluation of its Nature, Cost and Extent*, 2003.

<sup>10</sup> *ibid.* See also: Securities Industry Research Centre, *Identity Fraud in Australia: an Evaluation of its Nature, Cost and Extent*, 2003, ANAO Audit Report No. 24 2007-08, *DIAC’s Management of the Introduction of Biometric Technologies*, p. 34, and ANAO Better Practice Guide, *Fraud Control in Australian Government Agencies*, August 2004, Canberra.

licence, for example has a primary purpose of establishing an individual's eligibility for driving a motor vehicle, however will often be relied on as a primary identity document. The current range of identity-related credentials are of variable quality and accuracy, which exposes individuals, business and government to many risks from not being able to verify that a person is who they claim to be. Improving identity security has been a focus of many countries around the world. Some for, example, have introduced new identity cards, whilst others have focused on improving the robustness of existing credentials and the process by which these are verified. Within Australia, being able to verify with confidence an individual's identity is balanced against privacy considerations and broader community interests.<sup>11</sup>

**1.4** The credentials used in client enrolment processes and subsequently relied upon for establishing one's identity can be generically referred to as proof of identity (POI) documents. POI documents may be issued by Australian, state or territory government bodies, municipalities, private sector bodies, educational facilities, community organisations and overseas agencies. Within Australia, the ANAO has identified at least 75 types of POI documents accepted for eligibility for key Australian, state and territory government services.<sup>12</sup> A brief overview of the accepted POI documents is supplied in Figure 1.1. A more comprehensive list of POI document types is located at Appendix 3.<sup>13</sup>

---

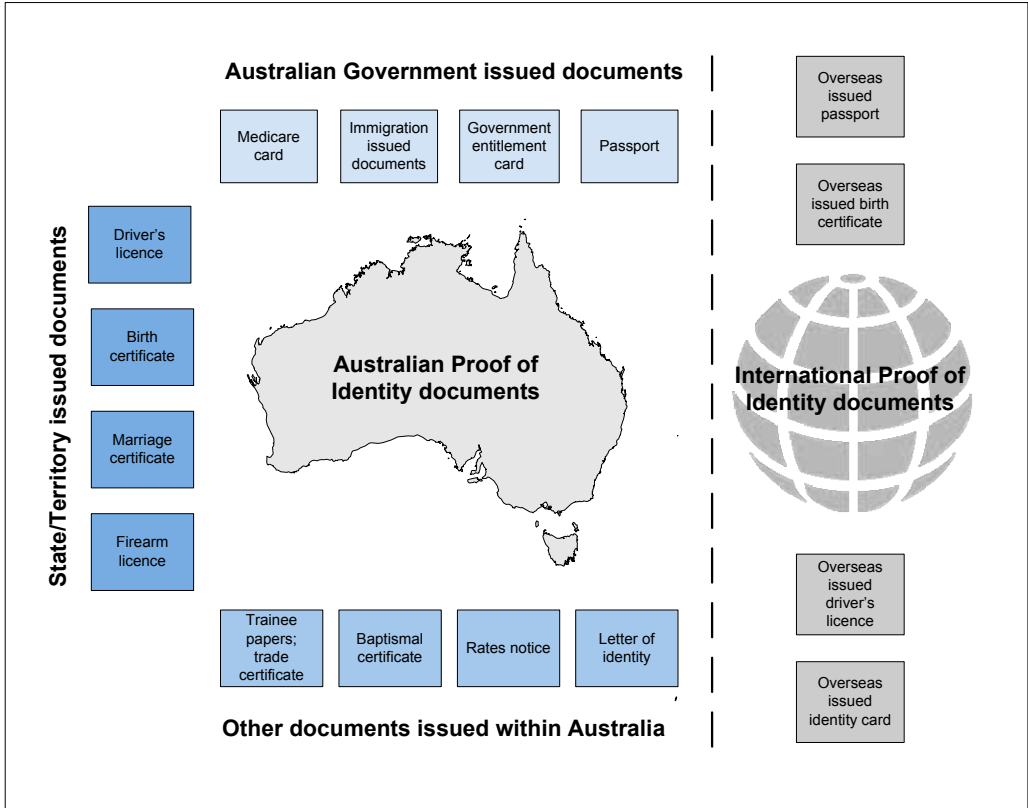
<sup>11</sup> Appendix 1 sets out a range of other Australian Government initiatives and international approaches

<sup>12</sup> The 75 types of acceptable POI documents is drawn from the enrolment requirements of obtaining a (i) Australian Passport, (ii) Department of Immigration and Citizenship issued citizenship certificate or travel document (visa), (iii) State and Territory Road and Traffic Authority issued drivers licence, or (iv) State and Territory Births, Deaths and Marriages registrar issued birth certificate.

<sup>13</sup> Each jurisdiction has differing standards that are reflective of States and Territory's varying demographics. For example, the Northern Territory has unique demographics that have prompted enrolling agencies to include POI documents that other states and territories have not accepted.



**Figure 1.1**  
**Examples of acceptable POI documents**



Note: 'Other documents issued within Australia' includes the POIs used by municipalities, private sector, education sector, community groups and the religious sector

Source: ANAO analysis, review of Australian, State and territory enrolment processes

**1.5** There is no uniform framework for the categorisation of POI documents within Australia. Each jurisdiction and registration process has elements that promote the POI value of certain documents over others. Agencies generally adopt an enrolment process that aligns with their operational or legislative need. For example, agencies use elements of, or a mixture between, 'primary' and 'secondary' POI document categories, the 100 point system<sup>14</sup> or the POI framework that was presented alongside the

<sup>14</sup> The 100 point system allocates certain points value to particular documents. See further the *Financial Transaction Reports Act 1988* and the *Financial Transaction Reports Regulations 1990*.

inaugural NISCG report to COAG in 2007 (see Appendix 4).<sup>15</sup> An ANAO review of the varying enrolment processes employed by agencies highlighted some of the key commonly relied upon POI documents. Table 1.1 provides a list of these documents. Also included in Table 1.1 is a conservative estimate of the total number of the current documents in the community.

**Table 1.1**

**Commonly used POI documents**

POI documents	Estimated total number of documents in the community (2008–09)
Australian Passports	9 900 000
Birth certificates/Birth registrations	15 322 900
Department of Immigration and Citizenship (DIAC) issued documents <sup>16</sup>	4 390 089
Driver's licences with photo (issued by State and territory Road Traffic Authorities)	15 663 221
Medicare Cards	11 964 638
<b>Total</b>	<b>57 240 848</b>

Note: Numbers may include re-issue of stolen, lost or damaged POI documents.

Source: ANAO analysis sourced from annual reports, ABS statistics and agency data.

**1.6** The use of fraudulent documents can facilitate a wide range of criminal behaviours. Identity crime may encompass the illegal use of a person's credit card details to make purchases over the internet or telephone, through to the assumption by one person of another's entire identity to open bank accounts, take out loans, and conduct other business illegally in that name. The crime may or may not involve financial fraud and can be used to cover up or enable various forms of criminal activity.

<sup>15</sup> This POI framework outlines evidence of commencement in Australia, linkage between identity and person, evidence of operating in the community and evidence of residence.

<sup>16</sup> Includes DIAC issued Certificate of Evidence of Australian Citizenship, Certificate of Evidence of Residence Status and DIAC issued travel documents.

**1.7** The following case study provides some examples of how identity crime is perpetrated.

### **Online techniques—general**

Identity-related criminal activity is constantly evolving as new ways to gain access to or manipulate identity data are found. Online techniques for procuring personal identifying information include:

- phishing email attacks are commonly perpetrated through the creation of fake emails purporting to be from trusted organisations such as banks;
- using a key logging device on computers; and
- stealing personal information in computer databases, and infiltration of organisations that store large amounts of personal information, such as government organisations and financial institutions.

### **Online social interaction**

Online social interaction, particularly social networking, is growing in popularity. However, some users of social networking websites engage in behaviour that puts them at risk of identity theft. Placing personal information on online social interaction sites can provide enough information for perpetrators to steal an individual's identity and open accounts in the individual's name.

### **Consumer scams**

There are increasing reports of high volume scams or frauds involving low or no value, purporting to offer lottery, job or other opportunities. Consumer scams are crimes of dishonesty such as forgery, counterfeiting, online deception, and theft that are targeted at people who seek to purchase goods and services. Potential victims can be those who use fixed line or mobile phones, computers and the internet, older people, and those who use professional advisers. These consumer scams may be used by crime groups to gather personal identification information which is then on-sold to other crime groups.

### **Traditional techniques**

Other ways of procuring personal identifying information include:

- stealing mail or rummaging through rubbish ('dumpster diving'); and
- eavesdropping on public transactions to obtain personal data ('shoulder surfing').

Identity crime can be difficult to detect as it can involve the use of lawful processes, such as a change of name (through a change of name certificate).

Source: Standing Committee of Attorney's-General, *The Model Criminal Law Officers' Committee Final Report on Identity Crime*, March 2008, p. 5–6.

## **The National Identity Security Strategy**

**1.8** Over the last decade, the differing standards and inherent risks within Australia's identity security framework has resulted in the Australian Government intensifying its focus on identity security. This focus is evident in various reports and activities including:

- the House of Representatives Standing Committee on Economics, Finance and Public Administration report in 2000, *Numbers on the Run: Review of the ANAO Audit Report No.37 1998–99 on the Management of Tax File Numbers*. The report noted the need for a Commonwealth agency to lead Proof of Identity (POI) reform across Australia and nominated tasking the Attorney-General's Department (AGD) with the responsibility;
- in 2005, the Australian Government announced the need for a National Identity Security Strategy (NISS) to combat identity theft and the fraudulent use of stolen and assumed identities as a matter of national priority and, subsequently, the Council of Australian Government (COAG) agreed that the preservation and protection of a person's identity is a key concern and a right of all Australians; and
- in 2007, COAG agreed to the development and implementation of the National Identity Security Strategy (NISS) to better protect the identities of Australians.

**1.9** The first public articulation of the NISS was through an Intergovernmental Agreement (IGA) signed by all parties to COAG in 2007. The NISS remains the current Australian, state and territory government policy. The NISS IGA states that 'the NISS will provide a framework for intergovernmental cooperation to strengthen Australia's personal identification processes.'<sup>17</sup> To support the objective of the NISS, the 'Parties agreed to work together to develop and implement the NISS'<sup>18</sup> which is comprised of six distinct elements that are represented in Table 1.2. A work program attached to the NISS IGA, providing further detail to the six elements, is also represented in Table 1.2.

---

<sup>17</sup> COAG, *An Agreement to a National Identity Security Strategy*, 2007, p. 3.

<sup>18</sup> *ibid.*

Table 1.2

**NISS six elements and associated work program**

NISS element	Element description and work program
1. Registration and enrolment standards	<p><b>Description</b>—Registration and enrolment standards for use by agencies which enrol individuals to issue government documents that may also function as key documents for proof of identity purposes.</p> <p><b>Work program</b>—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.</p>
2. Security standards for proof of identity documents	<p><b>Description</b>—Security standards for such documents to reduce the possibility of forgery or unauthorised alteration of documents.</p> <p><b>Work program</b>—It is intended that this element 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.</p>
3. Document verification service	<p><b>Description</b>—Improved ability for Government agencies across jurisdictions to verify information on such documents.</p> <p><b>Work program</b>—Development and implementation of a national Document Verification Service (nDVS).</p>
4. Standards in the processing and recording of identity data	<p><b>Description</b>—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.</p> <p><b>Work program</b>—Work will devise standards that will provide guidance on improving the accuracy of personal identity information held on government agencies' databases.</p>
5. Authentication standards	<p><b>Description</b>—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.</p> <p><b>Work program</b>—It is proposed that this element 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.</p>
6. Biometric interoperability	<p><b>Description</b>—Measures to enhance the national interoperability of biometric identity security measures.</p> <p><b>Work program</b>—This element will outline types of biometric systems, issues about standardisation and interoperability and community acceptance.</p>

Source: COAG, *An Agreement to a National Identity Security Strategy*, 2007.

**1.10** The six interdependent elements of the NISS have varying requirements, from developing standards through to the building of IT systems. Certain elements (for example, security standards and an improved ability to verify key documents) rely on other elements (registration and enrolment standards for such key documents). The six elements of the NISS are closely linked, may operate in close conjunction with one another, and are mutually enforcing.

**1.11** The NISS IGA establishes the overarching governance of the NISS, including the National Identity Security Coordination Group (NISCG), which incorporates broad representation from Australian, state and territory government agencies. The NISCG is also the primary vehicle for developing the details of the NISS. The NISS IGA establishes an internal review mechanism whereby all parties have agreed to assess the circumstances and the necessity for the agreement to continue from April 2010.

**1.12** The Attorney-General's Department (AGD), through its mandate to 'coordinate federal criminal justice, security and emergency management activity, for a safer Australia,'<sup>19</sup> and Ministerial direction, is the lead Australian Government agency for identity security issues, including the NISS. AGD has received \$30.8 million in funding for specific NISS elements.<sup>20</sup> However, there has been no additional funding from government to assist in the implementation of the NISS as a strategy. Consequently, the NISS operates in conjunction with each agency's core responsibilities. Table 1.3 details key milestones in the development and implementation of the NISS.

---

<sup>19</sup> Commonwealth of Australia, Portfolio Budget Statements, Attorney Generals Portfolio 2009–10, p. 2.

<sup>20</sup> There have also been a range of initiatives relating to identity security issues, while outside the direct of the scope of NISS, that operate in close connection with NISS including *Biometric at the border*, a 2004-05 Australian Government budget initiative of \$214 million over four years, involving the then Department of Immigration and Multicultural and Indigenous Affairs, Department of Foreign Affairs and Trade, the then Australian Customs Service and the Office of the Privacy Commissioner.

**Table 1.3****Key milestones in the development and implementation of the NISS**

Date	Activity
2003	AGD completes a feasibility study for a national Document Verification System (nDVS).
April 2005	Australian Government announces the National Identity Security Strategy.
May 2005	Budget 05–06 allocated \$5.9m to AGD to develop specific pilot programs for identity security related matters, including the prototype Document Verification Service (pDVS).
September 2005	COAG reaffirms its commitment to identity security in a special meeting on Counter–Terrorism, and begins working towards an IGA on the subject.
May 2006	Budget 06–07 allocated \$24.8m to AGD for the implementation of the nDVS over four years—NISS element No. 3, Improved ability to verify information.*
December 2006	The pDVS evaluation is finalised.
April 2007	COAG signs the NISS IGA and releases the inaugural report, which represents the first publicly available articulation of the six elements of the NISS
June 2007	AGD completes the Privacy Impact Assessment for the nDVS.
<b>Proposed</b>	
April 2010	All parties to the NISS IGA agreed to review the NISS IGA to assess the circumstances and the necessity for the NISS IGA to continue.

Note: An additional \$3.5m over four years was provided to the Office of the Privacy Commission, the Australian Security Intelligence Office and the Australian Crime Commission. Use of these funds was outside the scope of this audit.

Source: ANAO analysis of COAG, *An Agreement to a National Identity Security Strategy*, 2007, Annual Reports and Portfolio Budget Statements.

**Audit approach****Audit objective and scope**

**1.13** The objective of the audit was to assess the effectiveness of AGD's arrangements for coordinating the development the National Identity Security Strategy.

**1.14** ANAO's assessment was based on the following criteria:

- governance arrangements for the NISS;
- progress, to date, of the six NISS elements; and
- AGD's administrative arrangements for developing the NISS.

**1.15** The audit primarily examined the activities of AGD. The NISS is a whole-of-government initiative that involves a number of other Australian Government agencies, including the Department of Foreign Affairs and Trade (DFAT) and the Department of Immigration and Citizenship (DIAC). A range of state and territory agencies are also involved. While these agencies play important parts within the NISS, the focus of the audit was on AGD as lead agency for the Australian Government.

## **Audit methodology**

**1.16** The audit methodology comprised:

- interviewing key personnel in AGD;
- interviewing key participants of NISS, including Australian Government agencies as well as state and territory based road and traffic authorities, and births, deaths and marriages registrars;
- analysing relevant documentation, including policies, procedures and correspondence; and
- reviewing relevant literature.

**1.17** The audit was conducted in accordance with ANAO auditing standards at a cost of approximately \$235 000.



## 2. Governance

---

*This chapter reviews the governance arrangements for the development and implementation of the National Identity Security Strategy.*

### Introduction

**2.1** The governance arrangements for the development and implementation of the National Identity Security Strategy (NISS) was established by the Intergovernmental Agreement (IGA) to the NISS, signed by the Council of Australian Governments (COAG) in April 2007. The NISS IGA seeks to provide 'a framework for intergovernmental cooperation to strengthen Australia's personal identification processes.'<sup>21</sup> Broadly, the NISS IGA outlines the six elements of NISS, including undertakings for all signatories to the NISS IGA to further develop and implement the NISS to give effect to the COAG commitments. The Attorney-General's Department (AGD) as lead agency for Australian Government identity security matters has lead responsibility for coordinating the development of the NISS.

**2.2** The ANAO assessed the governance arrangements for the development of the NISS.

### Overview of NISS governance bodies

**2.3** To assist in transparency in departmental arrangements when whole-of-government work is put in place it is important that governance and accountability arrangements are clearly set out and understood. As noted in the Department of Prime Minister and Cabinet and ANAO Better Practice Guide *Implementation of Programme and Policy Initiatives*, at a minimum, the identification of a lead agency in whole-of-government initiatives is beneficial.<sup>22</sup>

**2.4** The NISS operates in a complex environment, involving not only numerous Australian Government agencies but also a variety of agencies at the state and territory level. The Australian Government and state and territory

---

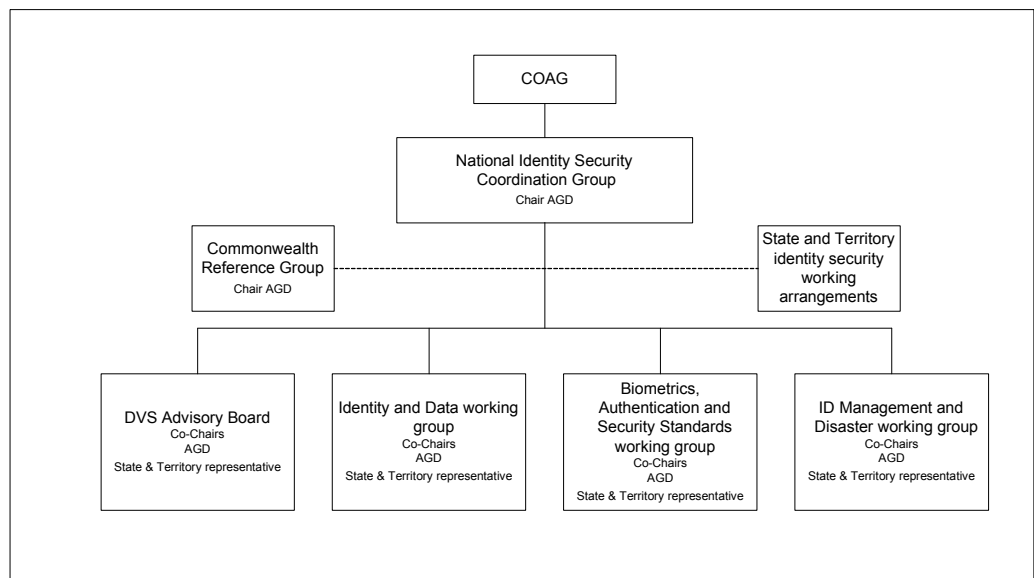
<sup>21</sup> COAG, op. cit., p. 3.

<sup>22</sup> Department of Prime Minister and Cabinet and ANAO Better Practice Guide *Implementation of Programme and Policy Initiatives*, October 2006, p. 14. See also ANAO Audit Report No.10 2007–08, *Whole of Government Indigenous Service Delivery Arrangements*, p. 22.

involvement in the NISS is set out in Figure 2.1, followed by a brief description of the role and function of the NISS governance bodies.

**Figure 2.1**

**National Identity Security Strategy group structure**



Source: ANAO analysis of AGD data.

**National Identity Security Coordination Group (NISCG)**

**2.5** The NISCG was formally established by the NISS IGA and is the ‘primary vehicle for developing the details of the NISS’.<sup>23</sup> The NISCG had been in operation since late 2005, following the COAG September 2005 decision to develop the NISS. Prior to the NISCG, a National Identity Security Steering Committee performed a similar function at the Commonwealth level only. The NISCG has representation from First Minister Departments of the Australian, 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 (CVS)<sup>24</sup>, Austroads<sup>25</sup> and the

<sup>23</sup> COAG, op. cit., p. 4.

<sup>24</sup> The CVS is an electronic service operated by the New South Wales Registry of Births, Deaths and Marriages on behalf of the Births, Deaths and Marriages registries of Australasia. Births, Deaths and Marriages registries currently use the CVS to verify documents issued by state and territory counterparts.

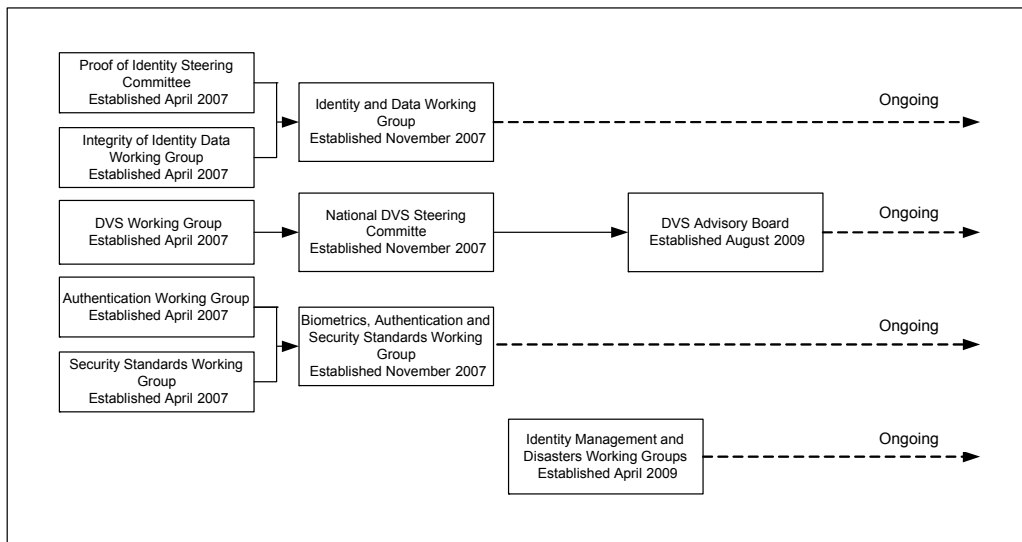
Federal Privacy Commissioner. AGD has always held the position of Chair of NISCG and performs the secretariat function for the NISCG. The NISCG is responsible for reporting annually to COAG on the progress against the NISS.

## NISCG Working Groups

**2.6** Working groups have been established to support the NISCG. The working groups are constituted pursuant to the NISS IGA and are designed to develop proposals for consideration of the NISCG. At the signing of the NISS IGA in 2007, five working groups were established. Since 2007, there has been some consolidation and changes to the group structure instigated and managed by AGD. The recent history of the working groups is represented in Figure 2.2.

**Figure 2.2**

### NISCG working groups



Source: ANAO analysis of AGD data.

**2.7** Figure 2.2 highlights that there has been a general alignment between the six NISS elements (see Table 1.2) and the working groups. Excluding the biometrics interoperability element, working groups were created to further

<sup>25</sup> Austroads is the association of Australian and New Zealand road transport and traffic authorities. Austroads manages the National Exchange of Vehicles and Driver Information System (NEVDIS). NEVDIS is a national database that provides access to all registered vehicles and licensed drivers in Australia.

develop the associated work programs of the NISS elements in April 2007. In November 2007, when the working groups were consolidated, the biometrics interoperability element of the NISS was specifically included with one of the new working groups.

**2.8** The objectives of each working group also align to the NISS elements. For example, the scope of the Identity and Data working groups is to: progress consistent approaches to ensure robust proof of identity enrolment processes are in place for all high value services and credentials; explore common approaches to emerging identity issues; explore common approaches to promote the integrity, interoperability and security of identity data; and recognise best practice in government and harness private sector expertise.

**2.9** The framework established by the NISS IGA has also facilitated the establishment of new working groups to coordinate the development of the whole-of-government responses to emerging risks. For example, in April 2009, following the 2009 Victorian bushfires, an Identity Management and Disasters working group (IMDWG) was established to contribute to improved disaster management and recovery operations by developing and implementing proposals that utilise identity management. While the objectives and direction of the IMDWG is not directly linked to a specific NISS element, the underlining focus of the IMDWG is consistent with NISS. The replacement of lost or destroyed documents, a common issue following a natural disaster, links closely to registration and enrolment standards.

**2.10** The composition of each working group is designed around expertise and interest. As there is a wide range of parties to the NISS, the working groups have facilitated involvement and access to the NISS agenda aligned to agency interests, across Australian, state and territory governments. For example, DFAT, through its ongoing work with the development of biometric passport technology, has been active within the working groups regarding security standards for POI documents.

**2.11** AGD's role within the working groups is currently as co-chair as well as providing the secretariat function. Overall, the establishment of the working groups has been effective in bringing together the various parties to the NISS. While the ANAO identified a few minor improvements that can be made by AGD in the administrative arrangements supporting the working groups, the working groups are aligned to the elements of the NISS and have provided a structured forum for the various stakeholders to share experiences and work towards implementation of the NISS elements.

## Commonwealth Reference Group

**2.12** The Commonwealth Reference Group (CRG) does not have a direct connection to the NISS. From its first meeting in 2003, the CRG was established as a reference group for identity security related matters of Australian Government agencies. While there are over 30 agencies invited to participate, over the last three years approximately 20 agencies, on average, have met four times. There are no terms of reference or clear mandate for the CRG. The AGD has always held the position of Chair of the CRG and facilitates the meetings and distribution of papers. In 2007, the Chair of the CRG in a letter to the other members described the CRG as a ‘forum in which to establish an Australian Government position on the NISS and to exchange information about identity management issues’.<sup>26</sup> In July 2008, the Chair emphasised within a CRG meeting that the CRG was ‘an important forum that should be used as a ‘clearing house’ to make decisions on overall Commonwealth strategy.’<sup>27</sup> Following inquiry by the ANAO, AGD advised that the department will initiate action to address the mandate, role and purpose of the CRG in early 2010.

**2.13** The ANAO review of meeting papers highlighted the role of CRG as a forum that discussed and endorsed papers. An example was the endorsement of the *Data Matching Better Practice Guidelines* as a ‘Commonwealth reference document’ in March 2009, relating to the NISS element ‘integrity of identity data’. This document was made available to the public in February 2010.

## Specification of roles and responsibilities in relation to developing and implementing the NISS

**2.14** The NISS IGA is an agreement between governments in which the various parties have ‘made undertakings to further develop and implement the NISS to give effect to COAG commitments’ aimed at strengthening Australia’s personal identification process.<sup>28</sup> Ultimately, however, authority for implementation decisions rests with each relevant jurisdiction. This poses particular governance challenges for the NISS, the success of which relies on complementary implementation decisions by the parties to the agreement.

---

<sup>26</sup> Letter from Chair of Commonwealth Reference Group to members dated 12 October 2007.

<sup>27</sup> Commonwealth Reference Group Minutes, 28 July 2008.

<sup>28</sup> COAG, op. cit., p. 3.

**2.15** Clear specification of roles and responsibilities for individual agencies and of a lead agency is one way of aiding the implementation of cross-agency activities, such as the NISS. However, unlike more recent COAG agreements, the NISS IGA does not clearly task specific parties with key implementation responsibilities.<sup>29</sup> AGD confirmed that they did not consider ‘that the NISS IGA provides a mandate for the *implementation* of measures developed in relation to the five non-nDVS related elements of the NISS,’ rather, the ‘NISS IGA was intended to be an aspirational document that provided a framework for jurisdictions to work cooperatively to strengthen Australia’s personal identification processes.’<sup>30</sup> In practice, AGD, as the Australian Governments lead agency on identity security issues has taken on a role coordinating the development of the NISS, and the ANAO observed that the Department’s approach has been consistent with this perspective. That is, AGD has sought to work through voluntary engagement by all parties for the development and implementation of the six NISS elements.

**2.16** A consequence of this approach is that no single agency in a position to accept accountability for the implementation of the NISS elements (nDVS excluded). In the case of AGD, the Australian Government ‘lead agency’ considers it has limited leadership authority and no responsibility in relation to the implementation of the NISS elements (nDVS excluded). As discussed in Chapter 3, a further consequence of this is evident in the absence of consolidated information on the extent to which the various parties to the NISS have actually implemented the agreed activities. The ANAO considers that a key leadership role for AGD in this case, would be to identify and seek to address gaps and uncertainties in the governing instruments and initiate the appropriate remedial action.

**2.17** The parties to the NISS IGA have agreed to review and assess the circumstances and necessity for the NISS IGA to continue after three years of operation, namely from April 2010. The ANAO considers that there would be considerable benefit for the AGD and NISCG, in the process of reviewing the NISS IGA, to work together and detail, formalise and document the roles and responsibilities of the key parties to the NISS.

---

<sup>29</sup> See for example, *National Indigenous Reform Agreement (Closing the Gap) IGA*, 2 July 2009, *National Partnership Agreement on Youth Attainment and Transitions IGA*, 2 July 2009 and *National Partnership Agreement on Energy Efficiency IGA*, 2 July 2009.

<sup>30</sup> AGD advice to ANAO dated 16 December 2009.

## Recommendation No.1

2.18 The ANAO recommends that, to assist in the implementation of the National Identity and Security Strategy (NISS), the Attorney-General's Department, in consultation with the National Identity Security Coordination Group, formalise the specific responsibilities of key agencies of the NISS.

**Attorney-General's Department response:** *Agreed.*

2.19 Appendix 1 sets out AGD's complete response to the recommendation.

## 3. Progress against the NISS elements

---

*This chapter assesses progress in implementing the six NISS elements and their contribution to the overall NISS objective.*

### Introduction

**3.1** The NISS IGA established six elements, which, when developed and implemented, were expected to provide a framework for intergovernmental cooperation to strengthen Australia's personal identification processes. At the time, the work program attached to the NISS IGA was considered to be 'a work-in-progress requiring further consideration.'<sup>31</sup>

**3.2** The development and implementation of each NISS element was expected to contribute to the overall NISS objective. Further, the individual outputs should be linked to the NISS objective. The ANAO assessed progress against each of the NISS elements, in terms of their original intent, in turn, and their contribution to achievement of the overall NISS objective.

### Progress achieved against the elements of the NISS

#### The NISS elements (nDVS excluded)

**3.3** The ANAO reviewed progress of each NISS element. These are detailed in Appendix 5. The ANAO observed that in each case there had been activity but it often did not align with the original specific actions set out in the work program attached to the NISS IGA. For example, four of the six NISS elements<sup>32</sup> were about the development and implementation of 'standards'. However, the ongoing development of all four standards has been to develop 'better practice guides' which has resulted in a variance from the original intent of the NISS IGA. The development of registration and enrolment standards provides an example.

---

<sup>31</sup> COAG, op. cit., p. 3.

<sup>32</sup> Registration and enrolment standards, security standards for POI documents, standards in the processing and recording of identity data, and authentication verification.



### Registration and enrolment standards

The work program attached to NISS IGA states that the intent of this element was '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.

A Gold Standard Enrolment Framework (GSEF) was developed for use by government agencies who enrol individuals for the purposes of issuing government documents that may also function as key documents for POI purposes.

The current form of the GSEF is a 'best practice guide' which agencies can choose to implement. It is drafted to apply to a limited class of agencies based on individual agency's own determination. It does not, however, specify which agencies should apply GSEF and as a best practice guide is a collation of aspirational processes that are generally relevant in client registration and enrolment processes.

The second aspect of this NISS element also specified the development of standards for 'key' documents. The current version of the GSEF states that the POI framework (Appendix 4) should be read in conjunction with the gold standard. However, the GSEF does not identify 'key' documents, and there is no articulation of what constitutes a 'key' document in the NISS IGA.

**3.4** The implementation of the agreed activities is also unclear. The ongoing development of the NISS elements has resulted in two of the four standards (drafted as better practice guides) agreed to pursuant to the NISS.<sup>33</sup> However, it is not clear the extent to which these have actually been implemented by the parties to the NISS IGA. For example, the Gold Standard e-Authentication Requirements (GSAR) was endorsed by the NISCG in March 2008. AGD, however, has had a limited role in monitoring the adoption and implementation of the GSAR—through receiving updates via working groups and the CRG. Consequently, neither AGD nor any other party holds sufficient information to provide assurance that completion of this element is contributing to the NISS objective. While there are examples of individual agencies adopting aspects of the GSAR,<sup>34</sup> there is also no publicly available, consolidated information on the extent to which Australian, state, and territory

<sup>33</sup> The Gold Standard e-Authentication Requirements (GSAR) and the Security Standards for Proof of Identity Documents.

<sup>34</sup> For example, Tasmania has developed an *Identity and Access Management Toolkit* which is based on elements of the NISS, including the GSAR, see <[http://www.egovernment.tas.gov.au/information/security\\_and\\_sharing/identity\\_and\\_access\\_management\\_toolkit](http://www.egovernment.tas.gov.au/information/security_and_sharing/identity_and_access_management_toolkit)> [accessed 16 December 2009].

government agencies responsible for issuing relevant POI documents have incorporated these requirements into their business processes and operations.<sup>35</sup>

## **Development and implementation of the nDVS**

**3.5** The development of the nDVS can be contrasted to the other NISS elements in that there is a specific funding tied to a system designed to be used in the verification and enrolment processes. The announcement in the 2006–07 Budget stated of that:

The document verification service will verify the accuracy of details contained in documents presented by people as proof of identity when applying for a government clearance or enrolling for services or benefits at an authorised agency. The service will also help to detect fraudulent documents and will use cross referencing to help detect the use of stolen documents.<sup>36</sup>

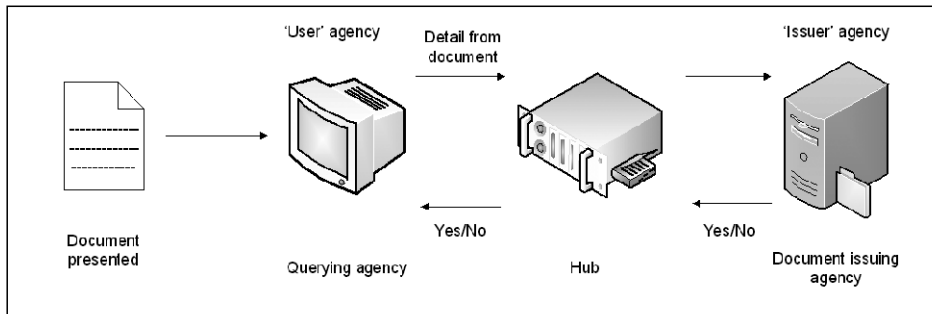
**3.6** The nDVS is designed to assist agencies in the introduction of a more rigorous and accurate enrolment process. The nDVS provides a means of checking information within documents presented with the records of the document issuing agency. Broadly, if the details provided by clients matched the information held by the issuing agency, a 'Yes' response is transmitted, otherwise a 'No' response should be returned, indicating that the document details were not verified.<sup>37</sup> Pivotal to the design of the nDVS is an independent 'Hub' that connects between all the different 'Issuers' and 'Users'. The information flows can be shown in Figure 3.1.

---

<sup>35</sup> Similarly, in relation to the Security Standards for proof of identity documents element, the 2009 NISCG report to COAG highlights that implementation of this element is now essentially complete. However, the security standards element as stated in the NISS IGA is dependant on the definition of the first element (registration and enrolment standards for key documents) for which implementation has been slow. Further, neither the NISCG, the working groups, nor the AGD has specified what constituted 'implementation' of this element, to what tier and to what level.

<sup>36</sup> Australia Government, *Budget Paper No.2, Budget Measures 2006–07*, p. 121.

<sup>37</sup> There are also various different error messages transmitted.

**Figure 3.1****Information flows of nDVS**

Source: ANAO analysis of AGD information.

**3.7** The Australian Government commitment to the nDVS in the 2006–07 Budget was a \$28.3 million commitment over four years (including \$1.1 million in capital funding), with \$24.8m for AGD.<sup>38</sup> This funding was in addition to \$5.9 million provided in the 2005–06 Budget for two identity security pilot programmes. One of the pilot programmes was a prototype document verification service (pDVS), the precursor to the nDVS.

**3.8** The pDVS established the technical viability of the nDVS, exploring the technical and operational issues associated with a document verification service. Testing for the pDVS was undertaken from February to June 2006, simultaneous to the announcement of the nDVS. The pDVS project was finalised in December 2006 with an evaluation report which noted the successful ability to verify documents balanced against issues associated with verification failures. Contrary to conventional practice, the decision to proceed with the nDVS was taken prior to the completion of the pDVS phase.

**3.9** The physical build of the nDVS used the same IT infrastructure as the pDVS. While improvements continue to be made to the nDVS following the government announcement, the major task of AGD in implementing this government measure is ensuring the nDVS contributes to the NISS objectives through widespread use. Extensive use, in turn, rests on the nDVS being

<sup>38</sup> The ANAO did not specifically assess the activities of the Office of the Privacy Commission (who were funded to conduct a series of privacy audits), the Australian Security Intelligence Office or the Australian Crime Commission in relation to this audit who also received funding relating to the nDVS (totalling \$3.5 million over four years). The Australian Crime Commission was funded to implement a Lost and Stolen Document Register. This process was terminated in April 2008.

connected to the agencies that issue documents relied upon in establishing a person's identity. Further uptake by user agencies will, in part, be determined by the convenience, speed and reliability of the nDVS, when compared to other means of document verification. The ANAO examined progress in connecting agencies to the nDVS, usage of the nDVS to date and management of barriers to further uptake of the system.

### *Connecting potential nDVS issuers and users*

**3.10** The potential issuer agencies who needed to be engaged were made clear from the beginning of the nDVS planning process. Connection to the agencies that issue key documents used as evidence of commencement of identity in Australia (birth certificates and record of immigration status) and linkage between identity and person (Australian Passport and driver's licence) was required for widespread use. As a direct consequence, the original planning documents specified that all state and territory Births, Deaths and Marriages registries and Road, Traffic Authorities, as well as DIAC and DFAT, would be connected to the nDVS as 'issuer' agencies by June 2008.

**3.11** The engagement with 'issuer' agencies was to be achieved by entering into a Memorandum of Understanding (MOU) with the various responsible 'issuer' agencies. As at February 2010, many key identified issuer agencies were still not connected to the nDVS, although some progress had been made particularly during 2009. While AGD identified the obstacles of obtaining jurisdictions sign-on, the resultant strategies employed, such as bi-lateral negotiations, have taken longer than expected to come into effect. Table 3.1 lists all the MOUs entered into regarding the nDVS.

**Table 3.1****List of MOUs for the nDVS**

	Agency	Customer type	Most recent agreement
1	Centrelink <sup>39</sup>	Access to DVS links	25 July 2007
2	Centrelink	Develop, operate DVS Hub	14 April 2009
3	DFAT	Issuer–Develop and maintain interface	4 October 2007
4	DIAC	Issuer–Develop and maintain interface	21 February 2008
5	New South Wales, Registry of Births, Deaths and Marriages	User/issuer	6 November 2008
6	Austroroads Incorporated	Issuer via link with NEVDIS	5 January 2009
7	New South Wales ,Roads and Traffic Authority	User/issuer	6 February 2009
8	Western Australia, Registry of Births, Deaths and Marriages	User/issuer	1 April 2009
9	Tasmanian Department of Justice,	User/issuer	18 May 2009
10	Australian Capital Territory, Roads Transport Authority	User/issuer	3 August 2009
11	Northern Territory Registry of Births, Deaths and Marriages	User/issuer	14 August 2009
12	Australian Capital Territory, Registry of Births, Deaths and Marriages	User/issuer	28 August 2009
13	Northern Territory, Department of Planning and Infrastructure	Issuer	16 September 2009
14	Tasmanian, Registrar of Motor Vehicles	User/issuer	23 September 2009
15	New South Wales, Office of State Revenue	User/issuer	30 September 2009
16	DIAC	User	12 November 2009
17	Queensland, Department of Transport and Main Roads,	User/issuer	12 November 2009
18	Queensland, Registry of Births Deaths and Marriages	User/issuer	25 November 2009

<sup>39</sup> The first Centrelink MOU was in relation to using the physical links established by the nDVS. No service was delivered under this MOU and the MOU was subsequently terminated 19 November 2009.

	Agency	Customer type	Most recent agreement
19	DFAT	User	10 February 2010
20	South Australia, Department of Transport, Energy and Infrastructure	Issuer	17 February 2010
21	South Australia, Births Deaths and Marriages Registration Office	Issuer	23 February 2010

Source: ANAO analysis of AGD information.

**3.12** During the course of the audit, the ANAO observed that AGD has not maintained a reliable record of all MOUs. Audit fieldwork revealed the non-existence of an MOU that should have been in place, as well as identifying an MOU that was not known to key personnel within AGD.<sup>40</sup> The implementation of a central repository of MOUs would assist AGD to clearly identify the scope and nature of its responsibilities and obligations, and more easily identify and track the progress of all MOUs.

**3.13** Overall the establishment of MOUs to participate in the nDVS has taken longer than expected. As at February 2010, many key issuer agencies, such as the Victorian based agencies as well as the Western Australian RTA, were not connected.

## **Use of nDVS has been limited to date**

**3.14** Use of the nDVS is integral to its successful implementation. While AGD has been successful in entering MOUs with a range of agencies, particularly in recent times, actual use of the nDVS has been very limited to date and well below expectations. On average there have been less than ten transactions per day. This stands in contrast to the nDVS project scope that estimated that when in operation, the nDVS should be able to handle up to one million transactions per day. The nDVS hub was built to meet these expectations.<sup>41</sup>

**3.15** There is a range of factors contributing to the low use of the nDVS. A key issue is that establishing a connection to the nDVS and incorporating the

<sup>40</sup> There were also examples of MOUs relating to the pDVS, whereby expired MOUs had been extended, bringing into question the MOU's authority and legitimacy.

<sup>41</sup> The current hub management MOU with Centrelink requires the development of a system that can handle 250 000 transactions per day. AGD advised ANAO this difference was due to an error in the original description as each request results in four transactions, which equates to 1 000 000 transactions.

nDVS into business processes, is likely to be implemented only when a clear benefit of the nDVS is realised to potential users. This involves a system that is more convenient, useful and reliable than alternative methods, particularly in delivering timely accurate responses to queries. The delivery of timely and accurate responses, however, has been an ongoing issue for the nDVS. As the system owner, it is the role of AGD to understand and respond to issues that create barriers to greater system use, to manage these issues, and to formulate effective solutions. AGD's approach in this regard is discussed below.

### *Timely results*

**3.16** Delivering timely results is critical for users of the nDVS as it affects customer service standards. Through technical working groups, AGD has involved jurisdictions and potential users in the design and specifications of the pDVS and nDVS. AGD has implemented a 20 second response time in the current *DVS Service Management Plan* and nDVS design. However, issuer agencies have noted potential adverse effects of a system that allowed this length of response time.<sup>42</sup>

**3.17** Notwithstanding the desire to have short response times, current response times are longer than desirable. While the majority of transactions are less than 20 seconds, from the available data in the last three months of nDVS transactions (July–September 2009), 25 per cent of transactions were longer than 20 seconds. AGD has sought to work with the technical issues causing the delays, however the lengthy response time still remains an issue, more than two years after implementation.<sup>43</sup>

**3.18** In addressing the timeliness issue, AGD has sought to respond to issues as, and when, they occur. This approach, however, has not worked in ultimately solving the timeliness issue. Further, the inability of the nDVS to consistently deliver timely results has not assisted in the promotion of the nDVS to potential users. Understanding users' needs and ensuring the nDVS delivers upon agreed expectations is a key ongoing issue for the implementation of the nDVS.

---

<sup>42</sup> Potential user agencies advised ANAO that the roll out of the nDVS is likely to be limited until the system is developed with a maximum response time of 10 seconds.

<sup>43</sup> There are also issues relating to system design with external systems. For example, some agencies have an internal time out after 15 seconds due to internal factors including customer service requirements, causing the transaction being not progressed when the response time is greater than 15 seconds, but within the 20 second timeframe.

## *Accurate results*

**3.19** Producing accurate responses is another ongoing issue that existed throughout the life of the pDVS and nDVS. For example, the nDVS has been operational since October 2007. Throughout this time, the nDVS has produced a combination of both 'Yes', 'No' and 'Error' responses. As at November 2009, accounting for over 50 000 transactions (pDVS over 45 000 transactions, nDVS over 4500 transactions), no fraudulent document has been identified. This does not mean that the system have produced 50 000 'Yes' responses. Instead, 38 per cent of all nDVS responses, and 11 per cent of the pDVS responses have been false negatives and 'Error' responses. Testing of the false negatives responses has identified that these are attributable to (i) user errors (incorrect data entry) or (ii) data errors (inconsistencies between details recorded on the document and the electronic record held by the agency). AGD has worked with some agencies in searching protocols to remedy some of the data errors. The broad issue of data errors, however, continue to cause error responses since the original trial in the pDVS. The following case study highlights some of the issues relating to the nDVS producing accurate results.

### **Case study**

Access to certain government benefits and entitlements is dependant on eligible non-citizens having a correctly issued visa. The nDVS offers the potential benefit of being able to quickly verify that the person accessing government services does, in fact, have a valid visa. Currently, the majority of visas are issued electronically, where the authority to be in Australia is stored electronically by the Department of Immigration and Citizenship (DIAC) with no stamp or label placed in the passport. There is a record of which passports do have a valid travel authority issued. Therefore, potentially an individual can present a foreign passport and have their visa entitlement quickly verified.

During use of the nDVS in mid 2009, it became apparent that passports issued by certain countries were incorrectly returning a 'No' response, when users tried to verify if there was a valid visa for the individual presenting a passport. Testing of the responses revealed that the name fields in certain systems restricted a full reproduction of the person's name—at times middle names were abbreviated. The record on the foreign issued passport did not match those in the DIAC database and, as a consequence, there was not an exact match between the document presented and details on DIAC's database. The nDVS design allows for exact matches only, therefore the nDVS response is 'not verified', which is technically correct, notwithstanding that a valid visa had been issued.

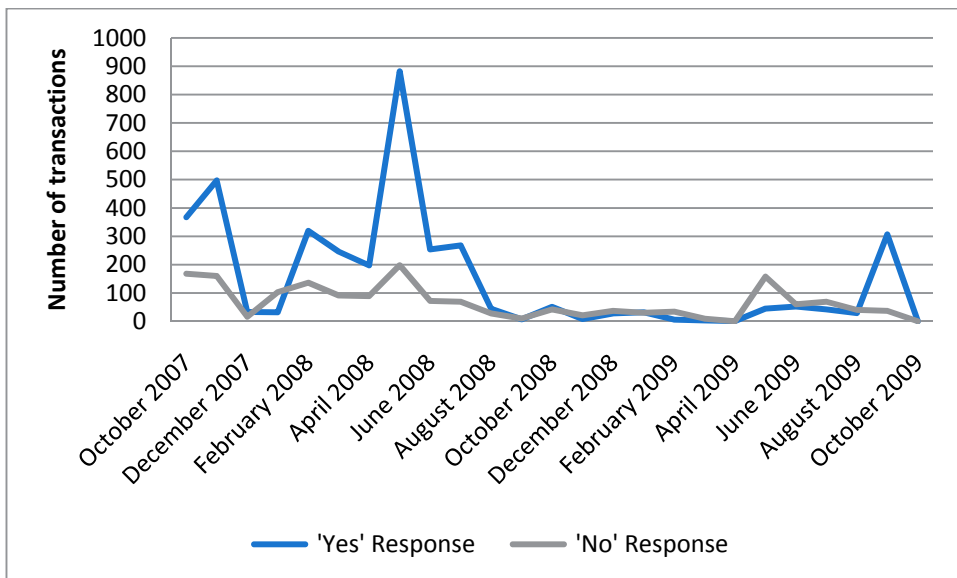


### Use of the nDVS

**3.20** Use of nDVS to date has largely been for testing or pilot programs by user agencies. The pilots, however, had not translated into widespread adoption due to some of the issues encountered. For example, in mid 2009 a newly signed 'user' piloted their use of the nDVS. Given the high rate of documents incorrectly returning 'not verified' due to data errors and timing issues, elements of the pilot was cancelled partly due the impact on customer service. Figure 3.2 shows the total transactions that have been processed by the nDVS hub, on a monthly basis, including both the 'Yes' and 'No' responses. While the nDVS does also produce error messages, these are not represented in Figure 3.2 due to different reporting throughout the life of the nDVS.<sup>44</sup>

**Figure 3.2**

#### Number of nDVS responses



Source: ANAO analysis of AGD data.

**3.21** In concept, the nDVS offers the potential for an enhanced identity management service whereby agencies can quickly verify the contents of particular documents presented for use for identity related purposes. Notwithstanding the pDVS and over two years of implementation, the project is still resolving practical implication issues and is rarely used. AGD's

<sup>44</sup> Error responses accounted for around one per cent of all transactions of available data.

approach to the nDVS has not been successful in delivering the originally intended results. Accordingly, there would be benefit in AGD systematically reviewing, with key potential users, the barriers to system uptake and formulate remedial strategies accordingly. These strategies may include changes to the nDVS, assisting with changes to user's systems and work practices, or considering the future of the nDVS itself. It is unlikely in the immediate future that use of the nDVS will significantly contribute to strengthening Australia's personal identification processes. AGD's approach to planning for successful completion of the nDVS is discussed in Chapter 4.

## **Contribution of each element to the overall NISS objective**

**3.22** The NISS has an objective of strengthening Australia's personal identification processes. To support this objective, each NISS element requires clear deliverables that would be developed, and that when implemented, would contribute to the NISS. However, progress in significant activities relating to some elements has been limited, and it is difficult to assess how the various activities surrounding the NISS elements have contributed to achieving the overall objective. Further, while the nDVS has been built, the lack of use by potential users means that it is not delivering on the original intentions.

**3.23** The NISS IGA established a mechanism whereby parties to the NISS would assess the circumstances and the necessity for the NISS IGA to continue from April 2010. The ANAO suggests that AGD use this opportunity to work with the NISCG to also evaluate the circumstances and the necessary objectives of the current six elements and assess whether they can be more clearly linked to the overall NISS objective.

## **Recommendation No.2**

**3.24** To more closely align the deliverables of the six National Identity Security Strategy (NISS) elements to the NISS objective, the ANAO recommends that the Attorney-General's Department, in consultation with the National Identity Security Coordination Group, assess the current objectives and appropriateness of the six NISS elements.

**Attorney-General's Department response:** *Agreed.*

**3.25** Appendix 1 sets out AGD's complete response to the recommendation.

## 4. Departmental arrangements for developing the NISS

---

*This chapter reviews AGD's administrative arrangements relevant to the development of the NISS. In particular, the ANAO reviewed the planning, monitoring and reporting arrangements for the NISS, as well as AGD's project resourcing.*

### Introduction

**4.1** Sound administrative processes are central to ensuring that: programs deliver an outcome that aligns with the intended purpose; stakeholders are kept informed of progress; and the Australian Government resources are spent appropriately.

**4.2** To assess the effectiveness of AGD's departmental arrangements for developing the NISS, the ANAO examined AGD's:

- planning framework;
- monitoring and reporting of performance; and
- project resourcing and budgeting.

### Planning framework

**4.3** Systematic and structured implementation planning reduces the risk of delay to, and dilution of, outcomes. In a practical sense, this involves: creating a map of how an initiative will be implemented; addressing matters such as time frame; phases of implementation; roles and responsibilities; and resourcing.<sup>45</sup> Successful implementation is assisted by a robust risk management approach, including the identification, assessment and treatment of implementation risks. *Australian Standard/New Zealand Standard ISO 31000:2009 Risk Management—Principles and Guidelines* proposes a logical and systematic methodology for establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risks.

**4.4** The implementation of the NISS presents the specific challenge of a whole-of-government approach. This includes several key Australian

---

<sup>45</sup> Department of Prime Minister and Cabinet and ANAO, *Better Practice Guide—Implementation of Programme and Policy Initiatives*, October 2006, p. 23.

Government agencies as well as state and territory policy departments and line agencies. In particular, the state and territory BDMs and RTAs play an integral role in their issuing of documents, namely birth certificates and driver's licences respectively, that are widely accepted in the community as evidence of a person's identity.

## **Planning for the NISS as a whole**

**4.5** The NISS outlines a framework for intergovernmental cooperation and details a work program for the six elements of the NISS. In its role of lead agency responsible for coordinating and developing the NISS, it was expected that AGD would have:

- a planning process that incorporated a risk-based approach for the entire strategy; and
- assisted the NISCG in setting the work program for successful implementation of the six NISS elements.

**4.6** The AGD advised the ANAO that rather than planning for the NISS, or elements other than the nDVS, the department relied on the higher level groups such as the NISCG to establish the work program for the NISS. Further, AGD advised that nDVS excluded, the other elements of NISS are 'policy development streams' and that as a consequence neither planning documentation nor a project methodology was prepared or used for the elements. A more robust approach to planning and managing implementation would have likely assisted in providing greater discipline to progress specific NISS elements, through the articulation of a shared understanding of the intended outcomes and monitoring of progress.

## **Planning for specific elements of the NISS**

**4.7** There was specific planning for one of the six NISS elements—the nDVS. Initially a project brief was developed in 2006–07 and AGD finalised the first project plan in July 2007. The project plan was finalised following both:

- the Government's announcement of a Budget measure to support the implementation of the nDVS in May 2006; and
- a request from the Cabinet Implementation Unit (Department of Prime Minister and Cabinet), for a project plan to be developed to provide a framework to report against.

**4.8** To assist agencies in developing implementation plans, the CIU has released a *Guide to Preparing Implementation Plans* (CIU Guide) that outlines key requirements. The nDVS project plan was developed in line with the CIU Guide and was endorsed in July 2007. The project plan provided AGD with a framework for implementation of the nDVS, including breaking down implementation into four consecutive project stages. The incorporated risk management plan included the assessment and prioritisation of key risks to implementation. The CIU Guide highlights that ‘The risk management section is one of the most important parts of an implementation plan’.<sup>46</sup>

**4.9** The nDVS, as at February 2010, was some 18 months behind the original project plan implementation dates. This is largely due to the materialisation of one of the key risks identified in 2007, namely the ‘Failure to obtain agreement from States and Territories to participate in the nDVS resulting in a failure to achieve full project objectives.’ Without key agencies signed on as ‘issuer’ agencies, the utility of and desirability of the nDVS from a user’s point of view is diminished.

**4.10** At the time of the original project plan, AGD’s approach to managing the risk of lack of take up was to develop a negotiation strategy that addressed the legal and policy issues. This strategy, however, was never formally developed. Instead, AGD embarked on a range of activities intended to cultivate agency participation with the nDVS including:

- encouraging sign-on of agencies through bilateral negotiations including the conduct of ‘road show’ demonstrations;
- encouraging sign-on of agencies through the inclusion of a standing agenda item at successive NISCG meetings; and
- escalation of the issue to First Ministers through appropriate channels.

**4.11** As noted in Table 3.1, there has been a significant increase in late 2009 in issuer agencies entering into MOUs to participate in the nDVS. Overall, therefore AGD’s approach has had some success in obtaining issuer agency participation, albeit more slowly than expected. As discussed in Chapter 3, however, increased sign-on of issuer agencies has not translated into increased user activity. The ANAO considers that the NISS project and program

---

<sup>46</sup> Department of Prime Minister and Cabinet, *Guide to Preparing Implementation Plans*, p. 9.

management is an area that requires greater management focus. AGD's new planning framework may assist in this regard.

## **AGD planning framework**

**4.12** The planning framework within AGD has undergone significant transformation in the last three years since the initiation of the NISS. At the time of the initiation of the NISS, there was no departmental strategic plan or cascading divisional/group plans. Moreover, while there were a range of planning documents for Information Technology (IT) related projects, there was limited information for non-IT related projects or programs.

**4.13** There have been a series of developments within AGD that have sought to strengthen the departmental planning and risk management framework. In late 2008, AGD issued a departmental Strategic Plan, a process repeated in 2009. In July 2009, AGD endorsed a revised corporate planning framework that defines the outcomes, program objectives, targets and deliverables for the financial year, and provides guidance to support the implementation of activities. AGD also established a project management office. The revised model is a significant development that should provide business line areas with tools to assist in the planning and implementation of policy and program initiatives. While the new framework is currently in an introductory phase, application of the project management methodology to NISS and the related six elements would assist AGD's ability to effectively coordinate the development of the NISS.<sup>47</sup>

---

<sup>47</sup> The ANAO notes the Australian Government is currently trialling the Portfolio, Programme and Project Management Maturity Model (P3M3) developed by the United Kingdom's Office of Government Commerce, following the recommendations of the *Review of the Australian Government's use of Information and Communication Technology*, 2008, by Sir Peter Gershon. The P3M3 provides a framework with which organisations can assess their current performance and put in place improvement plans with measurable outcomes based on industry best practice. Any future project management developments by AGD would need to be mindful of this context.

## Recommendation No.3

**4.14** To improve program effectiveness, the ANAO recommends the Attorney-General's Department adopts a structured planning approach for all elements of the National Identity Security Strategy, against which progress and achievement can be measured and reported.

**Attorney-General's Department response:** *Agreed.*

**4.15** Appendix 1 sets out AGD's complete response to the recommendation.

## Monitoring and reporting of performance

**4.16** An effective performance monitoring and reporting system is a key aspect of a well governed activity. It supports ongoing assessment of progress and risks and informs decisions about whether program objectives are achievable, or whether the program's scope, timing or resourcing need to be reviewed. In the context of NISS, the NISS IGA establishes an annual framework for reporting to COAG. AGD also has its own internal and external reporting requirements.

### *Formal reporting*

**4.17** Pursuant to the NISS IGA, the NISCG is required to report back to COAG every 12 months. AGD has coordinated the NISCG report, as both primary drafter, and consolidator of input. NISCG has reported to COAG in April 2007, April 2008 and June 2009. Following the initial report in 2007, these succinct (2–4 page) reports highlight specific outputs relating to the six NISS elements.

### *Monitoring and reporting at the whole-of-government level*

**4.18** The achievement of national goals for identity security is long-term in nature. Where the outcomes sought by government are at a high level and can only be achieved in the longer term, the use of intermediate outcomes, which can be achieved within a shorter time frame and which are amenable to the development of effectiveness indicators is considered good practice. Currently, the reports to COAG highlight specific outputs achieved rather than describing outcomes achieved consistent with the NISS—there are no intermediate outcomes or targets relative to the states or territories' current achievements to assist in this task. The absence of intermediate outcomes or targets limits AGD's ability to coordinate and manage the reporting of performance against the national goals.

**4.19** Going forward, it would be beneficial to seek the agreement of the states and territories to a structured approach that more clearly links the NISS related activities with the NISS objective. This may be accomplished by the use of baseline data and identifying intermediate outcomes or targets to assist in assessing progress towards the desired medium term effects of the NISS.

### **Case study: Reporting progress of nDVS**

**4.20** AGD also has specific reporting requirements for the nDVS. Following the initial Budget announcement of the nDVS, AGD reported to the CIU within the Department of Prime Minister and Cabinet, quarterly as required. Following Australian Government reprioritisation in July 2008, AGD was no longer required to report to the CIU.

**4.21** AGD has prepared *Executive Progress Reports* about the nDVS for the National DVS Steering Committee (now DVS Advisory Board). While these reports are made in response to governing bodies, reporting periods have varied between 30 and 331 days. The content of the *Executive Progress Reports* tracks key project deliverables, risks and other key relevant items. ANAO testing of the progress reports revealed that, at times, there was not alignment between the reports, actual AGD activity and the respective nDVS project plans. For example, the delayed reporting on significant events including announcement and documentation of user agreements signed and entered into.

**4.22** Performance reports are one mechanism that can be used to inform stakeholders of relevant issues and considerations. They also provide a history of a project that can be used for analysis for future development. Irregular and inaccurate reporting reduces assurance that the relevant governing bodies for the nDVS that the information they are receiving is accurate and timely. The nDVS is governed by a multi-jurisdictional advisory board that relies on AGD for information. Overall, there is scope for AGD, through accurate and timely performance reporting, to assist the DVS Advisory Board to make better informed decisions.

**4.23** Effective monitoring and reporting of projects can aid effective project governance in that it encourages decisions on project direction to be made in the context of the overall project, rather than in isolation. Public reporting of NISS progress to date has been limited. Further, irregular and inaccurate reporting has restricted the information on which the governing bodies could undertake thorough and systematic assessments of the relevant issues relating



to implementation of the nDVS. In August 2009, a revised DVS team structure was agreed to by the relevant agencies, with the establishment of the DVS Advisory Board that reports directly to NISCG. The ANAO considers that this is an opportunity for AGD to establish a monitoring and reporting regime that better supports the DVS Advisory Board in making informed decisions.

## Project resourcing and management

**4.24** AGD is responsible for project resourcing and management of the nDVS. As noted in Chapter 1, the non-DVS elements of the NISS were not specifically funded. Prior to the nDVS, AGD also had responsibility for the prototype Document Verification Service (pDVS) and a data integrity pilot. The total funding and expenditure for AGD and the nDVS is presented in Table 4.1. The ANAO notes in relation to total funding for the nDVS, there has been an underspend of the allocated budget across the relevant financial years, largely as a result of lack of progress to date.

**Table 4.1**

### nDVS funding and expenditure by AGD (\$m)

	2006–07	2007–08	2008–09	2009–10
Original Budget	8.2	5.2	5.7	5.7
Carried Forward	-	1.3	1.3	2.1
Available funding	8.2	6.5	7.0	7.8
Actual expenditure	6.8	5.2	4.9	-

Notes: Numbers have been rounded.

Source: ANAO analysis of Portfolio Budget Statements and AGD data.


**4.25** In relation to the nDVS, specific funding for AGD is split into two major components, namely the build and maintenance of the DVS Hub, and staffing and other costs. In relation to the build and maintenance of the nDVS, AGD has outsourced this component to Centrelink, with a setup cost of \$1.2 million in 2006–07, a further \$650 000 paid in 2007–08, plus ongoing monthly fees. The cost of the nDVS Hub and ongoing monthly fees was estimated based on the pDVS in the original advice to government in 2006. At the time of audit fieldwork, Centrelink was in the process of costing the arrangement of the nDVS Hub and AGD advised they would use the estimates as a basis for future negotiations.

**4.26** The remainder of the nDVS budget can be broadly spilt between the staffing costs of AGD and other significant IT related costs. AGD informed the ANAO that due to the delayed uptake and less than optimal use of the nDVS, staff costs intended for the nDVS budget had been reallocated to other tasks that broadly related to the NISS. AGD was not able to quantify to what extent staff funded from the nDVS budget were working on other matters.

**4.27** AGD has also used the nDVS funding to assist 'issuer' agencies with their operational establishment costs. The original nDVS project funding did allow for IT contingency costs, including for issuer agencies. As such, specific funding for the redevelopment of systems was made available to certain agencies. For example, the NSW Registry of Births, Deaths and Marriages (NSW BDM) received a one-off capital grant of \$500 000 to fund CVS redevelopment in November 2008.<sup>48</sup>

**4.28** Since 2005, the Australian Government has allocated \$30.8 million to AGD towards identity related security measures, including \$24.8 million towards the nDVS. There has been an underspend of the available funding over the financial years due to lack of progress with the nDVS and some of the funds allocated for the nDVS have been used for related tasks.

---



Ian McPhee  
Auditor-General

Canberra ACT  
21 April 2010

---

<sup>48</sup> The CVS is an electronic service operated by the New South Wales Registry of Births, Deaths and Marriages on behalf of the Births, Deaths and Marriages registries of Australasia. The CVS supports connection of all BDMs to the nDVS.

# Appendices



## Appendix 1: Formal comments on the proposed report



06 APR 2010  
2-30

Australian Government  
Attorney-General's Department

Secretary

09/11531

1 April 2010

Peter White  
Group Executive Director  
Performance Audit Services Group  
Australian National Audit Office  
19 National Circuit  
BARTON ACT 2600

Dear Mr White

### **Attorney-General's Department arrangements for the National Identity Security Strategy**

Thank you for providing the Attorney-General's Department with the opportunity to comment on the report of the ANAO's performance audit of the National Identity Security Strategy (the Strategy).

The identity security environment has evolved since the Council of Australian Governments first agreed to develop the Strategy in 2005. The Intergovernmental Agreement (IGA) underpinning the Strategy is also due for review from April 2010. The ANAO's performance audit is timely, providing an opportunity to review progress and identifying ways to improve as the Strategy moves forward in 2010-2015.

The Department accepts the three recommendations of the report and has commenced work to implement them. I am confident that the recommendations can be addressed through the review of the IGA and through continued application of the Department's new project management framework. As requested, formal Departmental comments are attached to this letter. These comments address each of the recommendations. A short summary of the comments, for inclusion in the report summary and brochure, are also attached. Officers from my Department have already provided you with informal, editorial commentary on the report.

Finally, I wish to express my appreciation for the ANAO's willingness to engage with officers in my Department on issues arising from the audit in such a cooperative and positive manner.

The action officer for this matter is Elsa Sengstock who can be contacted on (02) 6141 2725.

Yours sincerely

Roger Wilkins AO

3-5 National Circuit, Barton ACT 2600 Telephone (02) 6141 6666 www.ag.gov.au ABN 92 661 124 436

## Full Response

The Attorney-General's Department (AGD) welcomes the Report of the ANAO's performance audit of the Department's arrangements for the National Identity Security Strategy (the Strategy). AGD accepts the ANAO's recommendations and has commenced work to implement them.

Development of the Strategy takes place in a complex, multi-jurisdictional environment. Measures to strengthen Australia's identity security are developed to take into account the differing needs and priorities of each jurisdiction and agency. Implementation of measures to support the Strategy ultimately depends on the decisions of individual governments, which will necessarily be informed by operational and financial considerations.

The identity security environment has evolved since the Council of Australian Governments (COAG) first agreed to develop the Strategy. In 2005, the work of the Strategy was defined within a conventional framework of preventing crime, particularly identity theft. Protecting against the harms facilitated by the use of false or stolen identities remains a key priority for government efforts to prevent terrorism and organised crime, as well as to enhance border security. However, the importance of identity management to facilitate benefits has grown over the last few years. The expansion of the digital economy poses new challenges and opportunities for governments, particularly for citizen-centric, whole-of-government online service delivery. Australia's federated system of identity credentials, and the intersection of public and private sector management of identity, also creates a greater need for partnerships with business and the community to achieve the overarching goal of the Strategy.

Work to develop and implement the Strategy since 2005 has achieved some important outcomes and addressed vulnerabilities to Australia's identity security. Without this work, critical risks may have remained undetected until a potentially serious incident occurred. The progress that has been achieved to date provides a firm foundation for taking the Strategy forward.

The Intergovernmental Agreement that underpins the Strategy (the NISS IGA) provides for a review after three years' operation, to assess the circumstances and the necessity for the Agreement to continue. The review, which is to commence from April 2010, provides an excellent opportunity to address issues identified in the ANAO report. The review of the NISS IGA also provides an opportunity to reshape and refresh the work agenda and ensure

that the Strategy remains relevant to addressing current and future challenges to identity management.

### Recommendation No 1

AGD agrees that it could be beneficial to achieving the overall objectives of the Strategy if the NISS IGA clearly articulated the accountabilities of the parties involved. To this end, AGD agrees with Recommendation No 1, and will initiate action—through the National Identity Security Coordination Group (NISCG)—to formalise the roles and responsibilities of key agencies of the Strategy.

AGD agrees that more recent IGAs provide useful models for more clearly expressing the roles and responsibilities of stakeholders and will explore those models with jurisdictions in the context of the review of the NISS IGA. However, the Department notes that the IGAs cited in the Report relate to COAG initiatives that are linked to substantial Commonwealth funding. AGD notes that, in the absence of any financial incentive to offset the implementation of identity management initiatives, it may be difficult to secure the agreement of all jurisdictions to such changes.

As noted in the Report, AGD has initiated action to formalise the terms of reference and mandate of the Commonwealth Reference Group on Identity Security (CRG).

Finally, AGD welcomes the assessment in the Report that there is general alignment between the Strategy elements and NISCG working groups, and that the framework provided through the NISS IGA has facilitated the establishment of ad hoc working groups to assist whole-of-government responses to emerging issues (such as the 2009 Victorian bushfires).

### Recommendation No 2

AGD acknowledges that the activities that have been undertaken, and outputs produced, have not always strictly matched the original work program as articulated in the NISS IGA. The NISS IGA itself provided that the work program was to be considered as a ‘work-in-progress’, requiring further consideration. Work undertaken in relation to the various Strategy elements was driven and defined by NISCG. Accordingly, AGD considers that the activities and outputs were commensurate with the evolving objectives of the Strategy.

However, AGD agrees that it is timely to assess the current objectives and appropriateness of the elements of the Strategy. AGD therefore agrees with Recommendation No 2 and will initiate action, through NISCG, to ensure that deliverables remain linked to objectives. Again, action to address this recommendation will take place in the context of the review of the NISS IGA.

AGD recognises that progress on implementing the national Document Verification Service (nDVS) has been slower than anticipated, and that this, and other complex issues, have delayed uptake of the system by government agencies. AGD acknowledges that the resolution of some issues has taken time, and in some instances is not complete. However, AGD considers that it has been responsive to emerging problems.

The Report concludes that planning for the nDVS was inadequate, and that AGD did not fully appreciate key risks to the project or implement appropriate treatments where those risks materialised. While AGD does not wholly agree with this conclusion, AGD does support ANAO's suggestion to conduct a systematic review of barriers to uptake of the nDVS and developing remedial strategies as a matter of priority. AGD also acknowledges the need for a central register of nDVS MOUs, and has taken action to address this.

### Recommendation No 3

AGD agrees with Recommendation No 3, which seeks to improve program effectiveness through the adoption of a structured planning approach for all elements of the Strategy, against which progress and achievement can be measured and reported.

For Strategy-related work falling within its direct responsibilities (including the nDVS), AGD will continue to improve upon its use of planning tools, including application of the new AGD Project Management Framework. Planning and management of measures to support the Strategy (other than the nDVS) is the responsibility of NISCG. However, as lead agency, AGD will initiate action, through NISCG, to enhance planning of the future work program of the Strategy.

The Report also raises concerns about the difficulty in assessing the impact of various Strategy-related activities because of a lack of reporting on implementation of measures. The Report also notes that, in light of the relatively high-level and long term goals of the Strategy, it would be useful to identify intermediate outcomes that can be achieved in shorter timeframes and that could be measured and reported upon.



AGD considers that these issues could be addressed through the review of the NISS IGA, and that subject to jurisdictions' views, a more rigorous monitoring and reporting process could be put in place. AGD notes, however, that it may be difficult to quantify the impact of initiatives given the lack of baseline data and reliability of data sources.

In relation to particular concerns expressed in the Report about planning and reporting on the nDVS, AGD will ensure that careful attention is given to the accuracy and timeliness of future reports on the nDVS for the DVS Advisory Board.

AGD considers that the underspend on the available funding is appropriate given the delay in incurring certain expenses associated with the nDVS, and notes that this funding will be required as more agencies connect to the nDVS.

## Appendix 2: Other Australian Government initiatives and international approaches to identity security

### Other Australian Government initiatives

The development of a single national identity card or consolidation of identity credentials has also been promoted within Australia as a means of addressing a range of identity related issues with varying political success. The *Australian Card Bill 1986* was introduced into Parliament in 1986 by the then Labor government with the intended purpose of preventing losses to revenue through the taxation system and payment of Government benefits. After defeat in the Senate, in 1987 the Bill was reintroduced without change. It was once again rejected by the Senate and became the trigger for a double dissolution election in 1987. Following the resultant election, the Bill was reintroduced for a third time but was laid aside following legal advice and loss of political support.

In 2005, the then Prime Minister John Howards revisited the concept of a national identity card in the wake of the London bombings, stating:

We haven't made a decision to have an ID card in this country, but it should properly be on the table, and we should properly assess whether in the light of what's happened in the 17 or 18 years that have gone by since the Australia Card was debated, and I acknowledge back then I had a view which is critical of that.<sup>49</sup>

While a national identity card was not progressed, in April 2006, Cabinet approved an access card to replace 17 health and social services cards within the Human Services portfolio. On 7 February 2007, the access card bill (*Human Services (Enhanced Service Delivery) Bill 2007*) was introduced into Parliament but was initially withdrawn after privacy concerns. An exposure draft of a revised Bill was released in June 2007. Sub-section 6(2) of the Bill specifically states that 'It is also an object of this Act that access cards are not to be used as, and do not become, national identity cards.' Following the November 2007 election, the new government decided not to proceed with the access card.

---

49 Prime Minister, Door stop interview, 15 July 2005, Sydney.

## International approaches

The concept of a national identity card is common to many countries, including many European countries, however it is used less within common law countries such as the United Kingdom, New Zealand and Canada. The development of a national identity strategy and a related document verification service, however, is a common trend, partly due to the issues countries face with regards to identity fraud and balancing privacy issues with a government's ability to be able to confidently interact with its citizens. The following survey highlights the variety of approaches currently in progress.

### *United Kingdom*

The United Kingdom has adopted the National Identity Scheme (the Scheme), a program which aims to allow everyone with the opportunity to have an identity card if they choose. Under the Scheme, an identity card will offer a way for an individual to prove their identity in a wide variety of circumstances. Depending on the level of identity assurance required for a particular transaction, an individual's identity will either be checked visually, through entry of a PIN number or by checking fingerprints via a chip on the card, or for the highest level of assurance, a check against the National Identity Register (NIR).

### *New Zealand*

The Department of Internal Affairs and State Services Commission has developed what is called the Identity Verification Service (IVS), which is intended to allow people to verify their identity to government agencies online and in real-time to a high level of confidence, using their name, date of birth, place of birth and sex. The purpose of the new service is to allow citizens to use the Internet as a more convenient way to prove themselves when they are dealing with government agencies. The roll out of the IVS is part of a broader whole-of-government authentication project and still in development stages.

### *Canada*

While the Government of Canada has not announced a specific identity strategy, it has undertaken a number of initiatives in the area of identity management, including its own versions of Australia's Document Verification Service, known as the National Routing System (NRS). The NRS' primary use is by Passport Canada, Canada Revenue Agency and Statistics Canada. Future functionality in relation to broader use by more agencies is in the relatively early stages of development.

## Appendix 3: List of POI document types

Table A 1 provides a comprehensive (but not exhaustive) list of POI document types accepted by various Australian, state and territory government agencies when enrolling individuals for services. The ANAO reviewed the varying enrolment processes of each agency that intended to use the nDVS as at the time of fieldwork, and collated the incidence of use of each type of document. These are listed in order of the most commonly relied upon to those least commonly relied upon.

These ‘types’ of documents were created by grouping some POI documents. For example, many agencies accepted various government entitlement cards, such as a Veteran’s Affairs Card or a Health Care Card—these were all grouped as ‘A card evidencing a client’s entitlement to a government benefit’.

**Table A 1**

### List of commonly accepted Proof of Identity (POI) document types

POI document type	
1	Australian Passport
2	Driver's Licence
3	Birth Certificates
4	A card evidencing a client's entitlement to a government benefit
5	Medicare Card
6	Financial institution card
7	Citizenship papers
8	Student identity document
9	Department of Immigration and Citizenship issued travel documents/permissions
10	Firearm Licence
11	Australian Defence Force identity documents
12	Police Officer identity card
13	Proof of age cards
14	Utility or services account
15	Overseas issued passport
16	Financial institution statement
17	Overseas passport with valid visa

POI document type	
18	Rates notice
19	Department of Immigration and Citizenship issued Certificate of Evidence of Residence Status
20	Australian Defence Force service records
21	Financial institution passbook
22	Report from educational facility
23	Change of name document issued by a Births, Deaths and Marriages agency
24	Security Guard/ Crowd Controller Licence
25	Passport Office issued Document of Identity
26	Proof of electoral enrolment
27	Marriage Certificates issued by a Births, Deaths and Marriages agency
28	Current vehicle registration papers
29	Department of Foreign Affairs and Trade issued Consular Identity Card
30	Rental/Lease contracts
31	New South Wales Photo Card
32	Deed Poll document
33	Taxation notice
34	Divorce papers
35	State or Federal Government employee photo–identity card
36	Insurance policy documentation
37	Trade Certificates
38	Stored photograph and signature on database
39	Birth Card
40	Tasmanian Government Personal Information Card
41	Evidence of change of name
42	Acknowledgement letter from Indigenous Community
43	Overseas issued Birth Certificate
44	Department of Foreign Affairs and Trade issued Document of Identity
45	Evidence of Health Insurance membership
46	Employment record
47	Land valuation notice

POI document type	
48	Department of Immigration and Citizenship issued Certificate of Identity
49	Proof of Identity declaration
50	Driver's accreditation
51	Driving authority
52	Mobility Parking Scheme Card
53	Security Industry or Commercial Agents & Private Inquiry Agents operator licence
54	Boat Operator photo licence
55	Tax File Number confirmation
56	PAYG summary
57	Northern Territory Security Identification
58	Northern Territory (NT) Approved Identity Card (with photo)
59	Other financial documents
60	Mortgage papers or deeds
61	Letter from School Principle
62	Baptismal Certificate
63	Overseas Driver's Licence
64	Department of Foreign Affairs and Trade issued travel document with valid visa
65	Other licence type
66	Motoring association card
67	Registration certificate from a professional board
68	United Nations High Commissioner for Refugees (UNHCR) document
69	National identity card
70	Correspondence from government service providers
71	Other overseas documents
72	Registry staff accepted documents
73	Photo identity
74	Security access card
75	Other documents containing a signature and photograph such as air crew identity document, seafarer identity document or military identity document

Source: Analysis of 18 published POI frameworks used by 17 different Australian, State and territory Government agencies in their enrolment processes.

## Appendix 4: POI framework

**Table A 2**

**POI framework as presented in the Report to Council of Australian Governments, April 2007**

Objective	Documents Satisfying the Objective
<b>A</b> Evidence of commencement of identity in Australia (Mandatory for all agencies)	<ul style="list-style-type: none"> <li>• Birth certificates</li> <li>• Record of Immigration Status: <ul style="list-style-type: none"> <li>– Foreign Passport &amp; current Visa</li> <li>– Travel Document &amp; current Australian Visa</li> <li>– Certificate of Evidence of Residence Status</li> <li>– Citizenship Certificate</li> </ul> </li> </ul>
<b>B</b> Linkage between Identity and Person (Photo & signature)	<ul style="list-style-type: none"> <li>• Australian Drivers Licence (current &amp; original)</li> <li>• Australian Passport (current)</li> <li>• Firearms Licence (current &amp; original)</li> <li>• Foreign Passport</li> </ul>
<b>C</b> Evidence of Identity Operating in the Community (Could be another Category A or B document)	<ul style="list-style-type: none"> <li>• Medicare Card</li> <li>• Change of Name Certificate – Non Standard POI – (for marriage or legal name change – showing link with previous name/s)</li> <li>• Credit or Account Card</li> <li>• Centrelink or DVA card</li> <li>• Security guard/Crowd control Licence</li> <li>• BDM Issued Marriage Certificate</li> <li>• Tertiary ID Card</li> </ul>
<b>D</b> Evidence of residential address (Used only to provide evidence of residential address if not provided by a Category B or C document)	<ul style="list-style-type: none"> <li>• Utilities notice</li> <li>• Rent details</li> </ul>

Source: Attachment A to NISCG, *Report to the Council of Australian Governments on the elements of the National Identity Security Strategy*, 2007.

## Appendix 5: Progress of the NISS elements (nDVS excluded<sup>50</sup>)

### Registration and enrolment standards

#### Work program (NISS IGA)

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.

This element involves the development and implementation of registration and enrolment standards. A draft version of a Gold Standard Enrolment Framework (GSEF) was developed prior to the COAG agreement and the GSEF principles were included in the 2007 NISCG submission to COAG. The GSEF specifies a premium or 'Gold Standard' approach for use by government agencies who enrol individuals for the purposes of issuing government documents that may also function as key documents for POI purposes. It is drafted to apply to a limited class of agencies based on individual agency's own determination.

In late 2009, AGD drafted a *Primer for a Review of Enrolment Standards* which was presented to NISCG in November 2009. This review document promotes a risk based framework and identifies and specifies key documents and the standard of enrolment necessary.

### Security Standards for proof of identity documents

#### Work program (NISS IGA)

It is intended that this element 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.

This element is intended to improve the technical security features of POI documents. It encompasses training considerations for front-line and second-line examiners<sup>51</sup> in detecting fraudulent identification, and highlights the need to review standards every three years to keep pace with developments in technology and patterns of fraud. The security standards for proof of identity documents (SS for POI) were detailed, proposed and agreed to in the inaugural

<sup>50</sup> The NISS comprises six elements (see Table 1.2). This appendix sets out progress in relation to five elements. Progress in relation to the sixth element, the nDVS, is discussed in Chapter 3.

<sup>51</sup> This includes, for example, customer support officers.



2007 report to COAG. The SS for POI recommends a set of security standards, with the aim of reducing the risk of forgery or unauthorised alterations of documents. The framework for the security standards is based on a tiered system of security features which should be applied on a risk-based approach to the type of document issued. The SS for POI was based on a substantial body of work performed by the Commonwealth Scientific and Industry Research Organisation.

## Standards in the processing and recording of identity data

### Work program (NISS IGA)

Work will devise standards that will provide guidance on improving the accuracy of personal identity information held on government agencies' databases.

This element is intended to ensure that government agencies responsible for issuing documents that are subsequently relied upon for identification purposes have mechanisms, based on standards, in place to ensure the integrity of identity data. The importance of this element is noted in the work program to the NISS IGA as a key element of the strategy, with particular importance to the effective operation of the nDVS.

A key background piece of work for this element was an integrity of identity data pilot project that was commissioned as part of the 2005–06 pilot programs on identity security related issues. In 2008, an *Integrity of Data Pilot* was completed. The project compared a random sample of 25 000 Australian Taxation Office records with records held by Centrelink, Medicare Australia and NSW Registry of Births, Deaths and Marriages. The pilot was designed to trial and develop processes to enable effective data matching between government agencies in order to improve the accuracy of their databases. The outcome of the pilot was to outline a range of policy issues relevant in the use of data matching exercises, which were to form the basis of standards.

Various papers have since been developed by AGD relating to 'integrity of data' including the *Improving the Integrity of Identity Data: Data Matching–Better Practice Guidelines, Change of Name, Change of Gender, Change of Date and Birth and Place of Birth* discussion papers.<sup>52</sup> The *Data Matching–Better Practice Guidelines* were made available on the AGD website in February 2010. A

<sup>52</sup> AGD has also developed other papers including *One person, One identity: Filling the gaps in identity security* and *Change of Date and Place of Birth procedures in Australia*.

common theme in the development of all these papers is the difficulties faced when dealing in a multi-jurisdictional environment with often seemingly competing policy and legislative environments.

## **Authentication standards**

### **Work program (NISS IGA)**

It is proposed that this element 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.

This element is intended to ensure that government agencies responsible for issuing POI documents have the appropriate means to authenticate an individual's identity. Initial progress on this element was strong. There was a clear objective to issue standards which was achieved in a relatively short time frame. The Gold Standard e-Authentication Requirements (GSAR) was being developed prior to the NISS IGA, and were escalated through the working groups and endorsed by the NISCG in March 2008. This was reported in the NISCG report to COAG in April 2008, however, the 2009 NISCG report to COAG made no update regarding further implementation of this element.

Simultaneous to the development of GSAR has been the National e-Authentication Framework (NeAF), released in January 2009 by the Australian Government Information Management Office. The NeAF was developed to provide a consistent, whole-of-government approach to managing identity related risks. The NeAF is endorsed by the Australian Online and Communications Council, which operates as the peak ministerial forum across Australia on strategic approaches to information and communications technology issues.

## Biometric interoperability

### Work program (NISS IGA)

This element will outline types of biometric systems, issues about standardisation and interoperability and community acceptance.

This element is intended to enhance the interoperability of biometric identity security measures. Broadly speaking, biometrics refers to the automated use of recognising a person through the use of distinguishing physiological or behavioural traits.<sup>53</sup> A person's biometric information can assist in identifying the person and/or verifying their claimed identity. The technology behind biometrics, and its associated standards, is evolving rapidly.

The 2007 report to COAG noted that the Australian Government has a preference for cooperating on international standards rather than developing purely local standards. International efforts to standardise biometrics has been led by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Civil Aviation Organisation (ICAO). Australia's involvement in the setting of standards is being driven by the Australian Government, in particular through the Department of Foreign Affairs and Trade (DFAT).<sup>54</sup>

There has been a range of activities designed to enhance the national interoperability of biometric identity security measures such as the *National Smart Card Framework*. The framework sets minimum standards to optimise smartcard interoperability and was developed by the Australian Government Information Management Office (AGIMO) and endorsed by the Online and Communications Council.

Within the NISS framework, the Biometrics, Authentication and Security Standards working group first met in February 2008 and was initially working primarily as an information sharing forum regarding biometric initiatives. In 2009, the focus turned the development of a biometrics policy. At the CRG working group level, a draft *Australian Government Biometrics Policy* and draft *Australian Government Implementation Guide* has been developed. These two documents have also been circulated through the NISCG and BASS working group for discussion and approval.

<sup>53</sup> *Biometrics Deployment of Machine Readable Travel Documents*, ICAO Document 9303, ICAO, 2004.

<sup>54</sup> National Identify Security Coordination Group, Report to COAG, April 2007, p. 53.

# Series Titles

---

**ANAO Audit Report No.1 2009–10**

*Representations to the Department of the Treasury in Relation to Motor Dealer Financing Assistance*

Department of the Treasury

Department of the Prime Minister and Cabinet

**ANAO Report No.2 2009–10**

*Campaign Advertising Review 2008–09*

**ANAO Audit Report No.3 2009–10**

*Administration of Parliamentarians' Entitlements by the Department of Finance and Deregulation*

**ANAO Audit Report No.4 2009–10**

*The Management and Processing of Annual Leave*

**ANAO Audit Report No.5 2009–10**

*Protection of Residential Aged Care Bonds*

Department of Health and Ageing

**ANAO Audit Report No.6 2009–10**

*Confidentiality in Government Contracts – Senate order for Departmental and Agency Contracts (Calendar Year 2008 Compliance)*

**ANAO Audit Report No.7 2009–10**

*Administration of Grants by the National Health and Medical Research Council*

**ANAO Audit Report No.8 2009–10**

*The Australian Taxation Office's Implementation of the Change Program: a strategic overview*

**ANAO Audit Report No.9 2009–10**

*Airservices Australia's Upper Airspace Management Contracts with the Solomon Islands Government*

Airservices Australia

Department of Infrastructure, Transport, Regional Development and Local Government

**ANAO Audit Report No.10 2009–10**

*Processing of Incoming International Air Passengers*

Australian Customs and Border Protection Service

ANAO Audit Report No.29 2009–10

Attorney-General's Department Arrangements for the  
National Identity Security Strategy

**ANAO Audit Report No.11 2009–10**

*Garrison Support Services*  
Department of Defence

**ANAO Audit Report No.12 2009–10**

*Administration of Youth Allowance*  
Department of Education, Employment and Workplace Relations  
Centrelink

**ANAO Audit Report No.13 2009–10**

*Major Projects Report 2008–09*  
Defence Materiel Organisation

**ANAO Audit Report No.14 2009–10**

*Agencies' Contract Management*  
Australian Federal Police  
Austrade  
Department of Foreign Affairs and Trade

**ANAO Audit Report No.15 2009–10**

*AusAID's Management of the Expanding Australian Aid Program*  
AusAID

**ANAO Audit Report No.16 2009–10**

*Do Not Call Register*  
Australian Communications and Media Authority

**ANAO Audit Report No.17 2009–10**

*Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2009*

**ANAO Audit Report No.18 2009–10**

*LPG Vehicle Scheme*

**ANAO Audit Report No.19 2009–10**

*Child Support Reforms: Stage One of the Child Support Scheme Reforms and Improving Compliance*

**ANAO Audit Report No.20 2009–10**

*The National Broadband Network Request for Proposal Process*  
Department of Broadband, Communications and the Digital Economy

**ANAO Audit Report No.21 2009–10**

*Administration of the Water Smart Australia Program*  
Department of the Environment, Water, Heritage and the Arts  
National Water Commission

**ANAO Audit Report No.22 2009–10**

*Geoscience Australia*

**ANAO Audit Report No.23 2009–10**

*Illegal Foreign Fishing in Australia's Northern Waters*  
Australian Customs and Border Protection Service

**ANAO Audit Report No.24 2009–10**

*Procurement of Explosive Ordnance for the Australian Defence Force*  
Department of Defence

**ANAO Audit Report No.25 2009–10**

*Security Awareness and Training*

**ANAO Audit Report No.26 2009–10**

*Administration of Climate Change Programs*  
Department of the Environment, Water, Heritage and the Arts  
Department of Climate Change and Energy Efficiency  
Department of Resources, Energy and Tourism

**ANAO Audit Report No.27 2009–10**

*Coordination and Reporting Australia's Climate Change Measures*  
Department of Climate Change and Energy Efficiency  
Department of Innovation, Industry, Science and Research

**ANAO Audit Report No.28 2009–10**

*The Australian Electoral Commission's Preparation for and Conduct of the 2007 Federal General Election*

# Current Better Practice Guides

---

The following Better Practice Guides are available on the Australian National Audit Office website.

## Innovation in the Public Sector

Enabling Better Performance, Driving New Directions Dec 2009

## SAP ECC 6.0

Security and Control June 2009

Preparation of Financial Statements by Public Sector Entities June 2009

## Business Continuity Management

Building resilience in public sector entities June 2009

Developing and Managing Internal Budgets June 2008

Agency Management of Parliamentary Workflow May 2008

## Public Sector Internal Audit

An Investment in Assurance and Business Improvement Sep 2007

## Fairness and Transparency in Purchasing Decisions

Probity in Australian Government Procurement Aug 2007

Administering Regulation Mar 2007

## Developing and Managing Contracts

Getting the Right Outcome, Paying the Right Price Feb 2007

## Implementation of Programme and Policy Initiatives:

Making implementation matter Oct 2006

Legal Services Arrangements in Australian Government Agencies Aug 2006

Administration of Fringe Benefits Tax Feb 2006

## User-Friendly Forms

Key Principles and Practices to Effectively Design  
and Communicate Australian Government Forms Jan 2006

Public Sector Audit Committees Feb 2005

Fraud Control in Australian Government Agencies Aug 2004

Better Practice in Annual Performance Reporting Apr 2004

Management of Scientific Research and Development Projects in Commonwealth Agencies	Dec 2003
Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003
Building Capability—A framework for managing learning and development in the APS	Apr 2003
Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	June 2001
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Commonwealth Agency Energy Management	June 1999
Controlling Performance and Outcomes	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997