

## Appendix B: Regulatory Impact Assessment

# Impact Summary: Information sharing for identity services

## Agency Disclosure Statement

This Regulatory Impact Assessment (RIA) has been prepared by the Department of Internal Affairs (the Department). It provides an analysis of options to enable the sharing of information within the Department and the creation of the customer single view.

Information sharing agreements between government agencies require the privacy of individuals to be considered and balanced against the need for government agencies to provide efficient, high quality services. The Department has been assessing options to enable a more efficient approach to authorised sharing of information. The intent is to allow sharing for a broader range of purposes, to reduce multiple requests for the same information, and to remove time delays in the provision of services to the public.

Consultation on an earlier Cabinet paper seeking approval to this approach has been undertaken with the Office of the Privacy Commissioner as well as the Ministry of Justice; Treasury; New Zealand Police; New Zealand Security Intelligence Service; the Department of the Prime Minister and Cabinet (Policy Advisory Group) has also been informed. Cabinet approved the proposed approach of replacing existing information sharing agreements with Approved Information Sharing Agreements and authorised public consultation. Public consultation has been carried out, with one submission received and no significant changes to the proposed approach.

The Privacy Commissioner is comfortable with the proposals presented under the recommended option and has expressed full support.

The recommended option will not incur significant additional costs to the Department. It is difficult to determine the number of people who may be impacted by the proposed approach but it is envisaged the recommended policy option will continue to provide additional benefits to the Department and its customers in the form of efficiency gains and better service provision.

None of the policy options would impair private property rights, restrict market competition, reduce incentives for business to innovate and invest, or override fundamental common law principles.

Darren Godden

Te Ara Manaaki

Service Delivery and Operations

Department of Internal Affairs

## STATUS QUO AND PROBLEM DEFINITION

The Department is the custodian of important data sets that are created through processes such as birth, death and marriage registration and applications for New Zealand citizenship or for a New Zealand passport. These data sets contain key information about an individual's identity and life events, and are relied on daily by New Zealanders and government agencies to access other government and non-government services. For example, birth and citizenship details are used by individuals and health service providers to verify that the individual is entitled to free health care in New Zealand.

The Privacy Act 1993, Information Privacy Principle 10 (IPP10), requires that specific authorising arrangements must be put in place to allow any information to be used for purposes other than those for which it is collected. The primary purpose for collecting identity and life event information held by the Department is set out in the primary legislation for each data set. Verification of identity and entitlement details is a secondary purpose, not covered by the primary legislation, so requires separate authorisation.

The current authorising arrangements that allow the Department to vary IPP10 for the provision of identity services consist of four Information Matching Agreements (IMAs). The IMAs that enable the sharing of information within DIA are:

- Births, Deaths and Marriages / DIA Passport Application Processing Information Matching Agreement July 2003
- Citizenship / Passport Application Processing Information Matching Agreement August 2003
- Citizenship / Births Information Matching Agreement 2005
- Citizenship / Births, Deaths and Marriages Application Processing Information Matching Agreement 2009.

These agreements are inflexible and inefficient to maintain and update, and do not support future directions for service transformation. A key constraint is that their application is tightly defined in existing legislation, and cannot be extended to enable the information sharing necessary for customer-centred service transformation without legislative change. As such they are at odds with the direction that is being taken by the Department, as articulated in the Te Ara Manaaki transformation programme.

Te Ara Manaaki is an innovative, solution-focused programme with a vision to transform the way New Zealanders access identity and life event services – putting customers and their whānau at the heart of what the Department does. Over the next three to six years, the Department will transform service delivery, making it easier for people to access the services they want, whenever and wherever they choose, enabled by mobile and digital platforms.

The Department requires an appropriate authorising framework for internal information to deliver Te Ara Manaaki objectives such as creating a single view of the customer and improving data quality. The primary problem is that the existing purpose statements are product-based and do not permit information to be shared for the purpose of establishing a single view of the customer.

The information matching needed to deliver Te Ara Manaaki objectives does not fit with the purpose statements detailed in Schedule 1A of the BDMRRA. To authorise the required information sharing, either Schedule 1A would need to be amended via a legislative change or the Department would need to develop an Approved Information Sharing Agreement (AISA). In the broader legislative context, the Privacy Bill currently before the House

proposes that the development of new information matching agreements be discontinued, and that future information sharing be authorised through AISAs.

An AISA is an enabling tool that enables government agencies to provide efficient and effective public services. An AISA can do this by allowing agencies to collaborate and share information without intruding on individuals' rights or exposing agencies to legal risk.

The Department is proposing an Identity Services AISA that would provide an overarching authorising framework for the internal sharing of birth, death, marriage, civil union, name change, citizenship and passport information. This will mirror the variation to IPP10 authorised by the existing IMAs, and will assist with the delivery of identity and life event services (i.e. birth, death, marriage, civil union, citizenship and passport services) to New Zealanders.

In addition to replacing the four IMAs, the Identity Services AISA will authorise a new capability to create the customer single view, a joined-up view of an individual DIA customer's identity and life event information to facilitate the provision of identity services. This will allow DIA to treat the person as an individual, rather than a series of unconnected life events, and to provide personalised, customer-centred services. It is also an essential foundation for future improvements to information quality, as it will be easier to identify and correct any discrepancies in records relating to the same person. It is important to note that the customer single view does not create any enduring record or new register.

The technology changes underpinning these improvements will be delivered as part of DIA's Te Ara Manaaki - Transforming the System of Service Delivery programme. One of the key objectives of this programme, as part of the government's digital transformation, is to ensure New Zealanders have access to personalised services when and where they need them. While the initial technology changes are expected to be delivered from late 2018 onwards, the new customer single view capability cannot be implemented until the authorising framework (the AISA) is in place.

## **Section 2: Problem definition and objectives**

The Te Ara Manaaki Strategy for Refreshing the Authorising Environment has established a vision for the future of sharing the identity and life event information the Department holds to support customer-centred services. . The strategy is intended to equip DIA with the right authorisations (laws, regulations and agreements) to enable appropriate and secure information sharing that protects individuals' privacy.

The Privacy Act sets out core requirements around privacy for all of government. Primary legislation also frames how the Department collects, stores and uses information. The legal environment in which the Department operates contains a range of instruments that define how information is to be shared between agencies.

There are a number of problems with the Department's current authorising environment for information sharing that make it difficult to meet the needs of customers and to transform services. The major barriers and problems that need to be addressed through the authorising environment are:

- **Confusion and duplication** - There are currently about 40 legal instruments that set out information sharing arrangements applying to the identity and life event information held by DIA. It is very difficult to maintain a clear overview of what is allowed and what is actually happening, and some agencies have multiple agreements with us. The sheer volume of current agreements means that any global changes such as move to a new technology approach will require a significant amount of work to update agreements.
- **Inflexibility/barriers to technology change** - Information sharing arrangements that are written into primary legislation are difficult to change, and that process takes considerable time. The degree of specificity required for IMAs means that they have to be updated every time a process or technical setting is varied; given that Te Ara Manaaki envisages iterative technology and process changes, this makes the process of updating existing IMAs time-consuming and likely repetitive as iterative technology changes are rolled out.
- **Inability to respond to customer needs** - This problem follows on from the previous point. Just as the sheer volume, complexity and detailed nature of existing agreements makes technology change difficult to authorise, they also create a barrier to responding flexibly to emerging customer needs and transforming services. At worst, time is invested in information sharing arrangements that are seldom, if ever, used because of their poor fit to needs. Wherever possible, the Department needs to create authorising arrangements that allow reuse and variation within appropriate controls.

These problems stem from the way that data sets of personal information have historically been created and held by government. In short, many of the data sets of personal information were created as islands of information, with little or no thought of sharing the information systematically and electronically with other government agencies or non-government organisations. The earliest requirements for sharing the Department held information with other organisations mostly relate to births, deaths and marriages, and are usually set out in other legislation that requires DIA to share specified information (e.g. the Veterinarians Act requires the Registrar-General to notify their professional body when the death of a member of their profession is registered).

New requirements for information sharing have emerged and in response information matching agreements began to be used for a wider range of situations, and proliferated. It became evident that they were not fit for purpose for some of the intended uses (e.g. agreements with multiple parties). Therefore the Approved Information Sharing Agreement (AISA) was introduced. AISAs are intended to be a much more flexible instrument that would meet a broader set of needs.

The Privacy Act allows for AISAs to be established for the information sharing for the purpose of providing public services. Each AISA is established by an Order in Council. There are currently seven AISAs in use by a range of government agencies. These include:

- Information sharing agreement between Inland Revenue and the Department of Internal Affairs
- Information sharing between Inland Revenue and New Zealand Police
- Information sharing agreement for improving public services for vulnerable children
- Information sharing agreement supporting research using the Integrated Data Infrastructure (IDI) at Statistics New Zealand
- Information sharing agreement between the Ministry of Education and the Ministry of Social Development
- Information sharing agreement between Inland Revenue and the Ministry of Social Development
- Information sharing agreement between the Ministry of Justice and the Crown Law Office

## **2.2 Who is affected and how?**

The central objective of the information sharing covered by the Identity Services AISA is to improve the Department's identity services for New Zealanders. Key benefits include:

- a customer's identity and entitlement to services will be able to be confirmed by checking their relevant Department-held records without the customer having to provide documents (e.g. birth certificate) as evidence;
- people applying for a Department identity service will be able to consent to the Department pre-filling their application with information that the Department already holds about them;
- the Department will be better enabled to confirm relationships between individuals, e.g. when an adult is applying for a passport on behalf of a child; and
- the Department will be able to advise an individual about services they may be entitled to.

The services that will benefit from this AISA include:

- birth, death, and name change registration and ordering of related certificates
- services relating to marriages and civil unions (licences, celebrant registration, certificates)
- citizenship services, and
- passports and other New Zealand travel document services.

The more integrated view of customer data will enable the Department to better identify data anomalies which will lead to improved fraud detection and investigation.

### **Departmental staff – customer responsiveness**

The 'customer single view' will enable the Department to have a temporary joined-up view of an individual customer's identity and life event information to facilitate the provision of identity services. This will allow the Department to treat the person as an individual, rather than a series of unconnected life events, and to provide personalised, customer-centred services.

### **Customer – transparency and consent**

A single agreement authorising this information sharing will make it easier for customers to understand how their information held by the Department may be used to facilitate other services that they request from the Department. At present customers would need to read four separate agreements in order to understand all the information sharing relationships involved in providing identity and life event services.

The customer single view is an essential foundation for future improvements to information quality, as it will be easier to identify and correct any discrepancies in records relating to the same person. This is expected to reduce the requirement to go back to customers to resolve information issues.

**2.3 Are there any constraints on the scope for decision making?**

Cabinet has already agreed to the broad approach to information sharing for identity services [CAB -18-MIN-0016 refers].

The primary legislation, the Privacy Act, sets the framework for what an AISA can contain and the issues it can address. Each AISA must be created by Order in Council and its operation is subject to review by the Privacy Commissioner.

The Te Ara Manaaki transformation programme is establishing a customer-centric operating model that will enable customers to provide, access and control data about themselves. The customer single view, which will be authorised by the Identity Services AISA, is an essential enabler of this outcome. Were this AISA not to proceed, there would be a significant negative impact on the delivery of the outcomes of Te Ara Manaaki.

**Section 3: Options identification**

**3.1 What options have been considered?**

A range of options was considered for renewing the authorising environment to enable Te Ara Manaaki outcomes. A summary of the advantages and disadvantages of each option is provided in the table below:

Policy Option	Advantages	Disadvantages
Legislative change	<ul style="list-style-type: none"> <li>• Would enable a bespoke solution to the sharing of identity information</li> </ul>	<ul style="list-style-type: none"> <li>• Multiple Acts would need to be changed meaning that there would be a long timeframe required for legislative and operational changes to be implemented</li> <li>• There are also uncertainties with the outcomes of legislative processes</li> <li>• A bespoke solution would not support improved information sharing practices with other agencies</li> <li>• Difficult to build in sufficient 'future proofing' given the current rate and scope of technology change</li> </ul>

Continue to use IMAs	<ul style="list-style-type: none"> <li>• No change needed</li> <li>• Less time intensive than developing an AISA</li> </ul>	<ul style="list-style-type: none"> <li>• Difficult to build in sufficient 'future proofing' given the current rate and scope of technology change</li> <li>• Current IMAs do not enable single customer view – they are too narrow in focus and inflexible (Schedule 1A of the BDMRRA and Schedule 4 of the Citizenship Act).</li> <li>• The future use of IMAs is in doubt given the proposals in the Privacy Bill currently being considered by Parliament</li> <li>• Would not enable multi-party information sharing</li> </ul>
Develop an Identity Services AISA	<ul style="list-style-type: none"> <li>• The development process provides a robust assessment process involving the Privacy Commissioner and public consultation</li> <li>• Can be structured to build in 'future proofing' that can take advantage of future technological change</li> <li>• An AISA would enable the Department to streamline its internal information sharing arrangements such four bilateral arrangements would be replaced by one agreement.</li> </ul>	<ul style="list-style-type: none"> <li>• An AISA is not an 'off the shelf' solution, each AISA must be custom designed – as such the process can take approximately 12- 18 months</li> </ul>

The prescribed process for developing and publishing an AISA is robust and transparent, which makes this a good option from a privacy perspective.

An AISA is a legal mechanism made by Order in Council under Part 9A of the Privacy Act that authorises the sharing of information between or within agencies for the purpose of delivering public services.

An AISA describes the specific agencies involved in delivering the public service, why they are delivering it, what personal information they need to share, and what they will do with the information, including how they will manage any privacy risks.

An AISA authorises agreed departures from information privacy principles if there is a clear public policy justification and the privacy risks of doing so are managed appropriately. By providing certainty around information to be shared, an AISA removes doubt around whether there are any privacy implications and impediments to information sharing. AISAs are also public documents.

An AISA can only be made if it meets a certain standard, including having checks and balances in place to protect the privacy of individuals. In addition, the Privacy Act requires an AISA to be made by following a transparent process. This includes:

- consulting with the Privacy Commissioner, who can review an AISA once it comes into effect and make other recommendations for change

- undertaking consultation with affected persons making an AISA under an Order in Council.

### 3.2 Which of these options is the proposed approach?

The Department considers that the best option is to develop an Identity Services AISA that will enable streamlined information sharing to support the Department's delivery of identity services. The development of the AISA will support the wider programme of work to transform customer services through technology, system, policy and process changes.

There are no areas of incompatibility with the Government's 'Expectations for the design of regulatory systems', in summary:

- the purpose of the AISA has been clearly articulated and will allow delivery of improved customer services in a cost effective manner without impacting on the privacy and security of personal information or undermining the principles of the Privacy Act.
- the introduction of the customer single view will enable the Department to provide responsive services to customers.
- the AISA has processes that produce predictable and consistent outcomes for regulated parties across time and place.
- there are no Treaty of Waitangi, human rights, gender or disability implications.
- there are opportunities to minimise unintended gaps or overlaps and inconsistent and duplicative requirements.
- legal obligations and regulator expectations and practices will be readily available, easy to navigate, and clear and easy to understand.
- the AISA has scope to evolve in response to changing circumstances or new information on the regulatory system's performance.

## Section 4: Impact Analysis (Proposed approach)

The Identity Services AISA will facilitate improved service delivery and enable us to better meet customers' needs and improve their interactions with us. While some efficiencies are expected, these are not quantifiable at this point.

The development of AISAs is a complex and time-consuming process that typically takes about 12-18 months. The Identity Service AISA is being developed as part of the Te Ara Manaaki programme of work. The costs of developing the Identity Services AISA and the technology needed to deliver the new customer single view will be met through the Department's baseline budget, as specified in the TSSD (Te Ara Manaaki) Single Stage Business Case which was approved by Cabinet in July 2017 [SEC 17-MIN-0052 refers]. The implementation of the Identity Services AISA is not subject to a future budget bid. The ongoing costs of the Identity Services AISA will replace the operational costs currently incurred by the four IMAs that will be superseded by the AISA.

<b>Affected parties</b> <i>(identify)</i>	<b>Comment:</b> nature of cost or benefit (eg ongoing, one-off), evidence and assumption (eg compliance rates), risks	<b>Impact</b> <i>\$m present value, for monetised impacts; high, medium or low for non-monetised impacts</i>
--	---	---

Additional costs of proposed approach, compared to taking no action		
Regulated parties	Cost of the technology and process changes to implement the AISA will be met within departmental baselines (are happening anyway so not marginal costs)	Low
Regulators	Not applicable	
Wider government	Not applicable	
Other parties	Not applicable	
<b>Total Monetised Cost</b>	<i>Not applicable</i>	
<b>Non-monetised costs</b>	<i>Not applicable</i>	

Expected benefits of proposed approach, compared to taking no action		
Regulated parties	Reduced duplication, future proofing	
Regulators	One consolidated, there will be one agreement to review, rather than the four current IMAs.	
Wider government	Continued high trust in privacy protections and government services	
Other parties	Streamlined interactions with government services	
<b>Total Monetised Benefit</b>	<i>Not applicable</i>	
<b>Non-monetised benefits</b>	<i>Not applicable</i>	

## 4.2 What other impacts is the approach likely to have?

There is considerable work under way across government to improve collaboration and innovation as a sector. One current area of focus is enabling information sharing and reuse across government, removing barriers where possible and appropriate while retaining appropriate controls.

Parliament is currently considering the Privacy Bill which seeks to update New Zealand's current Privacy Act 1993. The proposed changes will better align New Zealand's privacy law with international developments, such as the 2013 OECD Privacy Guidelines and the European Union's General Data Protection Regulation. The Bill addresses two technical

problems that have been identified with AISAs. These changes will make it easier for an AISA to apply to a class of agencies, and allow specified Crown agents to lead an AISA's development. The Bill preserves existing Information Matching Agreements but, in the future, information sharing will be authorised using AISAs rather than IMAs.

While the Department is closely monitoring these connected areas of change, neither is considered to pose any risk to proceeding with the Identity Services AISA.

## Section 5: Stakeholder views

### 5.1 What do stakeholders think about the problem and the proposed solution?

#### Public Consultation

In April 2018, Cabinet approved public consultation on the draft Identity Services Approved Information Sharing Agreement [CAB-18-MIN-0116 refers]. The public consultation period was 6 April 2018 to 4 May 2018.

Along with the draft Agreement, a discussion document and a Privacy Impact Assessment were released providing more background information. Both documents were available on the Department's website <https://www.dia.govt.nz/Proposed-Changes-to-DIA-Information-Matching-Agreements>. Submissions could also be made by email or by post.

To encourage submissions, the discussion document and the website invited feedback on the following specific areas:

- 1) New uses for information sharing
- 2) When information will be shared
- 3) Range of personal information to be shared under the proposed Agreement
- 4) Proposed privacy protections.

In addition, targeted stakeholders were advised of the consultation and invited to encourage others to submit.

#### Submission

One submission was received via email. The submitter argued that the proposed AISA is unnecessary, and that it would move New Zealand towards the creation of an effective "virtual citizen register", thus challenging much of the fundamental intent of the Privacy Act 1993. The submitter expressed a view that consent should be gained for every customer transaction before a single customer view is created.

The Department has considered the submission, but considers that the costs and delays associated with inserting a consent step into every customer interaction would outweigh any benefit. The Department also considers that any perceived risk of creating a 'virtual citizen register' is adequately mitigated by the design of the single customer view function, which will not create any new permanent register of citizens.

#### Privacy Commissioner

In accordance with section 96O of the Privacy Act, the Department consulted with the Privacy Commissioner on the draft Agreement. The Privacy Commissioner expressed support for the Department's approach and provided the following comment on the previous Cabinet paper (April 2018):

*The Privacy Commissioner is pleased with the level and nature of engagement on the policy development of the proposed AISA. As a result of this consultation, the draft AISA and associated documents have been amended to better explain the policy rationale and to better align the proposed AISA with Privacy Act requirements. The Commissioner is particularly pleased to note that specific sensitive information relating to adoption and gender reassignment will be excluded from the AISA, so as*

*to protect the privacy of those individuals. The Commissioner is supportive of consultation on the proposed AISA, which he considers will replace outdated IMAs and improve transparency around DIA's internal sharing of personal information.*

### **Technical refinement of the draft AISA**

After the public consultation process concluded, the Department identified some minor changes that, if made, would ensure that the AISA was better aligned with the relevant legislation. In summary the changes that were made improved definitions, added references to relevant legislation and ensured that there was greater consistency in language throughout the document.

The revised draft, including technical amendments but not substantive changes to the core policy proposals, has been forwarded to the Office of the Privacy Commissioner for information.

### **Conclusions and Recommendations**

The Department considers an AISA to be the best vehicle to enable information sharing to support the Department's identity services. It would authorise the sharing of information in an efficient and more effective manner, and it would enable the Department to transform customer services through the creation of a single customer view function. This approach has received support from the Privacy Commissioner.

## **Section 6: Implementation and operation**

### **6.1 How will the new arrangements be given effect?**

Once the AISA comes into effect the four IMAs will be cancelled as they will have been superseded. This will ensure that there are no active overlapping information sharing agreements. The benefits of the AISA will be realised over time as Te Ara Manaaki delivers its rolling programme of service improvements to customers supported by improved technology and systems. The first opportunity to improve services on the basis of this AISA may be as early as late 2018.

The development and implementation of the Identity Services AISA will sit within the Department's transformation programme, Te Ara Manaaki. To support implementation, operational policies and procedures will be updated and training provided to staff working with personal information and with customers.

The changes that are introduced through this AISA are expected to enhance the quality and consistency of the information held by the Department. This will in turn enable more streamlined customer transactions and more effective detection and investigation of data anomalies, including suspected fraud.

The AISA will be made publicly available via the Department's website. The AISA will continue the existing internal information sharing and enable the information held by the Department to be used to create the customer single view in support of the objectives of the Te Ara Manaaki programme.

## **Section 7: Monitoring, evaluation and review**

### **7.1 How will the impact of the new arrangements be monitored?**

The Department is required to report on the operation of an AISA at times specified by the Privacy Commissioner. These reports are concerned with whether the agreement is meeting

its goals and operating as intended. The maximum requirements of the report are that it may cover the costs and benefits of sharing, difficulties experienced, audits undertaken, amendments and safeguards put in place, complaints received, number of individuals whose information has been shared, number of transactions that have occurred and number of adverse actions taken as a result. No new data would be collected for the purpose of this reporting.

AISAs are subject to regular review by the Privacy Commissioner. The Privacy Commissioner can review the operation of the agreement on their own initiative 12 months after the Order in Council approving the agreement has been made and at any time that the Commissioner considers appropriate for subsequent reviews.

Any review by the Privacy Commissioner could question whether the agreement is failing to meet its goal in facilitating public services, unreasonably infringing privacy, or operating in an unforeseen way. It could also cover whether the costs of sharing are outweighing the benefits. If there are reasonable grounds to believe any of these are occurring, the Privacy Commissioner will prepare a report for the Minister of Internal Affairs, which will also be tabled in Parliament.