Commercial & Legal in Confidence

Final
Date: 6 November 2012

Privacy Impact Assessment Report

Unique Student Identifier (USI)

Prepared for the Department of Industry, Innovation, Science, Research and Tertiary Education

6 November 2012

SalingerPrivacy

MinterEllison LAWYERS

25 NATIONAL CIRCUIT, FORREST ACT 2603, DX 5601 CANBERRA
TEL: +61 2 6225 3000 FAX: +61 2 6225 1000
www.minterellison.com

Privacy Impact Assessment Report - Unique Student Identifier Table of Contents

Executive Summary

On 13 April 2012, the Council of Australian Governments (**COAG**) agreed to a proposal to introduce and implement a system that would allocate each student undertaking accredited courses in the vocational education and training (**VET**) sector with a 'unique student identifier'. The purpose of the USI is to allow an individual's VET records to be collated and accessible over the course of the student's lifetime. The implementation of this COAG project has been a collaborative effort between all jurisdictions, including the Australian Government.

The benefit of the USI in improving access to education data for students (and at no cost to students) is a privacy positive outcome. In considering how to best achieve this objective the Australian Government and state and territory governments will need to ensure that unnecessary privacy intrusions are minimised so far as practicable, and that any remaining privacy impacts are proportionate to the level of risk and justified by the positive outcomes.

This Privacy Impact Assessment (**PIA**) has examined both the 'privacy positives' and the privacy risks arising from the implementation of the USI scheme to the VET sector, based on the information provided to us as on 3 October 2012, and the provisions of the *Privacy Act 1988* (Cth) as currently in force.

We note that a range of sensible privacy-positive design elements have been adopted by the Department of Industry, Innovation, Science, Research and Tertiary Education (**DIISRTE**) to date in developing the USI system, which have had the effect of either eliminating or mitigating actual or potential privacy risks. Further, at the time of preparing this report, DIISRTE (with the Office of the Parliamentary Counsel) was in the process of drafting legislation to support the implementation of the USI, and which is also intended to manage privacy risks through imposing limitations on the collection, use and disclosure of the USI.

Privacy positives

We found the following 'privacy positives' arising from the proposed USI scheme:

- **Improved access to personal information:** One of the key objectives of a USI is to improve the ability of students to access and compile their educational data over time, and over multiple RTOs.
- **No charge for transcripts:** Not charging students for transcripts ensures compliance with the Access principle, i.e. the provision of personal information to the individual concerned at no or minimal cost. It also minimises privacy risks relating to the additional storage of billing data which would need to be protected from misuse.
- **Access to demographic data:** The development of a protocol between the USI Agency and the NCVER to manually handle student requests for access to demographic data held by the NCVER promotes the Access principle.
- **Quarantining of data**: Holding a student's education data in one database and organisation (NCVER), and their identity and contact data in another database and agency (the USI Agency), is a sensible data security strategy.
- **Limitations on creation of USI:** The inclusion of provisions in the USI legislation which will effectively prohibit RTOs from requiring students undertaking non-accredited courses to obtain a USI will assist in managing community concerns regarding the scope of the USI scheme. It will also promote compliance by RTOs in relation to their Disclosure obligations, and by training authorities and the NCVER in relation to their collection limitation obligations.

- **No retention of EOI data:** The design decision that the USI Agency will not retain evidence of identity (EOI) data minimises risks in relation to fraud and the creation of 'identity stores'. It also minimises compliance risks in relation to the Data Quality principle, having regard to the fact that some identifiers such as driver licenses and passport numbers change over time and may therefore have limited utility in any case.
- **Limitations on RTO collection of EOI data:** The inclusion of provisions in the USI legislation prohibiting the retention of EOI information by RTOs, and publicising the fact that students can apply directly to the USI Agency for a USI through a student communications strategy, are sensible approaches to managing the risk of collection and storage of EOI data (or copies of the EOI itself) by RTOs. The communication strategy is also relevant to ensuring compliance with the Direct Collection and Collection Notice privacy principles by the USI Agency, the NCVER and RTOs.
- **Restrictions on use:** Privacy-positive design principles adopted include that there will be no combination of a student's education data (held by NCVER) and their identity/contact data (held by the USI Agency), except at the instigation of the student, or under specified and limited circumstances set out in the legislation.
- **No retention of transcript:** The design decision that the USI Agency will not retain a copy of the educational data for that student once the requested transaction has been performed is a sensible data security strategy.
- **Limits on disclosure of data on transcript:** Limiting identity data on authenticated VET transcripts issued by the USI Agency to the student's name – and not including the USI – will assist in minimising risks such as identity fraud and the adoption of the USI beyond the education sector.
- **Limits on disclosure of education data to RTO/training authority:** Privacy-positive design principles adopted include that an RTO/training authority will only be allowed to access or download a student's education data by demonstrating that they have the student's USI and that the student has consented.
- **Limitations on disclosure of personal identifying information:** The system design prevents an RTO from looking up a student's address or other personal details without the student's consent.
- **Evidence of consent:** Privacy-positive design principles adopted to date include that a student will demonstrate their consent to an RTO/training authority's request to access or download their education data by way of an online, revocable nomination of that RTO/training authority.
- **Logging USI account access:** Allowing students to request an audit log of user access will assist students in managing their permissions, and to identify unauthorised access.

Privacy risks

Although we found a number of privacy risks relating to this proposal, we also found that each risk can be addressed through a number of mitigation strategies relating to the USI legislation, communications, working with stakeholders, transparency, and system design. However, whether this assessment remains true depends on the final form of the USI legislation in relation to authorising collections, uses and disclosures.

The privacy risks arising from the proposal may be summarised as:

- The risk that RTOs do not understand their obligations in relation to the retention of EOI information, resulting in a risk of unnecessary retention of information, and possible fraudulent or other misuse.

- The risk that students do not understand the purposes for which their information may be collected, used and disclosed, and by whom.
- The risk that students do not understand how to set and manage access permissions, including in relation to the form of transcripts.
- The risk that the USI system is subject to unauthorised access or misuse.
- The risk that the USI Agency collects or uses unnecessary or out-of-date student contact details.

Our recommendations to address these privacy risks are as follows:

Communications

- That student communications about the various access control settings and the limits to those settings be made available to students in plain language and in multiple community languages. **(Recommendation 6)**
- That the communication strategy for the rollout of the USI make clear that the USI Agency will not share data with any other government agency, except as provided for under the access arrangements for RTOs and training authorities and in the other limited and specified circumstances set out in the legislation (eg. under the research exemption). **(Recommendation 14)**

Working with stakeholders

- That the USI legislation is supplemented with guidance for RTOs to clarify the circumstances in which the retention of EOI information is, and is not, permissible. **(Recommendation 1)**
- That the USI Taskforce liaise with the NCVER to develop one or more template privacy notices, to be included as part of the standard enrolment questions in the AVETMISS standard for 2014 release. **(Recommendation 3)**

  Note: The privacy notice should provide:

  - a succinct, plain language explanation of what data is sent by the RTO to the relevant training authority (if applicable), the USI Agency and the NCVER, and
  - clarity that the questions asked about disability, indigenous status and language spoken at home are optional, but that if answered they will be provided to the relevant training authority (if applicable) and the NCVER.
- Alternatively, or in addition to Recommendation 3, that the USI Taskforce (and the USI Agency once it comes into operation) encourage RTOs to adopt template privacy notices by way of guidance and other communication strategies as appropriate. **(Recommendation 4)**

System design

- That the USI Taskforce work with SMS vendors to seek a method by which data about students that is not required to be reported by RTOs to an STA or the NCVER (i.e. students undertaking non-accredited courses), is not sent by RTOs. **(Recommendation 2)**
- That the design of the USI system include a prompt (such as a screen prompt on next log-in) to students with delegated RTOs and training authorities to review their delegations and check the accuracy of their information. **(Recommendation 5)**
- That the final database design specifications not preclude the development of more complex business rules around mediated access in the future. **(Recommendation 7)**

- That students have available to them a 'preview' function which allows students to see how their record will appear to RTOs/STAs, depending on the information and access controls they set. **(Recommendation 8)**
- That the USI Taskforce commission an independent Threat and Risk Assessment of the design of the USI Register and USI system before it is finalised, to assess compliance with the 2012 *Information Security Manual* in terms of the information security classification (both at the unit level and at the aggregate level) and data security controls to be applied. **(Recommendation 9)**
- That the NCVER review their proposed data security arrangements for 2014 onwards, as against the 2012 *Information Security Manual*, given the enhanced nature of the data to be collected with the introduction of the USI. **(Recommendation 10)**
- That the primary student address field in the USI Register not be overridden by different addresses supplied by later RTOs when searching for a student's USI. **(Recommendation 11)**
- That the USI Agency's website / student portal be designed such that at the point the student contacts the USI Agency to request a 'web view' or authenticated transcript of their education history, or to set permissions for an RTO/training authorities to access their educational data, the system should first require the student to check and confirm or update their preferred contact details. **(Recommendation 12)**

Governance

- That the USI legislation contains appropriate provisions to:
  - provide appropriate restrictions on the collection, use and disclosure of the USI and related EOI data, as set out in sections 4.6.2(c) and 6.4.1 of this report;
  - authorise the provision of the USI by RTOs and training authorities to the NCVER (either directly or via a training authority) for reporting purposes (unless such disclosures and collections will instead be authorised under standards made under the *National Vocational Education and Training Regulator Act 2011* (Cth));
  - if necessary, authorise transborder disclosures which might not otherwise be allowed under existing privacy principles that are applicable to RTOs and/or STAs;
  - if necessary, authorise the use and disclosure of the USI and associated data by the USI Agency and/or the NCVER (but not RTOs or training authorities) for research purposes, subject to the tests set out in section 9.1(c) of this report; and
  - deliver a nationally consistent enforcement regime which provides individuals with remedies for any privacy breaches, as set out in section 4.6.2(c) of this report. **(Recommendation 15)**

Transparency

- That the USI Agency adopt and follow the Office of the Australian Information Commissioner's guidelines on voluntary notification of serious data security breaches. **(Recommendation 16)**
- That this PIA Report be provided to the Office of the Australian Information Commissioner, and the Privacy Commissioner (or equivalent) for each State and Territory. **(Recommendation 18)**
- That this PIA Report be published on the DIISRTE website with the Government's response, and on the USI Agency's website once the latter is operational. **(Recommendation 19)**

Further assessments

- That DIISRTE commit to undertaking further Privacy Impact Assessments, and public consultation, for each future stage (if any) in the rollout of the USI. **(Recommendation 13)**
- That this PIA Report be reviewed and updated when the draft USI legislation is finalised. **(Recommendation 17)**

Based on our understanding of what the USI legislation is intended to achieve, as described in this report, we do not consider any of the identified risks to be material in the sense that they either present an unacceptable privacy impact, or would require mitigation measures that would cause significant delay to the implementation of the USI scheme for the VET sector. However this assessment should be reviewed once the drafting of the USI legislation is finalised.

Paul McGinness
Partner, Minter Ellison

Anna Johnston
Director, Salinger Privacy

6 November 2012

Chapter 1 - About this report

1.1 The scope of this PIA

1.1.1 What is within scope

(a) The primary purpose of this report is to analyse the possible impacts on the privacy of VET students' personal information in the proposed Unique Student Identifier (**USI**) system by reference to Australian privacy laws (as at 31 August 2012) and to identify and recommend options for managing, minimising or eradicating any negative impacts.

(b) This report examines the privacy impacts of the USI initiative, in the stage of its development as at 11 September 2012, having regard to:

(i) the type, amount and scope of personal information to be collected, recorded, stored, used and disclosed;

(ii) the necessity for collecting the personal information;

(iii) the likely disclosure of, and regimes providing access to, personal information collected under the scheme;

(iv) the organisations that will receive and/or share the personal information collected;

(v) compliance with obligations with respect to privacy law; and

(vi) community values and expectations with respect to privacy.

1.1.2 What is not in scope for this PIA

This PIA report:

(a) is not an assessment of the adequacy of information security arrangements for the proposed USI system. While ensuring appropriate data security is a critical privacy principle, expert assessment of the adequacy of information security arrangements will be required as the project moves towards a more detailed, operational level of design;

(b) does not assess the proposed USI system with respect to compliance with the proposed Australian Privacy Principles (**APPs**). This assessment has focused on the existing state of privacy regulation in Australia; and

(c) does not assess privacy risks by reference to the proposed APPs.

1.2 How should this PIA be used?

(a) Chapters 5 to 11 contain findings and recommendations with respect to the privacy impacts of the USI initiative on students whose personal information will be collected, used and disclosed as a result.

(b) This PIA report provides:

(i) clarity as to the privacy obligations applying to the various organisations participating in the USI initiative;

(i) an assessment of the proposed controls and safeguards in the design and governance models for the proposed USI system;

(ii) identification of risk areas for the proposal in relation to both privacy compliance and community expectations; and

(iii) recommendations to address those risks by minimising privacy intrusions and maximising privacy protections within the design, legislation, policies and procedures, and governance model for the proposed USI system.

(c) This report is intended as a valuable resource for the USI Taskforce at DIISRTE, as well as other stakeholders, to assist in finalising plans for the development of the USI and design of associated systems.

(d) The PIA can also be used to further inform and educate those involved in, or affected by, the initiative as it is implemented – for example, in the design of guidelines, education materials, staff training, system design and program evaluation.

(e) We note that subject to Ministerial approval, DIISRTE intends to make this report publicly available.[1]

1.2.2 Methodology

(a) To produce this report we have examined the documents specified in Schedule 1. In relation to the drafting instructions for the USI legislation as at 22 June 2012, we note that following subsequent discussions between DIISRTE and the drafters, the legislative provisions will take a secrecy/confidentiality approach to prescribing the circumstances in which USIs may be collected, used or disclosed. The USI legislation is not intended to 'fill in the gaps' of privacy laws in relation to personal information generally. The drafting approach is discussed further in Chapter 4.

(b) We have also held discussions with personnel from the USI Taskforce, and from the National Centre for Vocational Education Research (**NCVER**).[2]

(c) We have not directly undertaken consultation with other stakeholders or interest groups, other than to consider the documents set out in Schedule 1.

1.3 The process of assessing privacy impacts

(a) Identifying privacy impacts and risks involves an examination of how the proposal will *'affect the choices individuals have regarding how information about them is handled, the potential degree of intrusiveness into the private lives of individuals, compliance with privacy law, and how the project fits into community expectations'*.[3]

(b) The proposal is outlined in Chapters 3 and 4, and then assessed in Chapters 5 to 10 at each point in the life cycle of the 'personal information', as it is likely to be handled by the USI Agency and other participants in the USI scheme. The assessment is made with respect to compliance with privacy laws, and whether the proposal can meet community expectations.

---

1 The Office of the Australian Information Commissioner recommends that PIA findings be made public – see Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, August 2006, p.17. The benefits of doing so include 'demonstrating to stakeholders that the handling of personal information in the project has been critically analysed with privacy in mind; an increase in community confidence in the initiative; making a consultation process about the project more effective by better informing stakeholders regarding its privacy and information handling aspects; (and) fostering collaboration and communication, internally and externally' – see Office of the Privacy Commissioner, *Managing Privacy Risk*, November 2004, Parts A-6 and C-21.

2 20-22 March 2012; 8 and 31 August 2012; 11 September 2012; 2 October 2012.

3 Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, August 2006, p.xxi.

(c) A number of recommendations work together, and some deal with more than one privacy principle. Chapter 12 also draws together our conclusions about the privacy impacts – both positive and negative – and risks of the USI proposal.

(d) As instructed by DIISRTE, this PIA Report does not provide an opinion on the severity or degree of significance of any particular privacy risk. In accordance with AS/NZS ISO 31000,[4] such rating of risk should:

(i) be considered in the context of specific objectives;

(ii) involve relevant informed project personnel;

(iii) assess the likelihood of the risk event arising and the consequences of the event arising by reference to the specified objectives; and

(iv) apply criteria that is consistent with DIISRTE's risk management methodology (assuming that is consistent with the best risk management practice).
In undertaking any such risk assessment, it should be made clear whether such risk rating is made on the basis that risk mitigation measures are adopted or not.

1.3.2 What are the privacy laws?

Privacy laws in Australia present a fractured and imperfect picture.[5] General information privacy laws that currently apply to the various parties to be involved in the USI proposal are outlined as follows:

(a) the proposed USI Agency will be an Australian Government agency regulated by the Information Privacy Principles (**Fed IPPs**) in the *Privacy Act 1988* (Cth);

(b) the National Centre for Vocational Education Research (**NCVER**), a corporation, is regulated by the National Privacy Principles (**NPPs**) in the *Privacy Act 1988* (Cth);

(c) private sector registered training organisations (**RTOs**) with an annual turnover of at least $3 million are regulated by the NPPs;

(d) smaller private sector RTOs will not be regulated at all, unless they are also health service providers;

(e) enterprise RTOs run by Australian Government agencies, such as the Department of Defence, are regulated by the Federal IPPs;[6]

(f) government RTOs, and State Training Authorities (**STAs**), in the Northern Territory, Queensland, NSW, ACT, Victoria and Tasmania would be regulated by their own State / Territory privacy laws; and

(g) government RTOs and STAs in South Australia[7] and Western Australia are not currently subject to privacy laws.

---

4 Risk management – Principles and Guidelines

5 For a comprehensive overview of the various laws applying across the nation, see the Victorian Privacy Commissioner's interactive map titled 'Privacy and related legislation in Australia', available at www.privacy.vic.gov.au under Relevant Laws > Privacy Laws.

6 In practice, some of those agencies may actually be exempt from the Fed IPPs because of their national security status. For example, ASIO, DSD and ASIS all have fairly broad exemptions from the IPPs under s.7 of the *Privacy Act 1988* (Cth).

7 Government RTOs and STAs that are 'public sector agencies' as defined under s.3(1) of the *Public Sector Management Act 1995* (SA) are required to comply with a set of Information Privacy Principles pursuant to an administrative instruction, *Cabinet Administrative Instruction 1/89, also known as the Information Privacy Principles (IPPs) Instruction, and Premier and Cabinet Circular 12, as amended by Cabinet 18 May 2009.*

1.3.3 Meeting community expectations

(a) PIAs respond to public concerns not only about strict compliance with privacy and related laws, but also about the wider implications of government and business initiatives that affect the level of surveillance and monitoring of individuals in society.

(b) Authorising and imposing limitations on the collection, use and disclosure of personal information pursuant legislation may ensure that a particular activity complies with the privacy laws, and with generally-accepted privacy principles. However, that does not mean it will necessarily meet 'community expectations'.

(c) The former Australian Privacy Commissioner Malcolm Crompton has noted that:

> *'consumers everywhere eventually reach a level of concern where they no longer accept a situation of low security and regular loss of privacy through inappropriate use and sharing of information, even if legal.*[8]

(d) It is beyond the scope of this PIA to commission comprehensive research on expectations or attitudes with respect to the USI initiative, and reliable indicators of community expectations are notoriously difficult to produce.

(e) However, there are several sources from which we can extrapolate conclusions about what community expectations most likely will be. These include:

(i) a student survey carried out as part of the preparation of the business case for this proposal;

(ii) written submissions made about this proposal, for example in response to the Regulatory Impact Statement (**RIS**) published December 2011;

(iii) quantitative research such as surveys reflecting Australians' attitudes and expectations with respect to privacy generally; and

(iv) qualitative research such as focus group-based discussions of privacy.

(f) Previous research indicates that the use of personal information by government can raise concerns amongst the public, for example in relation to data sharing,[9] and proposals which include:

(i) new ways of identifying individuals;

(ii) requirements for individuals to present identification in more circumstances;

(iii) the creation of significant databases;

(iv) the possibility of negative consequences for the individual;

(v) an increase in government surveillance powers; or

(vi) the possibility of function creep.[10]

---

[8] Malcolm Crompton, 'The Trust Cluster', December 2005, p.3; available from www.iispartners.com

[9] Focus group research conducted in 2002 for the Strategy Unit of the UK Cabinet Office, outlined in Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, at part 4:25.

[10] Office of the Privacy Commissioner, *Managing Privacy Risk*, November 2004, p.16.

(g) Research has also indicated that Australians in general place greater store in the protection of privacy compared to some other countries,[11] and that community expectations about what constitutes an invasion of privacy are not necessarily reflected in law.[12] Australians may be reluctant to divulge their personal information not necessarily from fear of their information being misused or causing personal threat, but rather because they consider such requests perceived to be an invasion of privacy.[13] Therefore the communication of clear and convincing arguments in support of new proposals and the management of privacy issues is important in managing community expectations and concerns about privacy.

1.3.4 Making recommendations

(a) A PIA should *'identify avoidable risks and suggest measures to remove them or reduce them to an appropriate level.'*[14]

(b) Recommendations should however seek to achieve a balance between the interests of the agency making the proposal, and the people affected by the proposal. Those recommendations which are most strongly urged are therefore those which can significantly improve privacy protection for the people affected, without significantly impacting on the achievements of the proposal's objectives.

1.4 Qualifications and Assumptions

This PIA Report is subject to the following qualifications and assumptions:

(a) the privacy issues have been considered in relation to current privacy laws, and not in relation to proposed changes to privacy regulation in Australia such as the Australian Privacy Principles;

(b) any documents not listed in Schedule 1 are not material to assessing the privacy impact of the USI initiative;

(c) Minter Ellison and Salinger Privacy have not undertaken any consultations or investigations other than those set out in the Methodology at paragraph 1.2.2;

(d) we have not considered any existing privacy policies, guidelines or manuals, directions, or other internal or administrative documents of the NCVER, or of any RTOs and STAs.

---

[11] Drs Milagros (Millie) Rivera Sanchez, Hichang Cho and Sun Sun Lim, from the Information and Communication Management Programme at the National University of Singapore, conducted the research, which was funded by NUS's Faculty of Arts and Social Sciences. The survey was carried out across five countries by AC Nielson in May 2003: Australia, Singapore, South Korea, the United States and India.

[12] Privacy NSW, Annual Report 2002-03, pp. 27-30.

[13] Roy Morgan Research, 'Community Attitudes Towards Privacy 2004', June 2004 prepared for the Office of the Federal Privacy Commissioner.

[14] Office of the Privacy Commissioner, *Managing Privacy Risk*, November 2004, p.17.

Chapter 2 – Privacy principles used in this assessment

2.1 Overview

(a) Privacy is a broader and more flexible concept than confidentiality. Personal information privacy generally refers to a person's ability to control how their personal information is handled (i.e. collected, stored, accessed, checked, used and disclosed) throughout the life cycle of that information. By contrast, confidentiality only places restrictions on the disclosure of information, but can include information other than 'personal information'.

(b) As the USI system will involve the USI Agency and other participants, a number of different privacy laws and privacy principles will apply in practice. This PIA Report refers primarily to the NPPs, and uses a plain language explanation of the scope or importance of each NPP (below) as the starting point for our analysis in Chapters 5 to 10.

2.2 Collection of personal information

2.2.1 Anonymity and pseudonymity

NPP 8 provides that wherever it is lawful and practicable in the circumstances, organisations must give consumers the clear option of interacting anonymously or by using a pseudonym.

2.2.2 Collection necessity

Any collection of personal information by organisations must be 'necessary for one or more of its functions or activities', according to NPP 1.1.

2.2.3 Collection methods – lawful, fair and not intrusive

NPP 1.2 requires organisations to collect personal information only by lawful and fair means, and not in any unreasonably intrusive way.

2.2.4 Collecting sensitive personal information

(a) NPP 10.1 requires the collection of 'sensitive personal information' to generally be with the subject's consent, as required by or under law, or in emergency situations where the subject cannot communicate their consent.

(b) What is defined by privacy law as 'sensitive' differs across jurisdictions within Australia,[15] but at its core is a recognition that health information (incorporating information about disability), and information about people's ethnicity, race or religion, are deserving of additional protection.

2.2.5 Direct collection

(a) NPP 1.4 provides that if it is reasonable and practicable to do so, an organisation must collect personal information about a consumer only from that consumer.

(b) This principle of direct collection is not only about the transparency of the process, but also about ensuring the accuracy of the information collected, by giving the affected person the opportunity to correct any incorrect information, or challenge requested information as irrelevant.

[15] For example, the Federal Privacy Act protects criminal records as 'sensitive', but NSW privacy law does not.

(c) Where direct collection is not possible, best practice is to ensure that the consumer has provided authorisation for their personal information to be collected via another party.

2.2.6 Collection transparency and choice (notification, options)

NPP 1.3 and 1.5 requires organisations, when collecting personal information about a consumer (whether from the consumer or from someone other than the consumer), to take such steps as are reasonable in the circumstances to ensure that the consumer is aware of various matters, including the purposes for which their personal information will be used or disclosed, whether the collection is voluntary, any consequences of not providing the information, and how the consumer might gain access to the information.

2.3 Data security

(a) NPP 4 requires organisations to take reasonable steps to protect the personal information they hold from misuse, loss, and unauthorised access, modification or disclosure.

(b) NPP 4.2 requires organisations to destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under NPP 2.

2.4 Access and correction

(a) NPP 6.1 requires organisations to provide consumers with access to their own personal information within a reasonable time, unless an exception applies.

(b) NPP 6.5 requires organisations to take reasonable steps to correct any personal information they hold to ensure it is accurate, complete, up-to-date, relevant and not misleading.

2.5 Data quality

(a) NPP 3 requires organisations to take reasonable steps to ensure that the personal information they collect, use or disclose is accurate, complete and up-to-date.

(b) The principle of data quality, or accuracy, has been described as 'the most important' of all privacy principles, its status reflected in the fact that, unlike limitations on collection, use and disclosure, non-compliance cannot be authorised by another law.[16]

2.6 Use and disclosure

2.6.1 Use and disclosure of personal information

(a) NPP 2 places limitations around the use or disclosure of personal information for purposes other than the purpose for which the information was collected in the first place.

(b) NPP 2.1(a)(i) sets tougher standards for the disclosure of sensitive personal information than for other categories of personal information; for example, secondary purpose disclosures must be 'directly related to the primary purpose of collection'. 'Sensitive' personal information is defined to include information about people's health, disability, ethnicity, race or religion.

[16] *Director General, Department of Education and Training v MT* (GD) [2005] NSWADTAP 77 at [37]

2.6.2 Use and disclosure of unique identifiers

(a) NPP 7 limits the collection and use of government-issued identifiers by private sector organisations.

(b) The Identifiers principle recognises the risk that the unique numbers found on government-issued identity documents, such as driver's licences and passports, could be used to track, link and match records about a person, and thus build up a profile of that person. The desire to prevent this situation occurring is not only for the protection of people's privacy, and in recognition of Australians' general opposition to the idea of national identity cards, but is also a sensible strategy in terms of tackling identity-based crime.[17]

2.6.3 Transborder disclosures

NPP 9 applies in addition to the normal limitations on disclosures.

[17] The National Identity Security Strategy for example recognises that a multiplicity of identifiers, rather than a single national identifier, presents a more robust system of protection against identity theft and fraud.

Chapter 3 – Background and purpose of the USI

3.1 Background to the proposal

(a) This PIA Report assesses the implementation of a USI for the VET sector across Australia.

(b) In 2009, the Council of Australian Governments (**COAG**) gave its in-principle support for the introduction, from 2012, of a national unique student identifier for the VET sector that is capable of being fully integrated with the entire education system.[18] COAG issued the following Communiqué:

> *'Improving data collections for all education sectors is of critical importance to Australia. A national student identifier could track students as they progress through education and training and would further support a seamless schooling, VET and higher education experience for students. It would also provide valuable data to facilitate a VET system that is more responsive and flexible.'*

(c) In 2010, COAG directed the Ministerial Council for Tertiary Education and Employment (**MCTEE**) to develop a business case for a USI for the VET sector. A preliminary business case was considered by COAG in February 2011. On 13 April 2012, COAG considered the final business case and agreed that implementation of the USI should proceed. On 13 April 2012, COAG approved the proposed USI framework and on 14 July 2012, policy approval for the preparation of Commonwealth legislation establishing the USI Agency as a statutory authority was given by the Prime Minister.

(d) The USI Taskforce, previously with the Department of Education, Employment and Workplace Relations (**DEEWR**) but now with DIISRTE, is responsible for the development of the USI.

(e) We note that the USI scheme is being designed in a way that will allow for its possible expansion beyond the VET sector, should governments decide to do so in the future.

3.2 Objectives of the USI

(a) In February 2011, COAG agreed on the stated purpose of the USI:

> *'to record all accredited education and training undertaken and qualifications achieved for each individual who accesses Vocational Education and Training (VET) over his or her lifetime.'*[19]

(b) The following overview of the purpose of the USI has been provided by DIISRTE:

> *'The NCVER currently collects and holds unit level records of student enrolment and achievement in the VET sector but these records are not mapped to an individual over their lifetime. Given this, the data are not able to be accessed by students themselves and are not able to be used to best effect by RTOs, government policy makers or researchers.*

[18] This could involve early childhood education.

[19] 'Final business case for a Vocational Education and Training Unique Student Identifier', September 2011, p8.

> *The purpose of the USI is to provide a linking key to enable individual students to extract a record of their training achievements from the National VET Collection held by NCVER. Each student undertaking accredited education and training post 1 January 2014 will require a USI. That student's USI will then be appended to the record of the training they have undertaken and qualifications they have achieved which is reported to the NCVER by their training provider.*[20]

(c) The objectives of the project are in line with the VET transparency agenda, which is part of a broader commitment by the Australian Government and COAG to achieve key reforms with respect to a skilled workforce.

(d) The introduction of the USI, by enabling an individual to track their vocational education and training attainments, is intended to deliver the following benefits:[21]

(i) *'the USI will enable students, for the first time, to obtain a comprehensive, authorised transcript of their training achievements from a single source'*;

(ii) *'the USI will enable governments, for the first time, to access a national database of unit-record level information about an individual's VET attainments over subsequent academic years, which is necessary for the equitable and efficient delivery of training entitlements'*; and

(iii) *'the USI will, for the first time, enable policy makers and regulators to access precise VET participation information both at-point-in-time and longitudinal'.*

(e) Of particular note from a privacy perspective will be the ability of a student to collate their training history, in a verifiable format, even beyond the life of the original training provider; and to provide access to that data to future RTOs when seeking credit transfer or access to entitlements-based funding.

3.3 Further background: existing regulation of the VET sector

(a) RTOs are providers of nationally recognised training, issuing nationally recognised qualifications. The providers of VET include technical and further education (**TAFE**) institutes, as well as private providers, community organisations, industry skills centres and commercial and enterprise training providers. In addition, some universities and schools provide VET.[22] It is estimated there are approximately 5,000 RTOs in Australia.[23]

(b) At the date of writing, only RTOs receiving public funding and state government-owned RTOs are required to report data to the relevant STA. This data is then provided to the NCVER. Some RTOs elect to provide data directly to the NCVER. However, there is currently a proposal being considered by governments to address the problems of partial VET activity reporting which may result in a broader collection of data.

(c) The Australian Vocational Education and Training Management Information Statistical Standard (**AVETMISS**) is the primary data reporting standard with which RTOs who are required to report must comply, although additional reporting may also be required by their relevant STA.

---

20 DIISRTE, 'Detailed Business Requirements' dated 20 April 2012, p.10-11.
21 DIISRTE, 'Detailed Business Requirements' dated 20 April 2012, p.11.
22 http://www.asqa.gov.au/about-vet/australias-vet-sector.html
23 Skills Australia, *Skills for Prosperity: A Roadmap for Vocational Education and Training*, 2011.

(d) National standards for RTOs, other than those RTOs operating solely in Victoria or Western Australia, are set by way of a legislative instrument, made by the relevant Commonwealth Minister, but as first agreed to by the Standing Council on Tertiary Education, Skills and Employment, under s.185 of the *National Vocational Education and Training Regulator Act 2011* (Cth). The standards include essential standards for initial registration and continuing registration (**SNRs**), and Data Provision Requirements (**DPR**).

(e) RTOs operating solely in Victoria or Western Australia are governed by similar standards made under the Australian Quality Training Framework (**AQTF**): the *Essential Conditions and Standards for Initial Registration*, and the *Essential Conditions and Standards for Continuing Registration*.

(f) The various standards and conditions of registration include the following of relevance from a privacy standpoint:

(i) SNR 6.4: *'The applicant has a defined strategy and process to manage records to ensure their accuracy and integrity.'* A similar requirement is a condition of continued registration; see SNR 17.4.

(ii) SNR 12.3: *'The applicant must retain client records of attainment of units of competency and qualifications for a period of 30 years.'* Also see SNR 23.3 in relation to on-going registration, and AQTF Condition 6.

(iii) DPR 4.1: *'Both applicants seeking initial registration under the Act, and NVR registered training organisations, must have a student records management system that has the capacity to provide the National VET Regulator with AVETMISS compliant data.'* See also AQTF Condition 6.

(iv) SNR 12.4: *'The applicant must identify how it will provide returns of its client records of attainment of units of competency and qualifications to the National VET Regulator on a regular basis, as determined by the National VET Regulator.'* Also see SNR 23.4 in relation to on-going registration, and AQTF Condition 6.

(v) SNR 12.5: *'The applicant must meet the requirements for implementation of a national unique student identifier.'* Also see SNR 23.5 in relation to on-going registration, and AQTF Condition 6.

Chapter 4 - Description of the USI System

4.1 Key features of the USI System

Key design features of the USI system are summarised as follows:

(a) national identifier - the USI is intended to be a unique, national student identifier, issued once in the lifetime of each student;

(b) compulsory participation – all students undertaking VET courses from 1 January 2014 will be required to obtain a USI;

(c) linking VET records – the USI will be the 'key' to enable a person to obtain a complete record of their VET training; and

(d) aligned with current privacy obligations – the USI Agency, the NCVER, RTOs, STAs and VET regulators will be subject to USI-specific legislation, which will prescribe specific circumstances in which the USI and in some circumstances the related personal information may be collected, used and disclosed; but these bodies will also continue to have the same responsibilities under existing privacy laws in relation to the privacy of information in the USI system as they currently do in relation to personal information from other sources.

4.2 An overview of privacy and security measures

A multi-layered approach is intended to surround the USI system, and we understand that it will include the following:

Design

- verification of the evidence of identity (EOI) documents presented by students;
- additional validation checks built into the system to minimise the risk of duplicate or compromised USIs;
- student controls over access to their data by RTOs and training authorities; and
- audit trails of access to data.

Security

- security testing, to be conducted both before and after the USI system begins operation.

Communications

- education and training of users of the USI system, including students and RTOs.

Legislation

- prohibition under the USI legislation on the collection, use and disclosure of the USI without student consent, except in specified circumstances (see section 4.6.2 below for further discussion).

4.3 Scope and reach

(a) There are an estimated three million VET students studying each year.[24] From 1 January 2014, it is proposed that all students studying nationally recognised vocational education and training under the Australian Qualifications Framework (**AQF**), including international students studying in Australia and those studying for Australian qualifications overseas, will be required to obtain a USI in order to receive a VET qualification or statement of attainment from their RTO.

(b) Compliance with this requirement will be most likely driven by the RTOs providing the training programs. Students may apply for a USI themselves (from October 2013 onwards), or they may ask their RTO or another authorised entity to apply on their behalf.

(c) The USI will be allocated to students by the proposed USI Agency. The USI Agency will hold certain identity and contact data about each student in the USI Register.

(d) Each RTO will need to record each student's USI in their student management system (**SMS**). At the end of each calendar year,[25] RTOs must report certain training and demographic data, as now, to their STA and/or directly to the NCVER[26]. From 2014, RTOs will be required to include the USI in their reports. An additional data field that RTOs applying for a USI on behalf of a student will be required to collect is 'city/town of birth'. RTOs will also need to allow for a 'middle name' field.[27] This will assist the USI Agency disambiguate students with the same or similar names and same date of birth.

(e) At the national level, students' identity and contact data will be held in one database by the USI Agency, while their educational and demographic data will be held in an entirely separate database by the NCVER. The only common data field between the two databases will be the student's USI.

(f) Students will be able to request that their USI be used as the 'key' to bring together their data from these two sources. They may wish to do so for a number of reasons, including:

  (i) to review the data held about themselves, including saving and printing the data themselves;

  (ii) to request an authenticated transcript or an extract of their educational achievements (as recorded since 2014) - for example, to show to a prospective employer, or

  (iii) to allow an RTO or STA to see their past educational achievements, so that the student may:

    (A) request a credit transfer;

    (B) demonstrate evidence of achievement of a prerequisite course; or

    (C) support an application for funded training under an entitlements model.

---

[24] 'Final business case for a Vocational Education and Training Unique Student Identifier', September 2011, p. 23.

[25] We understand that in the future the reporting period may be reduced to half-yearly or quarterly reports, but as at the date of writing it is in annual requirement.

[26] As at the date of writing, we understand that only state-owned RTOs and RTOs in receipt of public funding must report data and this occurs via their STA.

[27] The collection of middle names is already a state requirement in some jurisdictions (as advised by DIISRTE on 5 October 2012).

(g) In such a case, the student can either make a request to the USI Agency through the online portal for a complete VET records transcript or an extract, or they can consent to an RTO or STA to request an authenticated transcript directly by way of an express delegation through the USI system. Once the student's identity has been verified through the use of a password and user ID, or the RTO/STA's identity and delegation has been confirmed, the USI Agency will send an automated request to the NCVER for the educational data relevant to that USI.

(h) The educational data and the identity data for the student will then be combined by the USI Agency in a single-use 'web view' for the purpose of responding to the student's request (or the RTO or STA's request on their behalf). The student can also request a non-tamperable PDF or hard copy version of their transcript. We understand the current design intention is that the USI Agency will not retain a copy of the educational data for that student once the requested transaction has been performed.

(i) The 'flows' of personal information throughout this process is illustrated at Figure 1 below.

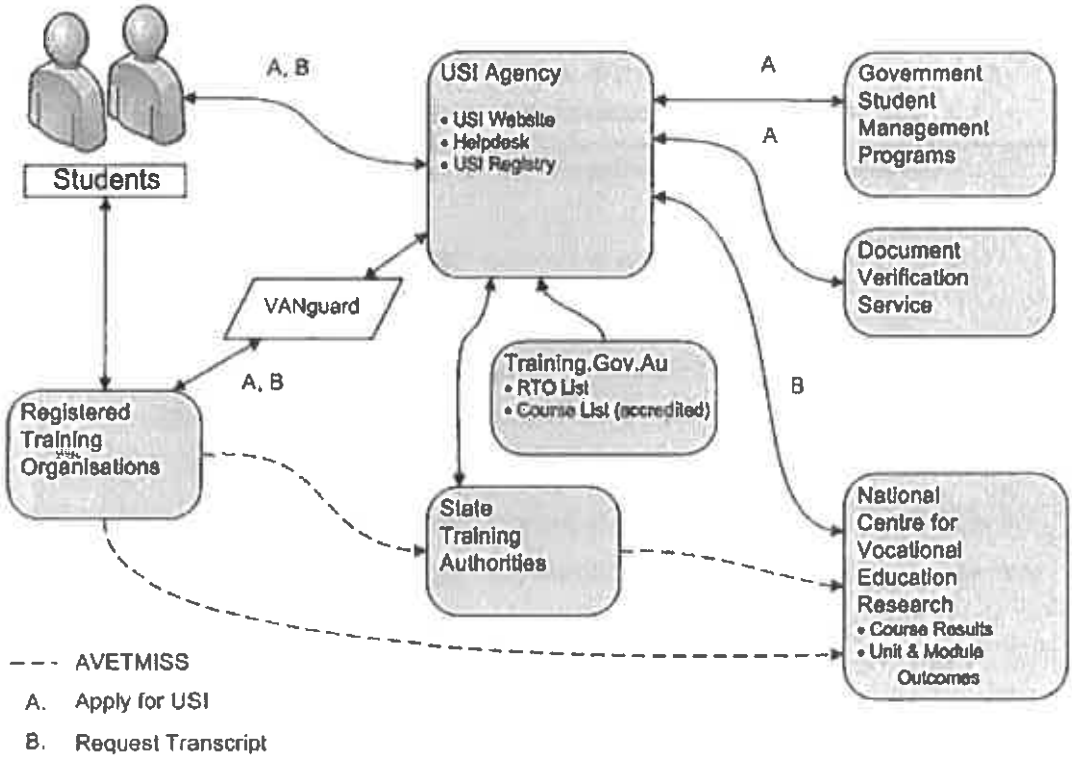

Figure 1: Illustration of information flows between parties involved in the operation of the USI[28]

[28] Diagram reproduced from the drafting instructions (version 2.3) for the *Unique Student Identifier Bill 2013* as at 22 June 2012.

4.4 Public expectations about a USI

(a) As part of the preparation of the business case on the USI, qualitative research was undertaken in 2011 to determine attitudes to the USI proposal amongst the various stakeholder groups, including students and RTOs. The research found that *'overall, stakeholders saw the USI as important and potentially valuable but not crucial'*.[29]

(b) Some stakeholders expressed *'doubts about the performance of government to effectively run a large-scale national identifier project through to completion'*, while *'concerns fell broadly into two categories: privacy protections and administrative/cost impacts for smaller RTOs.*[30]

(c) While students were described as 'generally supportive' of the proposal, the research report also noted that a *'caveat on this support relates to privacy and information and third party use issues'*.[31] In particular:

> *'there was significant concern among students that they would lose control of their information and would not be able to select (or restrict) the information viewed by others. This was especially important for students that may have had educational difficulties when they were younger and were now trying to improve their circumstances.*[32]

(d) A survey of 850 TAFE NSW students was also undertaken to assess student attitudes towards the USI. The results are summarised in Figure 2, below.

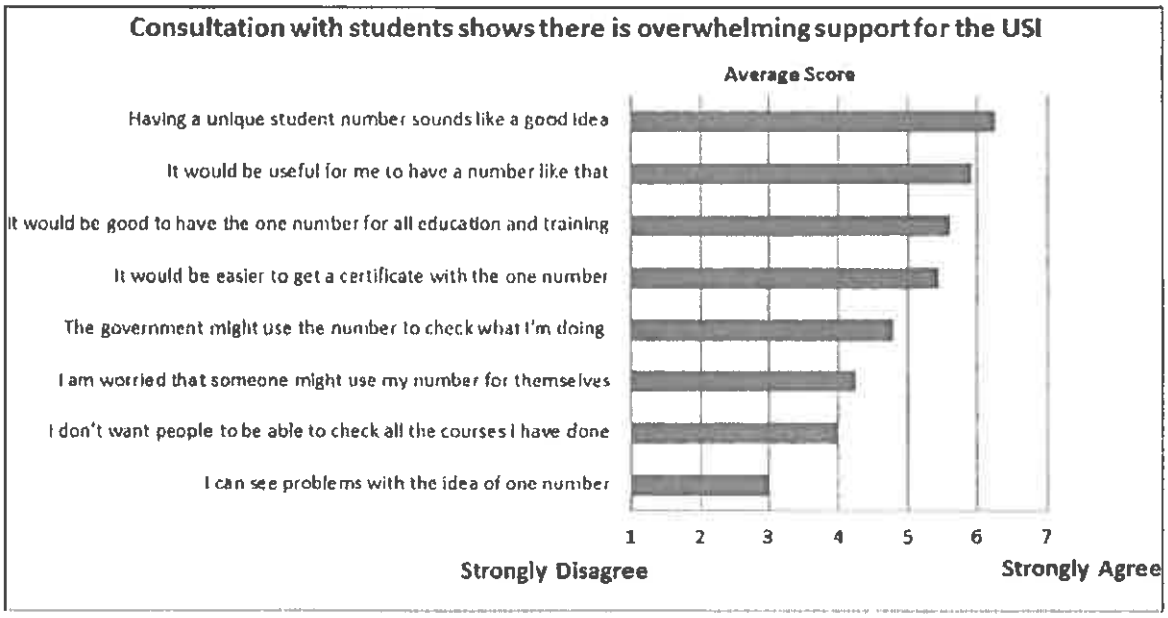

Figure 2: Results of student consultations about the proposed USI[33]

[29] The Nous Group, *Unique Student Identifier - Stakeholder Consultation Report*, July 2011, p.4.
[30] The Nous Group, *Unique Student Identifier - Stakeholder Consultation Report*, July 2011, p.4.
[31] The Nous Group, *Unique Student Identifier - Stakeholder Consultation Report*, July 2011, p.5.
[32] The Nous Group, *Unique Student Identifier - Stakeholder Consultation Report*, July 2011, p.9.
[33] 'Final business case for a Vocational Education and Training Unique Student Identifier', September 2011, p. 20.

4.5 The business case for the scheme

(a) The introduction of the USI is intended to deliver the following benefits:[34]

(i) *'the USI will enable students, for the first time, to obtain a comprehensive, authorised transcript of their training achievements from a single source'*;

(ii) *'the USI will enable governments, for the first time, to access a national database of unit-record level information about an individual's VET attainments over subsequent academic years, which is necessary for the equitable and efficient delivery of training entitlements'*; and

(iii) *'the USI will, for the first time, enable policy makers and regulators to access precise VET participation information both at-point-in-time and longitudinal'.*

(b) The Australian Privacy Commissioner has suggested that community concerns will likely be raised by proposals which include new ways of identifying individuals - such as unique identifiers - as well as the possibility of function creep.[35]

(c) The USI proposal contains both of these features. Given the possibility of expansion of the USI beyond the VET sector to other parts of the education system, a significant privacy risk faced by the USI proposal is a public questioning of the necessity and proportionality of the scheme.

(d) A submission from the Victorian Privacy Commissioner about the USI proposal puts the situation thus:

> *'It is important to remember, at the outset of any discussion of a proposed unique identifier, that identifiers are by their very nature, privacy invasive. Unique identifiers contain significant risks of 'function creep' - where incremental use of an unique identifier can lead to more personal information being gradually linked over time to that identifier. ...*
>
> *Additionally, there is a general public distrust of unique identifiers. This includes a perception that assigning numbers or identifiers to people dehumanises and reduces people to a 'number'. For those and other reasons, privacy legislation generally restricts the assignment, adoption, use and sharing of unique identifiers.'*[36]

(e) The submission goes on to question the necessity for the introduction of a USI:

> *'While unique identifiers may pose privacy challenges, that is not to say that they should not be introduced, but rather, that there needs to be extremely clear and convincing arguments for the necessity of their introduction. ... it is questionable whether the proposal is truly 'necessary' for the VET sector to operate efficiently or whether it would be merely administratively convenient.'*[37]

---

[34] DIISRTE, 'Detailed Business Requirements' dated 20 April 2012, p.11.

[35] Office of the Privacy Commissioner, *Managing Privacy Risk*, November 2004, p.16.

[36] Office of the Victorian Privacy Commissioner, *Submission to the Department of Industry, Innovation, Science, Research and Tertiary Education – Unique Student Identifier – Comments on the COAG Regulation Impact Statement*, 20 January 2012, p.2.

[37] Office of the Victorian Privacy Commissioner, *Submission to the Department of Industry, Innovation, Science, Research and Tertiary Education – Unique Student Identifier – Comments on the COAG Regulation Impact Statement*, 20 January 2012, p.3.

(f) The DIISRTE/DEEWR website refers to the following benefits of the USI:

> *'For the first time, every student who undertakes nationally recognised vocational education and training (VET) in Australia (or overseas from an Australian-registered provider) will be able to access his or her enrolment and achievement record from a single authoritative source.*
>
> ...
>
> *A record of enrolment and achievement across the lifetime of individual VET students will provide significant benefits for students, training providers and governments.*
>
> *For students, the initiative will make it easier to find, collate and authenticate their VET achievements into a single portable record. This will benefit students when undertaking further VET training, simplify the process of accessing credit for study previously undertaken, and allow them to provide a prospective employer with a single document that details all their VET achievements.*
>
> *Students can also give their provider online access to their VET records. For training providers, this may simplify credit transfer and help with verifying that a student has completed the pre-requisites for their course.*
>
> *For governments, de-identified information provided by the new initiative will improve the ability to analyse trends and identify future needs and areas for improvement in the VET sector. The initiative will also assist governments to manage their student entitlement programs.*
>
> *For researchers, de-identified data could be made available to create longitudinal datasets for research into students' pathways within VET.'*[38]

(g) The *Unique Student Identifier – COAG Consultation Regulation Impact Statement* (**RIS**) also provides a cost-benefit analysis of the introduction of the USI. Issues identified in the RIS as arising from the current inability to access enrolment and achievement data across the lifetime of individual VET students are as follows:[39]

(i) *'The data currently collected by the NCVER is not sufficient to support the student-centred (or entitlements based) training models that are being implemented in some states/territories. In addition, there is no way of knowing the extent to which individuals undertake VET with a number of providers over a given period.'*

(ii) *'In addition, the inability to access and analyse VET enrolment and achievement data at the individual student level over the lifetime means that state/territory and Commonwealth policy makers are restricted in being able to understand the pathways students are taking, in being able to assess the progress of disadvantaged students and in being able to assess whether individual students are accessing resources at agreed levels.'*

---

[38] See http://www.deewr.gov.au/Skills/Programs/USI/Pages/FAQ.aspx, site accessed 10 September 2012.

[39] *Unique Student Identifier – COAG Consultation Regulation Impact Statement* (December 2011), pgs 4-5. The RIS was cleared by the Office of Best Practice Regulation on 23 Mary 2012, and was available to COAG at its meeting on 13 April 2012 as part of the briefing accompanying the final business case.

(iii) *'Currently, longitudinal research databases for the VET sector can only be created through statistical matching. This limits the capacity of researchers to examine the distribution of educational opportunities and attainment across the population and analyse educational pathways over an individual's lifecycle.'*

(iv) *'The limitation in being able to readily access individual enrolment and achievement records over the lifetime is also a problem for RTOs, particularly at the time of student enrolment.'*

(h) We understand DIISRTE considers that the value of the USI compared to statistical (point in time) matching is that it would permit longitudinal (over time) analyses to support a flexible VET system that is more responsive to both student and labour market demand. In this regard, the RIS states that introducing the USI will:[40]

(i) *'lead to better data that can assist the identification of emerging issues in the VET sector in a more timely way for RTOs, employers and government. This will have a key long term benefit to underpin a more rapid response of the VET sector to changes in the economy thus making it more responsive to the needs of the labour market and the economy and make the workforce more readily adaptable to the changing skills needs of the future'*;

(ii) *'supporting reforms in the VET sector, including a more evidenced-based approach to policy and planning and the ability to create new student-centric innovations'*;

(iii) *'enabling greater transparency in the system and improving accountability and responsiveness across providers and governments'*, including enabling governments to better measure the effectiveness of their investment in the VET sector.

(i) We note that the RIS was open for consultation between December 2011 and January 2012.

(j) We recognise that it is ultimately a policy matter for the Australian Government as to whether the benefits of a USI will outweigh the privacy risks and the costs involved in its development and implementation. The measures to manage these risks are mainly centred around the Government's communications program.

(k) A number of stakeholder engagement activities have already been undertaken across Australia, and various communication strategies are being developed to increase awareness and understanding of the USI in terms of its rationale, benefits and operation.

(l) It is intended that the USI Agency, once operational, will establish and maintain regular communication channels with users of the USI system.

4.6 Governance of the USI Agency and the broader scheme

4.6.1 Governance of the USI Agency

(a) The USI Agency will be established under Commonwealth legislation as a statutory authority, headed by a Chief Executive Officer to be appointed by the Minister in consultation with SCOTESE.

[40] RIS, pgs 5, 12-13.

(b) The USI Agency will be a statutory agency for the purposes of the *Public Service Act 1999* (Cth), and a prescribed agency under the *Financial Management and Accountability Act 1997* (Cth).[41] It will sit within the DIISRTE portfolio.

(c) It is intended that the USI Agency will commence operations on 1 July 2013.

4.6.2 Governance of the broader scheme

(a) As noted above, in addition to establishing the USI and the USI Agency, the USI legislation will contain provisions prohibiting the collection, use and disclosure of the USI without student consent, except where it falls within one of the prescribed categories of permitted purposes for collection, use or disclosure. We understand that some provisions will be in a Bill, such as those relating to the USI Agency and a research exemption, while others will be set out in regulations, such as the more detailed provisions relating to use and disclosure by VET-related bodies (i.e. RTOs and STAs).[42]

(b) While the scope of the permitted purposes is still being considered by DIISRTE, we understand that these are likely to included purposes that are directly related to:

(i) managing the operations of national and state training systems;

(ii) managing a student's training information, including (but not limited to) –

(A) verifying a student's USI;

(B) providing for STAs to undertake their program management obligations;

(C) providing and managing AVETMISS compliant data;

(D) facilitating the transfer of a student's records from one RTO to another if the student chooses to undertake training elsewhere;

(E) conducting auditing and investigation functions;

(iii) participating in an investigation of a suspected compromised or duplicate USI, or where there is a suspicion of a USI that has been fraudulently obtained;

(iv) providing for the VET regulators to perform their functions as specified by the relevant legislation;[43] and

(v) facilitating VET sector policy development and research, by allowing the use and disclosure of the USI and other personal information held by the USI Agency and/or the NCVER for research purposes, in prescribed circumstances.[44]

(c) DIISRTE has also advised:[45]

(i) the use of the USI by STAs for determining a student's eligibility for funding entitlements will be authorised by that student's consent only, and not by the USI legislation;

(ii) the use and disclosure of the USI and education data by RTOs to the NCVER (and NCVER's corresponding collection of the USI and education data) for reporting purposes will be authorised by the USI Bill and regulations;[46]

---

41 Drafting instructions as at 22 June 2012, clause 5.3.1.1

42 Meeting with DIISRTE on 2 October 2012.

43 See *National Vocational Education and Training Regulator Act 2011* (Cth) and equivalent state and territory legislation.

44 Drafting instructions as at 22 June 2012, clause 5.4.1.1; comments provided by DIISRTE on 9 October 2012.

45 Meetings with DIISRTE on 11 September and 2 October 2012.

(iii) the use and disclosure of the USI and education data by STAs to the NCVER (and NCVER'S corresponding collection of the USI and education data) for reporting purposes will be authorised by the USI regulations;

(iv) the USI legislation will address the circumstances in which RTOs can retain EOI data, and for how long, with the intention being that RTOs should not retain EOI data at all if it is intended solely for USI purposes;

(v) a breach of the USI legislation will be deemed an 'interference with privacy' under the Commonwealth Privacy Act, which will trigger complaints handling and investigative powers of the Australian Information Commissioner to investigate the matter, even if the relevant organisation is not regulated by the NPPs or Federal IPPs.[47] This enforcement mechanism has the objective of providing a nationally consistent pathway for victims of any privacy breach to seek a remedy. The USI legislation itself will not impose penalties for breaches.

4.7 Features of the USI system for the purposes of this assessment

For the purposes of conducting this PIA, we see the USI system as containing a number of discrete features. Subsequent chapters of this report describe and analyse those features as follows:

(a) Chapter 5 reviews the processes for applying for a USI;

(b) Chapter 6 reviews the processes for reporting uses for the USI;

(c) Chapter 7 reviews the processes for viewing and updating a USI account;

(d) Chapter 8 reviews the processes for accessing VET training records;

(e) Chapter 9 reviews the processes for research activities; and

(f) Chapter 10 reviews plans in relation to data retention and data security.

[46] DIISRTE is obtaining advice from the states in relation to related transborder issues.

[47] A breach of the USI legislation may also constitute a breach of other legislation. DIISRTE has advised that it is discussing issues relation to enforcement and remedies with the Office of the Australian Information Commissioner.

Chapter 5 - Creation of a USI

5.1 Application procedure

5.1.1 An overview of the USI application channels

(a) An application for a USI can be made through the online portal by either:

(i) the student themselves;

(ii) an RTO on behalf of the student;

(iii) a VET admissions body on behalf of the student; or

(iv) any other entity on behalf of the student (such as their parent or guardian).

(b) The USI proposal is built on the policy position that VET students, regardless of their age (some VET students may be aged as young as 14), will have sufficient capacity to make decisions in relation to their personal information. However, a student may authorise a parent, guardian or any other entity to apply for a USI on their behalf.

(c) Where an application is made on behalf of a student, the authorised person will be required to confirm that they have the student's permission to provide the student's information to the USI Agency. The system will not record the details of the authorised person making the application.

(d) There is an inherent risk that a person may falsely claim to be applying for a USI on behalf of a student. It is not proposed that the USI legislation will provide offences in relation to unauthorised access to a student's USI account. Instead, the giving of false information to the USI Agency will be subject to an offence under section 137.1 of the *Criminal Code 1995* (Cth).[48]

5.1.2 Data collected by the USI Agency

(a) The personal information to be collected by the USI Agency from (or on behalf of) students in order to allocate their USI will be:

(i) identity data to ensure the uniqueness of the USI; and

(ii) contact data, to contact students as required.

(b) The identity data will include the following:

(i) first and family names;

(ii) middle name(s) (optional field);

(iii) previous name(s) (optional field);

(iv) gender;

(v) date of birth;

(vi) place of birth (city or town);

(vii) country of birth;

[48] As per discussions with the USI Taskforce on 8 and 31 August 2012. Section 137.1 of the *Criminal Code 1995* (Cth) provides an offence for knowingly providing false information to a Commonwealth entity, with a penalty of up to 12 months' imprisonment.

(viii) country in which the student is studying; and

(ix) evidence of identity (EOI) document type and details (e.g. drivers licence number and state of issue).

(c) Where possible, the data specifications for the relevant fields have been aligned with both the current and draft proposed (v7.0) AVETMISS requirements. However, the field for 'place of birth (city or town)' will be a new requirement, to be introduced for USI purposes only.

(d) The EOI information must be verifiable by the national Document Verification Service (**DVS**). The document 'type' will therefore be selected from a drop-down list. In the absence of this information, a USI can still be allocated if the student's identity is verified by the RTO (see further discussion at paragraph 5.1.3(d)).

(e) The contact data will include a postal address, email address, and home and mobile telephone number(s). These fields will be optional, however at least one form of contact data is required to be provided.

5.1.3 EOI procedures

(a) The USI system will link with the DVS in order to perform online, real-time checks of the EOI documents proffered by a student. The DVS checks that input details from EOI documents such as name, date of birth and document number match the details held for that document number by the issuing authority. The DVS system is available for checks against a wide range of documents, including common Australian EOI documents such as birth certificates, drivers licences and passports.

(b) The DVS is a check against forged or fake EOI documents. It has no ability to determine whether the person in possession of that EOI document is actually the person to whom the information relates.

(c) The DVS will be used by the USI Agency regardless of whether the student applies directly online for a USI, or through their RTO. Students will therefore be requested to provide one form of Australian EOI for verification.

(d) For students who cannot provide any EOI document that can be verified by the DVS (particularly offshore students studying offshore, students who are incarcerated and do not have access to EOI documents, and some students in remote areas without EOI documents), the RTO may be authorised by the CEO of the USI Agency to verify the identity of these students and a USI will be issued. The student can also contact the USI Agency directly for assistance.

(e) Initially, the name of the student to be recorded in the USI Register will need to match the name used on their EOI. Students will be able to update their personal details on the USI system to change their name or gender at a later date, on the basis of an EOI document which shows the new name or gender. Any transcript generated from that student's USI will show the last recorded name held in the USI Register at the time of the transcript request.

5.1.4 Establishing access controls

(a) If the student applies for a USI directly online, they will be asked to set a password and provide the answers to two check questions of their choice (such as 'mother's maiden name'), so as to streamline the student's future interactions with the USI Agency online in the event that they forget their password.

(b) Students will also be asked to nominate which RTO(s) and STA(s), if any, they authorise to access their educational records from the NCVER. The current design intention is that RTOs/STAs will not be able to view a student's personal and contact details without the student's consent. Students will be able to update or revoke these permissions online at any time.

(c) When a student applies for a USI through their RTO, the USI Agency will contact the student by text message, email or letter (depending on what contact information has been provided), giving them a link to the USI database. Once the student activates the link, they are given access to their USI account.

5.1.5 Personal information to be created by the USI Agency

(a) The USI will be randomly generated and will not follow any recognisable pattern. The design intention is that it will not be possible to identify a student, or glean any information about them, from their USI alone.

(b) The USI will comprise 10 characters, using nine randomly-assigned alphanumeric characters, and a tenth 'check' digit. The 'check' digit will help the USI system recognise whether the USI entered by a user (e.g. by an RTO entering a USI presented to them by a student, for the purpose of downloading the student's data) is a 'real' USI.

5.2 Application for USI by student

(a) When a student submits their personal identifying information online, the USI system will undertake internal checks to ensure all required data fields have been completed, and to ascertain the uniqueness of the student's information and identify any existing USI already allocated to the student. Once the internal checks are passed, the student's EOI document details are sent to DVS for verification.

(i) If the DVS does not verify the EOI document after three attempts, the student will be prompted to submit details of another EOI document.

(ii) If the EOI document is verified, the USI will be displayed on the screen. The student will activate their account by setting a password and selecting two security check questions from a drop down list. Activation is necessary for future access to the student's account and to be able to request transcripts.

(b) Activation is necessary for future access to the student's account and to be able to request transcripts.

(c) Offshore and other students who are unable to provide a DVS-verifiable EOI document can have their identity verified by an authorised RTO (see paragraph 5.1.3(d) above).

5.3 Application for USI by RTO

5.3.1 Application on behalf of student

(a) When an RTO collects information from a student to apply for a USI, they must have the student's permission to do so. We understand that the USI system will require RTOs to confirm (most likely by ticking a box on screen) that they have informed the student about the collection of their personal information.

(b) When the RTO accesses the USI portal, it will be redirected to the VANGuard User Authentication Service (UAS) webpage to verify the RTO's identity. VANGuard is a whole-of-government program delivered by DIISRTE, which enables businesses and government agencies to conduct secure online transactions. The VANGuard UAS will verify the RTO's digital credential (i.e. the RTO's registration number) to confirm the RTO's identity. This verification process operates in real time and will not involve the transmission of personal information.

(c) Following successful authentication by VANGuard, the USI system will then check training.gov.au to confirm that the RTO is currently operating. This verification process will also operate in real time and will not involve the transmission of personal information.

(d) Once the RTO's credentials are verified, a 'Conditions of Use' screen will be displayed. These conditions will include that the RTO:

(i) has the student's permission to collect and provide to the USI Agency the student's personal information; and

(ii) has the student's consent for the USI Agency to check the student's identity through the DVS.

(e) The RTO will be required to accept the conditions each time they log onto the USI system. If the RTO chooses not to accept these conditions, they are logged out and may not use any USI system functions.[49]

(f) If the student's data passes the internal and DVS checks (as described above), the USI will be displayed on the screen. The USI Agency will advise the student by email, SMS or post (depending on the contact data provided) of their USI and how to activate it.

5.3.2 Auto-population of data from SMS

(a) The USI system will be designed to provide for integration with RTO SMSs. This will enable personal identifying details and contact details held by the RTO in its SMS to be automatically uploaded into the relevant fields in the USI Register. It is noted that an RTO will require the student's permission to provide their details (whether collected for the first time on enrolment or already existing in a SMS) to the USI Agency.

5.3.3 Batched applications

(a) RTOs may wish to submit USI applications in batches where automated SMS applications support batch processing.

(b) The process for making batched USI applications is intended to work in a similar way to individual student applications as outlined above, but involving the sending of information to the USI Agency about a number of students at once.

---

[49] The making of false statements regarding student consent will be an offence under section 137 of the *Criminal Code 1995* (Cth).

(c) It is currently proposed that the USI Agency will not store whether permission was provided against each student record. Instead, the USI system will store user log-ons, and the RTO user ID that submitted the data to the USI Agency. Given that the RTO can only successfully submit student data if they have accepted the 'Conditions of Use' (which includes the condition that the RTO has the permission of the student(s) to provide their information to the USI Agency), this proposal provides no less privacy protection than having a specific flag indicating whether student permission was provided in each case. Therefore we have no recommendations to further mitigate risk in that regard.

(d) Batch processing may give rise to risks in relation to data accuracy, for example where the data relating to one student is entered into the USI Register against another student. DIISRTE has advised that internal validation check and quality assurance procedures within the USI Agency will be developed to minimise such risks. DIISRTE is also currently working with SMS vendors so that additional validation checks can be built into SMSs for integration with the USI system.

5.4 Application for USI by an authorised entity

(a) The USI proposal is built on the policy position that VET students, regardless of their age (some VET students may be aged as young as 14), will have sufficient capacity to make decisions in relation to their personal information. However, a student may authorise a parent, guardian or any other entity to apply for a USI on their behalf.

(b) Where an authorised person (such as a parent or guardian) applies for a USI on behalf of a student, they will access the portal and progress to a privacy screen. They will be required to indicate that they are making an application on behalf of a student and confirm as a 'Condition of Use' that they have the student's permission to provide the student's information to the USI Agency. The system will not record the details of the authorised person making the application.

(c) There is an inherent risk that a person may falsely claim to be applying for a USI on behalf of a student. It is not proposed that the USI legislation will provide offences in relation to unauthorised access to a student's USI account. Instead, the giving of false information to the USI Agency (eg falsely indicating that the student has authorised the person to apply for a USI on the student's behalf) will be subject to an offence under section 137.1 of the *Criminal Code 1995* (Cth).[50]

(d) Having regard to the practical difficulties in the USI Agency detecting and enforcing unauthorised applications for a USI,[51] as well as the limited value for any party in fraudulently having a USI allocated to another person, and weighing up the privacy positive in minimising the amount of personal information collected by the USI Agency, we have no recommendations in this regard.

---

[50] As per discussions with the USI Taskforce on 8 and 31 August 2012. Section 137.1 of the *Criminal Code 1995* (Cth) provides an offence for knowingly providing false information to a Commonwealth entity, with a penalty of up to 12 months' imprisonment.

[51] We note that an authorised entity can only access a student's USI account if the student has given them their password.

5.5 Analysis of application procedures

5.5.1 Anonymity and pseudonymity

(a) NPP 8 provides that where it is lawful and practicable in the circumstances, organisations must give individuals the clear option of dealing with the organisation anonymously or by using a pseudonym.

(b) The USI will act as a pseudonym in the data collected by the NCVER. In terms of that data collection alone, the use of a USI instead of a student's names is a privacy positive approach.

(c) However, in their interactions with their RTOs, students will – as now – be required to provide their full name and other identifying details. This is to be expected in a learning environment in which the student is working towards nationally recognised qualifications.

(d) We therefore have no recommendations in relation to this privacy principle.

5.5.2 Collection necessity

(a) In accordance with NPP 1.1, any collection of personal information by an organisation must be 'necessary for one or more of its functions or activities'.

(b) A number of design features adopted in the development of the USI proposal are aimed at minimising the collection of personal information about students, and in particular unnecessary personal information. For example, as the USI Agency only requires one form of communication with the student, the student has the option of only providing a mobile number, email address or postal address (although the student can chose to provide all contact details).

(c) In relation to identity management, all students will be required to provide details in relation to one EOI document (i.e. document type and number) which can be verified through the DVS before a USI is issued.

(d) Privacy risks are posed by any storage of students' EOI information, such as identity fraud by USI Agency staff, or threats from malicious external parties.

(e) The USI Register's interface with the DVS is being designed such that the student's EOI document type and EOI document identifier is validated in real time with a time-stamped receipt. Only the DVS receipt will be retained by the USI Agency, and a flag raised in the system to indicate that the student has passed the DVS check.

Privacy Positive

The non-retention of EOI data by the USI Agency minimises risks in relation to fraud and the creation of 'identity stores'. It also minimises compliance risks in relation to the Data Quality principle, having regard to the fact that some identifiers such as driver licences and passport numbers change over time and may therefore have limited utility in any case.

(f) For students who apply for their USI through their RTO, there is a residual risk that the RTO may store information about the EOI or retain a photocopy of the EOI document itself. This risk is proposed to be managed in the following ways:

(i) *Communication strategy:* Students will be given information on how to apply for their USI online, directly with the USI Agency, by way of a range of communication channels including media campaigns, USI Agency and STA websites, and printed material to be distributed by RTOs at training premises or during the enrolment process.[52]

(ii) *Legislative measures:* It is proposed that the USI legislation will include a provision requiring RTOs to destroy personal information collected, as soon as practicable after the USI application is made, unless the information can be retained for a permitted purpose other than obtaining a USI.

A breach of the USI legislation will be deemed an 'interference with privacy' under the Commonwealth Privacy Act, which will allow the Commonwealth Information Commissioner to investigate the matter.

Privacy Positive

The inclusion of provisions in the USI legislation requiring RTOs to destroy EOI information collected by RTOs, and encouraging students to apply directly to the USI Agency for a USI through a student communications strategy, are sensible approaches to managing the risk. The communication strategy is also relevant to ensuring compliance with the Direct Collection and Collection Notice privacy principles by the USI Agency, the NCVER and RTOs.

Recommendation 1

That the USI legislation is supplemented by guidance for RTOs to clarify the circumstances in which the retention of EOI information is, and is not, permissible.

(g) We understand that some RTOs report to their STA or the NCVER about all students, including those only enrolled in non-accredited courses. They do so because this is easier to manage from their student management systems (SMS), rather than only reporting data that is currently required under the funding agreement with the STA. With the implementation of the USI, there is a related risk that some RTOs may seek to require all of their students to obtain a USI, and not just those undertaking accredited VET courses. The allocation of USIs to students who do not require them could also raise community concerns about the expansion of the identifier scheme by stealth.

(h) We understand that while the USI legislation will not explicitly prohibit RTOs from requiring students undertaking non-accredited courses to obtain a USI or provide their existing USI to the RTO, such conduct will effectively be prohibited because it will not be one of the prescribed authorised purposes for the collection or use of the USI.[53]

[52] Information on how to apply for a USI through an RTO will also be included.
[53] Discussions with DIISRTE on 31 August, 11 September and 2 October 2012.

Privacy Positive

The inclusion of provisions in the USI legislation which effectively prohibit RTOs from requiring students undertaking non-accredited courses to obtain a USI will assist in managing community concerns regarding the scope of the USI scheme. It will also promote compliance by RTOs in relation to their Disclosure obligations, and by STAs and the NCVER in relation to their Collection Limitation obligations.

Recommendation 2

That the USI Taskforce work with SMS vendors to seek a method by which data about students that is not required to be reported by RTOs to a STA or the NCVER, is not sent by RTOs.

5.5.3 Collection methods – lawful, fair and not intrusive

(a) NPP 1.2 requires organisations to collect personal information only by lawful and fair means, and not in an unreasonably intrusive way.

(b) We have no cause for concern about the USI scheme's compliance with this principle, and therefore make no recommendations.

5.5.4 Collecting sensitive information

(a) NPP 10.1 requires the collection of 'sensitive personal information' to generally be with the subject's consent, as required by or under law, or in emergency situations where the subject cannot communicate their consent.

(b) While the NCVER collects demographic data about a student's disability, indigenous status, and language spoken at home, the design of the USI system interface between the NCVER and the USI Agency ensures that there will not be any disclosure of this sensitive personal information from the NCVER to the USI Agency. We therefore make no recommendations in relation to this principle.

Direct collection

NPP 1.4 provides that if it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

This principle of direct collection is not only about the transparency of the collection process, but also about ensuring the accuracy of the information collected, by giving the affected person the opportunity to correct any incorrect information, or challenge requested information as irrelevant.

Where direct collection is not possible, best practice is to ensure that the individual has provided authorisation for their personal information to be collected via another party. Given that the RTO can only successfully submit student data if they have accepted the 'Conditions of Use' (which includes the condition that the RTO has the permission of the student(s) to provide their information to the USI Agency), the system design offers the USI Agency some degree of assurance that the student has provided authorisation for the collection of their personal information.

The ability for students to apply for their USI online, directly with the USI Agency rather than via their RTO, will also address compliance with this privacy principle. We therefore make no further recommendations on this point.

Collection notice

NPP 1.3 and 1.5 require organisations, when collecting personal information about an individual (whether from the individual or from someone other than the individual), to take such steps as are reasonable in the circumstances to ensure that the individual is aware of various matters, including the purposes for which their personal information will be used or disclosed, whether the collection is voluntary, any consequences of not providing the information, and how the individual might gain access to the information.

The USI Agency and NCVER each have obligations to ensure students are informed about the collection of their data. However, for students applying for their USI via their RTO, the privacy notice will need to be provided by the RTO. In the absence of clear communications, students are unlikely to realise what information about themselves will be sent beyond their RTO. This indirect method of collection and notice poses a risk of non-compliance for the USI Agency and the NCVER.

The following strategies are aimed at assisting compliance with this privacy principle:

(i) *USI system design:* Where a student applies for a USI via the online portal, a privacy notice and user intention screen will be displayed, containing information about the collection of their data.

(ii) *Communication strategy:* As discussed above, students will be able to apply for their USI online, directly with the USI Agency. There will also be information on the USI Agency's website about how the USI will work, and what data is held by RTOs, STAs, the USI Agency and the NCVER.

Development of a template privacy notice for RTOs to use is also recommended. The AVETMISS includes a set of standard enrolment questions for RTOs to ask students; this would appear to be a logical place to include a template privacy notice for RTOs to adopt as well. It may be appropriate for there to be two different templates: one for publicly funded RTOs which send data through a STA, and the other for private RTOs which report directly to the NCVER.

Recommendation 3

That the USI Taskforce liaise with the NCVER to develop one or more template privacy notices, to be included as part of the standard enrolment questions in the AVETMISS standard for 2014 release.

Note: The privacy notice should provide:

- a succinct, plain language explanation of what data is sent by the RTO to the relevant STA (if applicable), the USI Agency and the NCVER, and
- clarity that the questions asked about disability, indigenous status and language spoken at home are optional, but that if answered they will be provided to the relevant STA (if applicable) and the NCVER.

Recommendation 4

Alternatively or in addition to Recommendation 3, that the USI Taskforce (and the USI Agency once it comes into operation) encourage RTOs to adopt template privacy notices by way of guidance and other communication strategies as appropriate.

Chapter 6 - Reporting and use of the USI

6.1 How the NCVER will collect information

(a) The NCVER currently collects data indirectly from publicly-funded and state government owned RTOs via their relevant STA, although some RTOs elect to provide data directly to the NCVER. A proposal to address issues relating to partial VET activity reporting is currently under consideration by Commonwealth, state and territory governments, which may result in a broader collection of data. The NCVER makes available data validation software for RTOs and STAs to use.

(b) The data collected by the NCVER includes demographic information about students, such as disability, indigenous status and language spoken at home, as well as educational achievement data. This includes subjects completed, subjects attempted but not completed, and qualifications issued.

(c) From 2014, the NCVER will also collect the USI of each student. The NCVER will use the USI for better analysis of the data they are collecting for policy analysis and research purposes. In the long term, the USI will enable accurate mapping of total education and training pathways over an individual's life if COAG decides to expand its use beyond the VET sector in the future.

(d) The RTO will remain the official issuer of the qualification.

(e) Currently, publicly-funded RTOs include students' names in their reports to their relevant STA. STAs validate and compile all the data for their State or Territory, and forward most of it on to the NCVER. However, some data, such as student address, is stripped out before being reported to the NCVER. Students' names are encrypted before being sent to the NCVER, using an algorithm which provides NCVER with some degree of confidence about the uniqueness of each record, without being able to 'reverse engineer' the data to determine the student's actual name. From 2014 onwards, the USI will make this process redundant, and the students' names could potentially be stripped entirely from the datasets to be sent from the STAs to the NCVER.

(f) We understand that the NCVER is moving to make the data reporting process web-based, using secure socket layer (**SSL**) technology for receiving uploads of data from RTOs and STAs.

6.2 How the USI Agency will use the information

(a) The USI Agency will house the USI Register. Identity data and contact data for each student will be included in the USI Register, as well as information about each student's delegations in relation to access to their data by RTOs and STAs, and security check questions and answers.

(b) Business processes are being developed to manage duplicate and compromised USIs, including the ability to transfer educational records from one USI to another, and to deactivate and archive any 'wrong' USIs. We understand that in the event of uncertainty about whether or not a 'new' student already has a USI (for example in the case of a partial name match), the system will be designed to provide for the issue to be resolved before a USI is created or returned, rather than risk compromising an existing USI by potentially linking two different students' data together.

The USI Agency will notify the relevant student(s) of the outcome of its investigation into potential duplicate or compromised USIs. If a duplicate or compromised USI is identified, the USI Agency will also notify the relevant RTOs and training authorities.

(c) As noted above, the USI Agency will not hold any educational or demographic data about students. At a student's request, educational data (but not demographic data) will be pulled down from the NCVER, using the USI as the 'key', and combined with some of the identity data for the student in a single-use 'web view' of PDF document for the purpose of responding to the student's request, such as for an authenticated transcript. The student can also request a paper copy transcript.

(d) The USI Agency will not retain a copy of the educational data for that student once the requested transaction has been performed. The USI Register's audit log will show that an authenticated transcript or extract was issued on a particular date for a certain USI, but not what its contents were.

6.3 How the USI Agency will disclose information

(a) The current design intention is that the USI Agency will only provide data to students themselves, to RTOs, STAs and authorised persons with the student's permission, or to approved researchers.

(b) As noted above, a student may wish to allow an RTO or STA to see their past educational achievements, so that the student may:

(i) request a credit transfer;

(ii) demonstrate evidence of achievement of a prerequisite course; or

(iii) apply for funded training under an entitlements model.

(c) The USI system will enable students to set and revoke permissions for RTOs and STAs to access VET records held by the NCVER and linked via their USI, and to therefore limit the types of information that will be disclosed in transcripts and extracts.

(d) These processes are analysed further in Chapters 5 to 8.

6.4 How other organisations will use and disclose the USI

6.4.1 RTOs

(a) As noted above, the USI legislation will contain provisions to prohibit the use of the USI except for specified purposes. It is intended that the specified purposes will not include (and therefore will effectively prohibit) an RTO from:

(i) printing the USI on a student card, parking permits, library cards or other identity documents;[55] and

(ii) requiring students undertaking non-accredited courses to obtain a USI or provide their existing USI.[56]

[55] The USI Bill will also prohibit any entity from using the USI as that entity's identifier (as advised by DIISRTE on 2 October 2012).

[56] Drafting instructions as at 22 June 2012, clause 5.4.1.1.

6.4.2 STAs

(a) Given the inclusion of the USI in AVETMISS 7.0, publicly funded RTOs will be disclosing the USI to their relevant STAs, who may use the USI for their own purposes such as the management of the programs they fund through the RTOs. As happens with the data currently collected, STAs are expected to use the USI to assist in the process of analysing statistics to make funding, planning and policy decisions, and providing aggregate information to RTOs and employers about their students and apprentices.

(b) From the point of view of how the addition of a USI will impact on students' privacy, it must be noted that the State and Territory governments already receive a combination of educational, identity and contact data about each student, including their full name and address. While the USI will bring benefits to those State and Territory governments in terms of higher degrees of surety about the data they are collecting, it is not expected to have any net impact on students' privacy.

(c) One minor change expected to be brought about with the introduction of the USI is that State governments will be able to implement their entitlements-based funding programs on the basis of individual students' past educational achievements in any State or Territory, not just their own. This will improve the integrity of a national student-centred training model.

Chapter 7 – Accessing USI Accounts

7.1 USI account access channels

(a) Once a USI has been created and the account activated, a student's USI account can be accessed, and personal details updated, by:

(i) the student; or

(ii) an RTO authorised by the student.

(b) A student can access their USI account by:

(i) first, entering either their USI or identity information; and

(ii) secondly, their password.

(c) Students will be able to view their personal details, and view their account audit log.

Privacy Positive

Allowing students to view an audit log of user access will assist students in managing their permissions, and to identify unauthorised access.

(d) Most personal details will be able to be updated (subject to passing validity checks).[57] In the case of name and gender changes, details of an EOI document which contains the proposed new name or gender of the student will need to be provided for DVS verification. As noted in Chapter 5, EOI information will not be retained by the USI Agency.

(e) Where a student's name is updated, the existing name will move to the 'previous names' field.

7.2 Access by RTOs

7.2.1 Permissions

(a) Access to a student's USI account and VET records will be moderated by a series of access permissions or 'delegations' by the student. For each student's account, the USI Register will maintain:

(i) a list of permissions setting out those RTOs and STAs that are authorised to access the student's USI account and request VET training records; and

(ii) control settings to enable the student to specify the information which may be provided to the RTO or STA in a transcript.

(b) Students can for example set permissions to allow their RTO to access and amend some of their personal information, such as their contact details. In this way, a student may update the address held by the USI Agency, via their RTO.

(c) Students can revoke permissions at any time through their USI account.

[57] DIISRTE has advised that contact details will be able to be updated.

Privacy Positive

Evidence of consent: Privacy-positive design principles adopted to date include that a student will demonstrate their consent to an RTO/STA's request to access or download their education data by way of an online, revocable nomination of that RTO/STA.

(d) We understand that appropriate information and support will be made available to students to exercise proper decision-making and determine consent with regard to the controls described above.

(e) The current design allows a student to delegate multiple RTOs and STAs, with no set time period for their delegation. There is a risk that students will 'set and forget' who can access their USI account. Although this is a risk created by students themselves, the design of the system could potentially assist consumers to protect their own privacy, for example with reminders on each log in.

Recommendation 5

That the design of the USI system include a prompt (such as a screen prompt on each log in) to students with delegated RTOs and STAs to review their delegations and check the accuracy of their information.

(f) While the settings and mechanisms proposed to be made available to students for limiting access offers a privacy positive, there is also a risk inherent in the design complexity, such that students may not understand their own settings and how to manage access permissions.

Recommendation 6

That student communications about the various access control settings and the limits to those settings be made available to students in plain language and in multiple community languages.

7.2.2 Viewable details

While RTOs will be able to submit updated personal details with the student's permission, it is proposed that RTOs will not be able to view the student's existing personal identifying information or contact information in the USI account.

Privacy Positive

The system design prevents an RTO user from looking up a student's address or other details without the student's consent.

7.3 Future-proofing the system

(a) VET students can be as young as 14 years of age. A policy position has been taken that if a student has sufficient capacity to be undertaking VET training (or contemplating taking more training or seeking employment based on their qualifications), they have enough capacity to seek access to their personal information or request educational transcripts without parent/guardian involvement.

(b) However, it should be recognised that this policy position will not hold true if a decision is made in the future to expand the USI scheme beyond the VET sector, for example into the early childhood and primary education sectors. Database design decisions taken now should not preclude the development of more complex business rules around mediated access in the future.

Recommendation 7

That the final database design specifications not preclude the development of more complex business rules around mediated access in the future.

Chapter 8 – Accessing VET training records

8.1 Obtaining VET training record transcripts

(a) A significant privacy positive of the USI scheme is that it will improve students' ability to access their own educational data.

Privacy Positive

Improved access to personal information: One of the key objectives of a USI is to improve the ability of students to access and compile their educational data over time, and over multiple RTOs.

(b) We understand that authenticated transcripts are likely to be printed on special watermarked paper and signed by an authorised officer of the USI Agency, so that employers, RTOs and STAs have some degree of assurance about the document being presented to them. Students will be entitled to request two hard copy authenticated transcripts per year free of charge. Students can request an unlimited number of 'web view' records and extracts which a student can save or print to their own computer, and at no cost.[58]

Privacy Positive

Not charging students for transcripts ensures compliance with the Access principle, i.e. the provision of personal information to the individual concerned at no or minimal cost. It also minimises privacy risks relating to the additional storage of billing data which would need to be protected from misuse.

8.1.2 Forms of access

(a) VET training records will be able to be obtained in the following formats:

(i) *a hard copy authenticated transcript issued by the USI Agency* – this can either be a full transcript or an extract;

(ii) *a non-tamperable PDF* – this can either be a full transcript or an extract; or

(iii) *'web*-based *view'* – this will contain all of the educational data and funding source information. It will be a full transcript.

8.2 RTO/STA access to transcripts

(a) Central to the USI system is the concept of personal control. With the exception of actions taken under the terms of a prescribed research exemption (see further in Chapter 9 below), there will be no combination of a student's education data (held by NCVER) and their identity/contact data (held by the USI Agency), except at the instigation of the student.[59]

[58] We note that the 'web-view' records and extracts which are saved or printed by students at no cost will not be authenticated versions.

[59] We note that such combined data is currently held at the RTO and STA level.

Further, an RTO or STA will only be able to request a transcript if permission has been granted by the student by way of delegation through their USI account. The main purpose for which a student may give an STA access to a transcript would be to enable the STA to assess a funding entitlement in response to an application or query from a student.

(b) Students may set and manage controls that will give general or limited access, as follows:

(i) *Choose who may see a transcript*: Students can select which RTO or STA can see any data at all; and/or

(ii) *Choose which information is contained in an extract of a transcript:* Students can limit what information a particular RTO or STA can obtain from the student's educational records, either in the form of a complete transcript or transcript extract (both of which are authenticated, although an extract will be clearly marked as such). For example, a student can suppress certain subjects that were not completed or undertaken with a particular RTO from being included in an extract.

(iii) Transcripts and extracts may take the following forms:

(A) a hard copy, signed document requested by, and only provided directly to, the student, which includes VET activity excluding funding source information;[60]

(B) an electronic, web-based view or PDF to be used by an STA or RTO with the student's consent for the purposes of establishing eligibility to participate in a government funded subsidy program which will include all of the student's educational information and funding source for any previous studies; and

(C) an electronic, web-based view or PDF used by STAs or RTOs with the student's consent for purposes such as establishing credit transfer, and will include either all of the student's educational information or an extract of the student's educational information.

(c) Students may also avail themselves of other means by which to protect and enforce their privacy rights, including:

(i) *View an activity history for their USI account:* As noted above, the USI system will provide an audit trail which will be viewable by students so they can see a history of actions, and any access by RTOs or STAs to their USI account; and

(ii) *Make enquiries and complaints:* Students may make enquiries and complaints in relation to the management of information in their USI account and the USI system to the USI Agency in the first instance, or to the Australian Privacy Commissioner otherwise.

Privacy Positive

Restrictions on use: Privacy-positive design principles adopted include that there will be no combination of a student's education data (held by NCVER) and their identity/contact data (held by the USI Agency), except at the instigation of the student, or under the terms of the research exemption.

[60] The hard copy authenticated transcript will be sent by the USI Agency directly to the student. The student can choose whether to provide the hard copy transcript to an RTO/STA.

Privacy Positive

Limits on disclosure: Privacy-positive design principles adopted include that an RTO/STA will only be allowed to access or download a student's education data by demonstrating that they have the student's USI and that the student has consented.

Privacy Positive

The flexible set of additional access controls available to the student in relation to RTO/STA access to educational data is a privacy positive aspect of the system design. Students can choose how much information they want an RTO or STA to see on their educational transcript/extract.

(d) As discussed in Chapter 7, there is a risk that students may not understand their own settings and how to manage access permissions. We recommend including a 'preview' tool which will allow students to see what their educational record will look like to the RTO or STA in question. Implementing a preview tool may be a simpler and more practical way of communicating to students how they can limit access to information than lengthy written explanations.

Recommendation 8

That students have available to them a 'preview' function which allows students to see how their record will appear to RTOs/STAs, depending on the information and access controls they set.

Chapter 9 - Research uses

9.1 External researchers

(a) One of the public benefits expected to arise from the implementation of a USI is improved quality of data for use in research contexts. The USI offers a higher degree of data integrity in terms of disambiguating unit-level student records, while protecting privacy by not directly identifying students. However, the inclusion of the USI in any datasets provided to external researchers does pose some risk of identification of individuals from the data, if the researcher has access to other information including the USI linking key.

(b) We consider best practice is to ensure that once the USI has served its purpose as a unique identifier and as a linking key, it should not be included in the datasets provided to external researchers. It is anticipated that in most cases involving access to data by external researchers, the USI will be stripped out prior to providing access. However, there may be cases where it is required by, or desirable for, external researchers to use the USI for initial data matching purposes, and then later strip out for the analysis of de-identified data.

(c) It is proposed that the USI legislation will provide for the USI Agency to disclose students' personal information and/or their USI for research purposes, subject to the following restrictions:[61]

(i) the student will have been previously informed that such a use of the USI and their personal information may occur in a privacy notice;

(ii) the use or disclosure of the information is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest;

(iii) either --

(A) that purpose cannot be served by the use of de-identified information, and it is impracticable for the organisation to seek the consent of the student for the use; or

(B) reasonable steps are taken to de-identify the information;

(iv) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication;

(v) the proposed use or disclosure has been approved by a Human Research Ethics Committee, constituted and functioning in accordance with the *National Health and Medical Research Council Act 1992* (Cth), on the basis that the public interest in the research or the compilation or analysis of statistics substantially outweighs the public interest in the protection of privacy;

(vi) the proposed use or disclosure has been approved by a committee comprising of a USI Agency representative and other members agreed by SCOTESE; and

(vii) the researcher will sign a declaration that the USI and related training information will only be used for the declared research purpose.

[61] Drafting instructions as at 22 June 2012, clause 5.6.1.

(d) The USI legislation will also provide for the USI Agency and NCVER to disclose a combined set of a student's personal identifying information held in the USI Register and national VET provider collection held by the NCVER for research purposes, subject to the same restrictions set out above.[62]

(e) It is not intended that the USI Agency will collect up to date contact details for students, therefore it is unlikely that it would be approached by researchers seeking to contact students to participate in surveys or other forms of research. Any disclosure of student contact details for research purposes would only be in accordance with the prescribed process.

9.2 Student access to NCVER data

(a) To date, the NCVER has been unable to make any link between a particular individual and the data they hold. As noted in Chapter 6, the introduction of the USI from 2014 will assist the NCVER to provide higher degrees of surety about the data collected for policy analysis and research purposes. The USI will also enable the NCVER to extract relevant demographic data on request from a student.

(b) However, the NCVER will be unable, on its own, to verify that the student seeking access to certain data is the student associated with the relevant USI. The USI Agency will therefore need to assist the NCVER in terms of identity verification for any such access requests. We do not anticipate that such access requests would be made very often, and therefore there is no need to establish an automated feed of demographic data to the USI Agency.

(c) It is intended that a protocol between the USI Agency and the NCVER will be developed for manually handling any requests from students or access to the demographic data held by the NCVER. DIISRTE has advised that it is currently discussing this with the NCVER.

Privacy Positive

The development of a protocol between the USI Agency and the NCVER to manually handle student requests for access to demographic data held by the NCVER promotes the Access principle.

[62] Drafting instructions as at 22 June 2012, clause 5.6.2.

Chapter 10 - Data security and quality

10.1 Data retention

(a) The current design intention is that once verified through the DVS, the EOI document number will be deleted and a flag will be set to indicate the document has been verified.

(b) We also understand that the intention is that personal information must be de-identified before the data in the USI Register production environment can be copied to any quality assurance, pre-production, test or development environment.

(c) These are both privacy-positive approaches to data retention.

(d) Data held within the USI Register will therefore be retained for 110 years from the student's date of birth. We understand that DIISRTE intends to develop a data archiving plan to describe what data will be archived, when data will be moved to the archive, how that data can be located and how archived data can be used in business processes.

10.2 Data security

(a) NPP 4 requires organisations to take reasonable steps to protect the personal information they hold from misuse or loss, and unauthorised access, modification or disclosure.

(b) Logical separation of data, in which different datasets are held in the one computer system but access to each dataset is controlled separately, is one way to manage data security. However, the mechanisms used to protect data that has been only 'logically' separated can be subverted in a number of ways, such as by malware or a database administrator with 'super user' privileges overriding the access control list.

(c) Physical separation of data, which is what is proposed for the implementation of the USI, offers greater comfort from a data security perspective - although of course no method is risk-free.

Privacy Positive

Quarantining of data: Holding a student's education data in one database and organisation (NCVER), and their identity and contact data in another database and agency (the USI Agency), is a sensible data security strategy.

(d) As noted in Chapter 6, at a student's request, educational data will be pulled down from the NCVER, using the USI as the 'key', and combined with some of the identity and contact data from the USI Register in a single-use 'web view', but not retained beyond the life of that transaction. This method of maintaining the 'quarantining' of educational data from identity and contact data is a sound strategy in terms of minimising misuse or loss of the data.

Privacy Positive

No retention of transcript: The design decision that the USI Agency will not retain a copy of the educational data for that student once the requested transaction has been performed is a sensible data security strategy.

(e) In order to disambiguate students from each other, the USI Register will hold various pieces of data about students, such as their date of birth, city/town of birth and the USI allocated to them. These are important pieces of data for the USI Agency to retain about each student. However, unnecessary exposure of those details about students could pose risks such as identity fraud for the students. It is therefore important to ensure that the data exposed by the USI Agency is kept to a minimum.

(f) It is intended that transcripts and extracts will contain the student's name, but not their USI.

Privacy Positive

Limiting identity data on authenticated transcripts issued by the USI Agency to the student's name – and not including the USI – will assist in minimising risks such as identity fraud and the adoption of the USI beyond the education sector.

The development of the USI system will need to ensure that proper controls are applied to minimise the risk of access to data by unauthorised external parties, as well as the risk of misuse by trusted insiders. Data security controls should typically include features such as SSL for data in transmission, role-based access controls, staff screening and training, and audit logs to track when authorised users have read or amended student data. The precise controls applied should be commensurate with the level of risk posed by the data, and set in accordance with the Australian Government Department of Defence's *2012 Information Security Manual*.

Recommendation 9

That the USI Taskforce commission an independent Threat and Risk Assessment of the design of the USI Register and USI system before it is finalised, to assess compliance with the 2012 *Information Security Manual* in terms of the information security classification (both at the unit level and at the aggregate level) and data security controls to be applied.

Recommendation 10

That the NCVER review their proposed data security arrangements for 2014 onwards, as against the 2012 *Information Security Manual*, given the enhanced nature of the data to be collected with the introduction of the USI.

10.3 Data quality

(a) NPP 3 requires organisations to take reasonable steps to ensure that the personal information they collect, use or disclose is accurate, complete and up-to-date.

The principle of data quality, or accuracy, has been described as 'the most important' of all privacy principles, its status reflected in the fact that, unlike limitations on collection, use and disclosure, non-compliance cannot be authorised by another law.[63]

However, the need to maintain 'up-to-date' records must be balanced against other privacy principles, such as the need to only collect personal information when necessary.

[63] *Director General, Department of Education and Training v MT* (GD) [2005] NSWADTAP 77 at [37].

The objective of the data quality principle is to ensure that data is 'fit for purpose'. Once a USI has been allocated to a student and they have been notified in writing of that fact, the USI Agency does not need to know the student's contact details until such time as the student instigates a transaction, such as by requesting an authenticated transcript.

We therefore suggest that the USI Agency does not need to maintain current data about students' addresses, because it typically will not need to use the contact data until such time as the student contacts the Agency first. However, in the event that the USI Agency does need to contact a student directly (e.g. to resolve a duplication error) and the address on the USI Register is found to be out of date, the USI Agency can approach the last RTO for the student's last known contact details.

Recommendation 11

That the primary student address field in the USI Register not be overridden by different addresses supplied by later RTOs when searching for a student's USI.

Recommendation 12

That the USI Agency's website / student portal be designed such that at the point the student contacts the USI Agency to request a 'web view' or authenticated transcript of their education history, or to set permissions for an RTO to access their educational data, the system should first require the student to check and confirm or update their preferred contact details.

(f) Any errors in the educational data related to a student will have come from the RTO which issued the qualification, and thus correction responsibility will rest with the RTO. We therefore make no recommendations about amending educational data.

(g) We note that the USI Agency will host relevant data on its own server, which will not be shared with or accessed by other agencies or organisations.

Chapter 11 – Further recommendations

The recommendations made in Chapters 5 to 10 addressed privacy risks, and corresponding mitigation strategies, as against a set of privacy principles.

This chapter makes further recommendations to minimise the impacts and risks of the proposal in a more 'global' or holistic sense.

11.1 Future expansion of the scheme

(a) As noted in Chapter 3, the USI is being implemented to allow for its possible expansion to other education and training sectors in the future.

(b) Public acceptance of the USI scheme will depend on trust that can only be achieved through transparency. It is intended that the communication strategy for the rollout of the USI will make it clear that governments may decide to expand the USI beyond the VET sector at a later stage.

(c) This PIA has only focussed on the application of a USI to the VET sector. Further assessments and consultations will be required as expansion plans develop.

Recommendation 13

That DIISRTE commit to undertaking further Privacy Impact Assessments, and public consultation, for each future stage (if any) in the rollout of the USI.

11.2 Governance of the USI Agency

(a) As discussed in Chapter 4, the USI Agency will be established as a statutory authority under the USI legislation.

(b) We understand that the technology for the USI system will be designed in-house by DIISRTE, and then be handed over to the USI Agency once it is established.

(c) We understand it is likely that the USI Agency will be physically located within a building leased by an existing Commonwealth department. However, the USI Agency will have its own staff, systems and IT infrastructure.

Recommendation 14

That the communication strategy for the rollout of the USI make clear that the USI Agency will not share data with any other government agency, except as provided for under the access arrangements for RTOs and training authorities and under the research exemption in the USI legislation.

Governance of the broader scheme

(d) At the time of preparing this PIA Report, the USI legislation was in the process of being drafted. Chapter 4 outlines the proposed drafting approach, as advised by DIISRTE as at 2 October 2012.

Recommendation 15

That the USI legislation contains appropriate provisions to:

- provide appropriate restrictions on the collection, use and disclosure of the USI and related EOI data, as set out in sections 4.6.2(c) and 6.4.1 of this report;
- authorise the provision of the USI by RTOs and STAs to the NCVER (either directly or via an STA) for reporting purposes (unless such disclosures and collections will instead be authorised under standards made under the *National Vocational Education and Training Regulator Act 2011* (Cth));
- if necessary, authorise transborder disclosures which might not otherwise be allowed under existing privacy principles that are applicable to RTOs and/or STAs;
- if necessary, authorise the use and disclosure of the USI and associated data by the USI Agency and/or the NCVER (but not RTOs or STAs) for research purposes, subject to the tests set out in section 9.1(c) of this report; and
- deliver a nationally consistent enforcement regime which provides individuals with remedies for any privacy breaches, as set out in section 4.6.2(c) of this report.

Oversight and reporting

Research in 2003, which compared Australians' attitudes and expectations about privacy with people in four other countries, suggests that 92% of Australians would feel more comfortable about their personal information being communicated over the internet if recipients were required by law to notify their customers of any breach of security that could compromise their personal information.[64]

The Australian Law Reform Commission has recommended the introduction of a new regime of mandatory notification of serious data security breaches. The Australian Government is currently considering this proposal. In the meantime the Australian Privacy Commissioner released guidelines encouraging voluntary notification of serious data security breaches.

Recommendation 16

That the USI Agency adopt and follow the Office of the Australian Information Commissioner's guidelines on voluntary notification of serious data security breaches.

Consultation

We make the following recommendations about publication of PIA reports to enhance public trust in the USI scheme, through transparency about the scheme's privacy impacts.

Recommendation 17

That this PIA Report be reviewed and updated when the draft USI legislation is finalised.

[64] Drs Milagros (Millie) Rivera Sanchez, Hichang Cho and Sun Sun Lim, from the Information and Communications Management Programme at the National University of Singapore, conducted the research, which was funded by NUS's Faculty of Arts and Social Sciences. The survey was carried out across five countries by AC Nielson in May 2003: Australia, Singapore, South Korea, the United States and India.

Recommendation 18

That this PIA Report be provided to the Office of the Australian Information Commissioner, and the Privacy Commissioner (or equivalent) for each State and Territory.

Recommendation 19

That this PIA Report be published on the DIISRTE website with the Government's response, and on the USI Agency's website once the latter is operational.

Chapter 12 – Conclusions

12.1 Assessing privacy impacts

(a) The success of the USI scheme will depend on the compliance of RTOs and students. Compliance depends on public acceptance. For the public to accept a scheme, they must trust it. For the Government to earn the public's trust, it must demonstrate that every attempt has been made to achieve the appropriate balance between competing objectives. This means minimising any unnecessary and avoidable privacy intrusions, and ensuring that the remaining privacy impacts are proportionate to the risks, and justified by positive outcomes.

(b) Identifying privacy impacts and risks involves an examination of how the proposal will *'affect the choices individuals have regarding how information about them is handled, the potential degree of intrusiveness into the private lives of individuals, compliance with privacy law, and how the project fits into community expectations.*[65]

(c) Privacy impact assessments therefore respond to public concerns not only about strict compliance with privacy and related laws, but also to concerns about the wider implications of government and business initiatives that affect the level of surveillance and monitoring of individuals in society.

(d) The need to examine issues beyond compliance with privacy laws is partly because in many respects, privacy principles in information privacy laws defer to other legislation that authorises or requires certain data to be collected, used or disclosed. As a result, the critical question is not whether or not the proposal will comply with the letter of the relevant privacy laws, but whether or not it will meet the spirit or intent of the law, and community expectations.

(e) A summary is provided below of our findings in relation to the 'privacy positive' aspects of the USI scheme, as well as recommendations to address those areas we identified as raising some degree of privacy risk.

12.2 Privacy positives of the USI proposal

The privacy positives identified in Chapters 5 to 10 are summarised as follows:

(a) **Improved access to personal information:** One of the key objectives of a USI is to improve the ability of students to access and compile their educational data over time, and over multiple RTOs.

(b) **No charge for transcripts:** Not charging students for transcripts ensures compliance with the Access principle, i.e. the provision of personal information to the individual concerned at no or minimal cost. It also minimises privacy risks relating to the additional storage of billing data which would need to be protected from misuse.

(c) **Access to demographic data:** The development of a protocol between the USI Agency and the NCVER to manually handle student requests for access to demographic data held by the NCVER promotes the Access principle.

---

[65] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, August 2006, p.xxi

(d) **Quarantining of data**: Holding a student's education data in one database and organisation (NCVER), and their identity and contact data in another database and agency (the USI Agency), is a sensible data security strategy.

(e) **Limitations on creation of USI:** The inclusion of provisions in the USI legislation which will effectively prohibit RTOs from requiring students undertaking non-accredited courses to obtain a USI will assist in managing community concerns regarding the scope of the USI scheme. It will also promote compliance by RTOs in relation to their Disclosure obligations, and by training authorities and the NCVER in relation to their collection limitation obligations.

(f) **No retention of EOI data:** The design decision that the USI Agency will not retain EOI data minimises risks in relation to fraud and the creation of 'identity stores'. It also minimises compliance risks in relation to the Data Quality principle, having regard to the fact that some identifiers such as driver licenses and passport numbers change over time and may therefore have limited utility in any case.

(g) **Limitations on RTO collection of EOI data:** The inclusion of provisions in the USI legislation prohibiting the retention of EOI information by RTOs and publicising the fact that students can apply directly to the USI agency for a USI through a student communication strategy are sensible approaches to managing the risk of collection and storage of EOI data (or copies of the EOI itself) by RTOs. The communication strategy is also relevant to ensuring compliance with the Direct Collection and Collection Notice privacy principles by the USI Agency, the NCVER and RTOs.

(h) **Restrictions on use:** Privacy-positive design principles adopted include that there will be no combination of a student's education data (held by NCVER) and their identity/contact data (held by the USI Agency), except at the instigation of the student, or under specified and limited circumstances set out in the legislation.

(i) **No retention of transcript:** The design decision that the USI Agency will not retain a copy of the educational data for that student once the requested transaction has been performed is a sensible data security strategy.

(j) **Limits on disclosure of data on transcript:** Limiting identity data on authenticated VET transcripts issued by the USI Agency to the student's name – and not including the USI – will assist in minimising risks such as identity fraud and the adoption of the USI beyond the education sector.

(k) **Limits on disclosure of education data to RTO/training authority:** Privacy-positive design principles adopted include that an RTO/training authority will only be allowed to access or download a student's education data by demonstrating that they have the student's USI and that the student has consented.

(l) **Limitations on disclosure of personal identifying information:** The system design prevents an RTO from looking up a student's address or other personal details without the student's consent.

(m) **Evidence of consent:** Privacy-positive design principles adopted to date include that a student will demonstrate their consent to an RTO/training authority's request to access or download their education data by way of an online, revocable nomination of that RTO/training authority.

(n) **Logging USI account access:** Allowing students to request an audit log of user access will assist students in managing their permissions, and to identify unauthorised access.

12.3 Privacy risks

The privacy risks identified in Chapters 5 to 10 are summarised as follows. Based on our understanding of the proposed design of the USI system and what the USI legislation is intended to achieve, we do not consider any of these risks to be 'material' in the sense that they require mitigation measures that would cause significant delay to the implementation process. However, whether this assessment remains true depends on the final form of the USI legislation in relation to authorising collections, uses and disclosures.

(a) The risk that RTOs do not understand their obligations in relation to the retention of EOI information, resulting in a risk of unnecessary retention of information, and possible fraudulent or other misuse.

(b) The risk that students do not understand the purposes for which their information may be collected, used and disclosed, and by whom.

(c) The risk that students do not understand how to set and manage access permissions, including in relation to the form of transcripts.

(d) The risk that the USI system is subject to unauthorised access or misuse.

(e) The risk that the USI Agency collects or uses unnecessary or out-of-date student contact details.

12.4 Recommendations to mitigate privacy risks

The recommendations made in Chapters 5 to 11 are summarised in the following categories:

12.4.1 Communications

(a) That student communications about the various access control settings and the limits to those settings be made available to students in plain language and in multiple community languages. **(Recommendation 6)**

(b) That the communication strategy for the rollout of the USI make clear that the USI Agency will not share data with any other government agency, except as provided for under the access arrangements for RTOs and training authorities and in the other limited and specified circumstances set out in the legislation (e.g. under the research exemption). **(Recommendation 14)**

12.4.2 Working with stakeholders

(a) That the USI legislation is supplemented with guidance for RTOs to clarify the circumstances in which the retention of EOI information is, and is not, permissible. **(Recommendation 1)**

(b) That the USI Taskforce liaise with the NCVER to develop one or more template privacy notices, to be included as part of the standard enrolment questions in the AVETMISS standard for 2014 release.

Note: The privacy notice should provide:

- a succinct, plain language explanation of what data is sent by the RTO to the relevant training authority (if applicable), the USI Agency and the NCVER, and
- clarity that the questions asked about disability, indigenous status and language spoken at home are optional, but that if answered they will be provided to the relevant training authority (if applicable) and the NCVER. **(Recommendation 3)**

(c) Alternatively, or in addition to Recommendation 3, that the USI Taskforce (and the USI Agency once it comes into operation) encourage RTOs to adopt template privacy notices by way of guidance and other communication strategies as appropriate. **(Recommendation 4)**

12.4.3 System design

(a) That the USI Taskforce work with SMS vendors to seek a method by which data about students that is not required to be reported by RTOs to an STA or the NCVER (i.e. students undertaking non-accredited courses), is not sent by RTOs. **(Recommendation 2)**

(b) That the design of the USI system include a prompt (such as a screen prompt on next log-in) to students with delegated RTOs and training authorities to review their delegations and check the accuracy of their information. **(Recommendation 5)**

(c) That the final database design specifications not preclude the development of more complex business rules around mediated access in the future. **(Recommendation 7)**

(d) That students have available to them a 'preview' function which allows students to see how their record will appear to RTOs/STAs, depending on the information and access controls they set. **(Recommendation 8)**

(e) That the USI Taskforce commission an independent Threat and Risk Assessment of the design of the USI Register and USI system before it is finalised, to assess compliance with the 2012 *Information Security Manual* in terms of the information security classification (both at the unit level and at the aggregate level) and data security controls to be applied. **(Recommendation 9)**

(f) That the NCVER review their proposed data security arrangements for 2014 onwards, as against the 2012 *Information Security Manual*, given the enhanced nature of the data to be collected with the introduction of the USI. **(Recommendation 10)**

(g) That the primary student address field in the USI Register not be overridden by different addresses supplied by later RTOs when searching for a student's USI. **(Recommendation 11)**

(h) That the USI Agency's website / student portal be designed such that at the point the student contacts the USI Agency to request a 'web view' or authenticated transcript of their education history, or to set permissions for an RTO/training authorities to access their educational data, the system should first require the student to check and confirm or update their preferred contact details. **(Recommendation 12)**

12.4.4 Governance

(a) That the USI legislation contains appropriate provisions to:

- provide appropriate restrictions on the collection, use and disclosure of the USI and related EOI data, as set out in sections 4.6.2(c) and 6.4.1 of this report;
- authorise the provision of the USI by RTOs and training authorities to the NCVER (either directly or via a training authority) for reporting purposes (unless such disclosures and collections will instead be authorised under standards made under the *National Vocational Education and Training Regulator Act 2011* (Cth));
- if necessary, authorise transborder disclosures which might not otherwise be allowed under existing privacy principles that are applicable to RTOs and/or STAs;

- if necessary, authorise the use and disclosure of the USI and associated data by the USI Agency and/or the NCVER (but not RTOs or training authorities) for research purposes, subject to the tests set out in section 9.1(c) of this report; and
- deliver a nationally consistent enforcement regime which provides individuals with remedies for any privacy breaches, as set out in section 4.6.2(c) of this report. **(Recommendation 15)**

12.4.5 Transparency

(a) That the USI Agency adopt and follow the Office of the Australian Information Commissioner's guidelines on voluntary notification of serious data security breaches. **(Recommendation 16)**

(b) That this PIA Report be provided to the Office of the Australian Information Commissioner, and the Privacy Commissioner (or equivalent) for each State and Territory. **(Recommendation 18)**

(c) That this PIA Report be published on the DIISRTE website with the Government's response, and on the USI Agency's website once the latter is operational. **(Recommendation 19)**

12.4.6 Further assessments

(a) That DIISRTE commit to undertaking further Privacy Impact Assessments, and public consultation, for each future stage (if any) in the rollout of the USI. **(Recommendation 13)**

(b) That this PIA Report be reviewed and updated when the draft USI legislation is finalised. **(Recommendation 17)**

Schedule 1 – Documents considered

(a) Department of Innovation, Science, Research and Tertiary Education, *Project: Implementation of a Unique Student Identifier for the Vocational Educational and Training Sector*, version 3, July 2012;

(b) Department of Innovation, Science, Research and Tertiary Education, *Unique Student Identifier – Draft Communication Strategy 2012-2014*, July 2012;

(c) Department of Innovation, Science, Research and Tertiary Education, *Drafting Instructions – Unique Student Identifiers Bill 2013*, version 2.3, 22 June 2012;

(d) National VET Data Strategy Action Group, *A Unique Student Identifier for Australia's Vocational Education and Training System: Overview of Responses to the Consultation Paper about introduction of a USI in VET*, September 2010;

(e) Information Integrity Solutions, *Legal, Governance and Privacy Review: Vocational Education and Training Sector Unique Student Identifier*, 24 June 2011;

(f) The Nous Group, *Unique Student Identifier Stakeholder Consultation Report*, July 2011;

(g) National Council for Vocational Education Research Limited, *AVETMISS VET Provider Collection Specifications – Australian Vocational Education and Training Management Information Statistical Standard*, Release 6.1, July 2011;

(h) Data and Performance Measurement Principal Committee for the Standing Council on Tertiary Education, Skills and Employment, *Final business case for a Vocational Education and Training Unique Student Identifier*, September 2011;

(i) Department of Education, Employment and Workplace Relations, *Unique Student Identifier - COAG Consultation Regulation Impact Statement*, December 2011;

(j) Thirteen submissions made during December 2011 and January 2012 in response to the Regulation Impact Statement, including from the Office of the Victorian Privacy Commissioner, *Submission to the Department of Industry, Innovation, Science, Research and Tertiary Education – Unique Student Identifier – Comments on the COAG Regulation Impact Statement*, 20 January 2012;

(k) USI Taskforce IT Development Working Group, *Business Process Mapping and Resource Requirements* (v.3), 25 January 2012;

(l) Department of Innovation, Science, Research and Tertiary Education, *Project: Implementation of a Unique Student Identifier for the Vocational Educational and Training Sector – Detailed Business Requirements*, version 2, 20 April 2012;

(m) Department of Education, Employment and Workplace Relations, *Risk Management Plan, 23* March 2012; and

(n) Department of Innovation, Science, Research and Tertiary Education, *Unique Student Identifier: Overview of Risk*, 23 March 2012.

Schedule 2 – Glossary and acronyms

AQF	Australian Qualifications Framework
AQTF	Australian Quality Training Framework
AVETMISS	Australian Vocational Education and Training Management Information Statistical Standard
COAG	Commonwealth of Australian Governments
DEEWR	Department of Education Employment and Workplace Relations (Note: As at the date of writing, the USI Taskforce had transitioned to DIISRTE)
DIISRTE	Department of Industry, Innovation, Science, Research and Tertiary Education
DVS	Document Verification Service, a web service provided by the Attorney-General's Department (and housed by DHS) that assists in identity verification processes by confirming the validity of State and federally-issued items of documentation, e.g. passports, drivers' licences
Enrolment Advocate	An RTO
Entitlement Administrator	An RTO or STA
EOI	evidence of identity
Fed IPPs	information privacy principles, found in the *Privacy Act 1988* (Cth)
LUI	Queensland Learner Unique Identifier
MCTEE	Ministerial Council for Tertiary Education and Employment (now SCOTESE)
NCVER	National Centre for Vocational Education Research
NPPs	national privacy principles, found in the *Privacy Act 1988* (Cth)
NVR	National VET Regulator
RTO	Registered Training Organisation
SCOTESE	Standing Council on Tertiary Education, Skills and Employment (formerly MCTEE)
SMS	Student Management System
STA	State Training Authority
TAFE	Technical and Further Education institution, registered training organisation owned and operated by a state government, public provider of training.
USI	Unique Student Identifier
VET	Vocational Education and Training
VSN	Victorian Student Number

About the authors

Minter Ellison

Minter Ellison is one of the largest full-service law firms in the Asia Pacific region, with more than 290 partners and 1,000 legal staff working throughout Australia, Hong Kong, the People's Republic of China, Mongolia, New Zealand and the United Kingdom. We represent over 150 different government departments, agencies and statutory authorities at federal, state, territory and local government levels, throughout Australia, New Zealand and the Asia Pacific including in the education sector.

Salinger Privacy

This report has been prepared with the assistance of Anna Johnston, Director of Salinger Privacy.

Ms Johnston was previously the Deputy Privacy Commissioner of NSW. She holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. Ms Johnston was admitted as a Solicitor of the Supreme Court of NSW in 1996, and is an accredited mediator.