Chapter 4

Challenges faced in undertaking digital transformation

Introduction

4.1 This chapter details evidence regarding critical challenges to digital transformation including:

- Cyber security, risk and resilience.
- Privacy:
- The diversity of users and their needs:

Critical challenges to digital transformation

Systems architecture issues

4.2 Many submissions focussed on practical and technological challenges facing infrastructure and platform design, including hardware legacy issues, as well as complexity arising from the digitalisation of a diverse range of government activities and services in compliance with the applicable legislative regime.[1]

Infrastructure design

4.3 Submissions on infrastructure and platform design covered a variety of issues:

- quality assurance;
- the need for a consultative approach to platform design;
- a whole-of-government approach to standards;
- that systems must comply with administrative law principles; and security; and
- privacy imperatives.

4.4 Several submissions emphasised that understanding the user's needs is paramount when designing digital systems, and recommended the co-design and user-testing of proposed government digital services.[2] Mr Chris Hamill noted the need for digital services to be designed to resemble traditional services that consumers are used to, both in terms of style and format, and in terms of procedure, 'familiarity' being the key to engaging the less computer literate or less confident consumer.[3]

4.5 Ms Louise MacLeod, Senior Assistant Ombudsman, Operations Branch, Office of the Commonwealth Ombudsman, agreed, stating the need for designers to

---

1 See, for example, SCOA Australia, *Submission 2;* Department of Human Services, *Submission 13;* National Archives of Australia, *Submission 22.*

2 Commonwealth Ombudsman, *Submission 12*, pp. 3 and 5; COTA Australia, *Submission 14*, p. 6; Mr Chris Hamill, *Submission 8*, p. 9; Federation of Ethnic Communities' Councils of Australia, *Submission 3*, p. 3.

3 Mr Chris Hamill, *Submission 8*, p. 3.

understand their users, and to build into the design of a system explanations of what information is sought, and why:

> so that people along the way understand what they have to complete, why they have to complete it and the consequences for not providing that information.[4]

4.6 The Royal Australian College of General Practitioners (RACGP) commented on the need for co-design, reporting that:

> A previous lack of general practice clinical engagement has resulted in the delivery of some products which are not fit for purpose…[5]

4.7 SCOA Australia identified a further ongoing, and potentially intransigent design issue that needs to be accommodated in digital transformation, being that government systems must be designed and built so that they can actually be used by their intended users who may be relying on old and outmoded devices:

> Firstly, users may be using a wide range of devices to access the system – Apple computer, Windows computer…MacOS, Windows 7 – 10 Linux… iPhone…Android,…All these devices will be expected to work with the government system.[6]

4.8 The CPSU contended that co-design in the development of public services be extended to include staff as well as the wider community, noting that employees are uniquely placed to provide input into how public services can be improved:

> Properly involving and utilising the capacity and experience of the APS workforce will result in better designed services.[7]

4.9 DHS has advised that it has established a position of Chief Citizen Experience Officer to focus systemic improvement of the user's experience with the department's digital services:

> [DHS] is also actively applying behavioural insights to understand how and why people make the decisions they do and using this knowledge to test and design more effective digital services.[8]

4.10 Furthermore, in relation to the Welfare Payment Infrastructure Transformation program, Mr John Murphy, Deputy Secretary, Payments Reform, DHS, , acknowledged 'it is not exclusively about digital':

> We fully recognise that for many people digital is a real, appropriate response but that a number of people, particularly those who are vulnerable, need to continue to have access to the services that the department provides

---

4 Ms Louise MacLeod, Senior Assistant Ombudsman, Office of the Commonwealth Ombudsman, *Committee Hansard*, 14 March 2018, p. 51.

5 Royal Australian College of General Practitioners, *Submission 15*, p. 5.

6 SCOA Australia, *Submission 2*, p. 3. See also: COTA Australia, *Submission 14*, p. 7.

7 Community and Public Sector Union (PSU Group), *Submission 16*, p. 11.

8 Department of Human Services, *Submission 13*, p. 26.

> day in and day out. Essentially, what we're also looking to do as part of this program is ensure that the people who need access to our experts, of whom we have many, are able to access those people in a very timely way.[9]

4.11 The DTA promotes its Digital Service Standard (DSS), which articulates criteria that agencies should adopt to establish a 'sustainable multidisciplinary team' to undertake the development process, and recommends a user-centred approach to design.[10]

4.12 Two submissions noted the need for independent reviews of systems design. The Commonwealth Ombudsman described the need for an 'external perspectives in the design, testing and implementation of new digital systems'.[11] Mr Ian Brightwell, who appeared in his private capacity, observed that agencies currently undergo a limited number of structured reviews such as 'Gateway' or the Implementation Readiness Assessments (IRAP). He recommended that review data should be shared more widely, including being published on the DTA's new program status dashboard.[12]

4.13 The Office of the Cyber Security Special Adviser (OCSSA) [now the National Cyber Security Adviser] and the Office of the Australian Information Commissioner (OAIC) are concerned about design that supports trust on line. The OCSSA recommended that cyber security be considered a core part of systems design to strengthen trust on line, noting:

> Security needs to be embedded in all levels of systems architecture, in software and apps, as well as applied to the end-points that public the use to access these systems.[13]

4.14 The OAIC similarly recommended the adoption of a 'privacy by design' approach to build privacy into systems and projects from the design stage onwards.[14]

4.15 With respect to the design of automated decision making systems such as the DHS' Online Compliance Intervention automatically generated debt letters, the Commonwealth Ombudsman noted that the system must be consistent with administrative law values of lawfulness, fairness, rationality, transparency and efficiency.[15] The Commonwealth Ombudsman noted that in 2004, the Australian

---

9 Mr John Murphy, Deputy Secretary, Payments Reform, Department of Human Services, *Committee Hansard*, 23 March 2018, p. 47.

10 Digital Transformation Agency, *Submission 10*, p. 21.

11 Commonwealth Ombudsman, *Submission 12*, p. 6.

12 Mr Ian Brightwell, private citizen, formerly the Chief Information Officer and Director of Information Technology at the New South Wales Electoral Commission, *Submission 17*, p. 5.

13 Office of the Cyber Security Special Adviser, *Submission 6*, p. 3.

14 Office of the Australian Information Commissioner, *Submission 1*, pp. 1–2.

15 Commonwealth Ombudsman, *Submission 12*, *Centrelink's automated debt raising and recovery system*, Report No 2/2017, April 2017, p. 26.

Research Council 'recommended the establishment of an interdisciplinary advisory panel to oversee automated systems'. The Commonwealth Ombudsman suggested:

> One solution to this problem may be for agencies rolling out automated decision making systems to consider establishing advisory panels or delivery units to oversee major digitalisation projects, which include external stakeholders, in particular, the DTA, the Commonwealth Ombudsman, the Office of the Australian Information Commissioner and the Australian National Audit Office in the earliest stages of design and planning.[16]

4.16 Ms Ward considered that the digital delivery of government services requires recognition of the value of embedding information management functionality into digital platforms and services. She considered that this functionality needs to be considered at the outset of technical development, rather than being retrofitted, to enable information to be properly managed. Ms Ward stated:

> …that digital delivery of government services should include information governance requirements and relevant whole-of-government and whole-of-agency digital government services delivery project, noting that the crucial role of information and data play in the delivery of trusted government services and reinforcing requirements under the Digital Continuity 2020 Policy that information management functionality be included in the design of digital platforms and services.[17]

Managing complexity

4.17 A number of department and agency submissions demonstrated the complexity of transforming to digital technology. Though the issues raised in the submissions have a whole-of-government application, the committee were advised that agencies each have their own particular challenges.

4.18 DHS advised that it made over $174 billion dollars in payments to citizens in financial year 2016–2017. It dealt with over 700 million digital and self-service transactions, with digital services being available 99.3 per cent of the time. It has 349 service centres across Australia, with 239 Access Points and 347 agents. It had 19 million visits to service centres, an average of 77 000 per day, and over 52 million phone calls.[18]

4.19 DHS explained the complexities it presently faces in seeking to implement welfare benefits:

> Services are delivered as prescribed by numerous Acts of legislation that describe how benefits and payments must be calculated and delivered.
>
> As the Government introduces new services and changes or ceases existing services, [DHS] needs to amend its systems, procedures and resources to

16 Commonwealth Ombudsman, *Submission 12*, p. 6.

17 Ms Teressa Ward, Assistant Director-General, National Archives of Australia, *Committee Hansard*, 14 March 2018, p. 37.

18 Department of Human Services, *Submission 13*, p. 5.

> maintain their integrity. [DHS] faces several challenges when implementing new or changed government policies. These include:
>
> - Policy initiatives that involve legislative uncertainty and/or rapid implementation
> - Ageing legacy systems that provide day-to-day critical services yet are costly to maintain, are at end-of-life and prevent rapid and/or agile policy implementation, and
> - High demand on technical, programme and project management capabilities, skills and resources.[19]

4.20 Mr John Murphy spoke about joining DHS after a banking career of some 36 years.[20] He reflected on the complexity of the digital task for the department:

> I would like to reiterate what I said earlier: the environment and the complexity in the government sector are far more pronounced than what you would see in the private sector…
>
> …Our challenges are, in no particular order: the redesign of the business processes; the ability to implement the changes that we need to make, and by that I mean the culture, the reskilling, the retraining of our people, and the right-sizing of the department, by which I mean having the right people in the right place; and then the technology. Certainly, as I say, it's probably unfair to draw a direct comparison between government and the private sector. My point would be that the expectations of customers have gone up significantly. That includes being able to do things digitally, being able to stay in the digital channel, and equally—I think we would all agree we would expect—to be able to access services anytime, anywhere. You've only got to look in the private sector. You have, generally speaking, more access and greater access to various services outside of the normal business hours. The idea of normal business hours fell away many years ago.[21]

4.21 The ATO advised that its computing environment holds data securely for 25 million clients and partners.[22] The ATO observed that it operates in a 'necessarily complex' environment, referring to its systems' 'co-dependencies'. The ATO stated that the taxation regime collects data from banks, states and territories, stock exchange companies, employers, private health insurance providers, Centrelink and other government agencies, and employee share schemes. It also interacts with the superannuation industry including self-managed superannuation funds, tax professionals, other government agencies, a variety of digital services providers, and intermediaries including financial advisers, insolvency practitioners and legal practitioners:

---

19 Department of Human Services, *Submission 13*, p. 32.

20 Mr John Murphy, Deputy Secretary, Payments Reform, Department of Human Services, *Committee Hansard*, 23 March 2018, p. 47.

21 Mr John Murphy, Deputy Secretary, Payments Reform, Department of Human Services, *Committee Hansard*, 23 March 2018, p. 48.

22 Australian Taxation Office, *Submission 9*, p. 5.

> While our IT infrastructure is extensive to support the vast array of systems, millions of transactions and interactions needed to administer the tax system and superannuation systems each year, we don't and can't do it in isolation. We are integrated; our systems, our data, our technology, or legislative framework and our infrastructure all have co-dependencies across the economic and digital landscape.[23]

4.22 The circumstances of Home Affairs' are directly opposite to those of the ATO in that it is aggregating its business systems, but is equally complex. Home Affairs technologies represent critical infrastructure that allow the department to protect and manage the Australia's territorial border. The breadth of technologies is underpinned by a complex technology foundation of networks spanning unclassified to top secret material, and storage data infrastructure which is delivered by a range of models from in-house support to fully managed commercial services.[24] Home Affairs' functions are undertaken 24 hours per day, seven days a week in 84 locations across Australia and 50 locations world-wide. It operates 250 SmartGates and kiosks, more than 3 000 CCTV cameras, patrol boats, surveillance aircraft, 2 000 terrestrial and satellite capabilities, 660 detection and inspection technology units and more than 11 000 personal defence equipment and wearables located within 48 armouries.[25]

4.23 Home Affairs submitted that it is managing complexity by:

> Removing the dependencies between applications by developing independent business systems, or decoupled domains, enables the ability to more effectively make changes to business functionality and reduces the time to implement new functionality or change business processes. Using this approach, changes to business policy, process or functionality can occur without the need to impact or involve other business systems. By aggregating critical business information into a single service and providing this service to all business systems, each decoupled business system gains by:
>
> - Having access to a deeper set of information
> - Allowing effective decision making
> - Simplifying and reducing maintenance requirements over time.[26]

4.24 Ms Ward identified a very different but equally significant complexity facing Commonwealth agencies' digital transformation is the capacity to retain and preserve Commonwealth records. She observed that Commonwealth records are being created in a range of digitalised formats. The obligation on departments and agencies in transferring material to the National Archives is to ensure the data, including

---

23 Australian Taxation Office, *Submission 9*, p. 16.

24 Department of Home Affairs, *Submission 4*, p. 3.

25 Department of Home Affairs, *Submission 4*, p. 3.

26 Department of Home Affairs, *Submission 4*, attachment, *Technology Strategy 2020*, p. 9.

metadata, is transferred in a readable format.[27] Ms Ward stated that the National Archives is aware:

> That around 87 per cent of agencies have moved from paper processes to digital processes, and we are also aware that data is being lost every day—either not well-managed, can't be found or kept in locations that aren't appropriate—and that access is rendered impossible both for now and the future.[28]

Legacy issues

4.25 A number of department and agencies' submissions demonstrated the difficulties arising from 'legacy' systems, such as new systems being overlaid on outdated hardware which in turn have been subject to ad hoc iterations of updates and upgrades, as well as outmoded business processes, and security vulnerabilities arising from old technologies.

4.26 Mr Ian Brightwell, who appeared in his private capacity, noted that ICT program failure in the APS is due in part 'to poor backend infrastructure and systems upon which to build online systems'.[29]

4.27 DHS drew attention to challenges it faces in delivering digital services, in particular that core ICT systems were not designed for modern digital services, such that changes to these services brings risk of unforeseen impacts.[30] The DHS stated:

> [DHS's] legacy ICT systems supporting delivery operations are now over 30 years old and were originally built to operate on a different scale…

4.28 [DHS] faces several key challenges in this area:

- The core ICT systems were not designed for modern digital services;
- Any changes to these systems brings the risk of unforeseen impacts, and
- Rules and processes are not standardised across payments, and complex rules cannot be easily changed.[31]

4.29 Mr Murphy summarised the legacy issue facing DHS:

> But, essentially, the environment that we're working in is one that was largely designed back in the seventies, eighties and nineties, which was largely constructed around paper and telephones and largely based on face-to-face interactions. I think it's fair to say that that mode of operating has largely continued. I think we would all recognise that, in this day and age—particularly around customer expectations of digital, simple, clear, easy-to-

27 Ms Teressa Ward, Assistant Director-General, National Archives of Australia, *Committee Hansard*, 14 March 2018, p. 39.

28 Ms Teressa Ward, Assistant Director-General, National Archives of Australia, *Committee Hansard*, 14 March 2018, p. 37.

29 Mr Ian Brightwell, *Submission 17*, p. 6.

30 Department of Human Services, *Submission 13*, p. 33.

31 Department of Human Services, *Submission 13*, pp. 32–33.

> use, safe and available anytime, anywhere—that is a very, very difficult proposition for the delivery of welfare without a fundamental change.[32]

4.30 Home Affairs stated that it will continue to sustain legacy technology capabilities as they are progressively decommissioned and replaced over the next 5–10 years. Home Affairs will actively manage the costs associated with making changes and enhancements of legacy technology capabilities to minimise the costs involved.[33]

4.31 Mr Osmond Chiu, Policy and Research Officer, CPSU, reported the difficulties facing APS staff who use the technology:

> many of the ICT systems that APS staff are using are quite old and outdated. The 2015-16 ICT trends report found that 44 per cent of the government's major applications are over a decade old and that 53 per cent of the government's desktops and laptops are past the end of their planned useful life. So when you have very old ICT software and systems, it can often mean that it takes a long time to log in and there can be massive delays.[34]

4.32 Mr Alastair MacGibbon, NCSA, and head of the ACSC observed that legacy systems are hard to protect against threats:

> …an issue we have– and government is very much not immune to [threats]—is the conflict of legacy systems. You have an application of a piece of software that only runs on a particular type of computer. You can't upgrade the computer system, because the software won't run on it. This happens not just in government…as a consequence, you end up with a series of legacy systems that are hard to protect. We know that newer systems generally have a lot of the bugs ironed out of them. The latest versions of the software have patched security vulnerabilities that previous versions haven't patched. If you're running old systems that you can't update the software on, then it could be that there are an increasing number of methods of attack, whether they're for state actors or criminal groups. Government is not immune from that.[35]

Cyber security, risk and resilience

4.33 Submissions from government specialists dealt with the need to embed cyber security protections and protocols in the design stage of infrastructure and software, being cognisant of the inherent vulnerability of internet based government

---

32 Mr John Murphy, Deputy Secretary, Payments Reform, Department of Human Services, *Committee Hansard*, 14 March 2018, p. 47.

33 Department of Home Affairs, *Submission 4*, p. 17.

34 Mr Osmond Chiu, Policy and Research Officer, Community and Public Sector Union, *Committee Hansard*, 14 March 2018, p. 13.

35 Mr Alastair MacGibbon, National Cyber Security Adviser, *Committee Hansard*, 14 March 2018, p. 42.

infrastructure and systems to malicious threats to their integrity. The submissions also address risk mitigation and systems resilience.[36]

4.34 The NCSA identified issues of cyber risk, stating that 'with the vast opportunity of the internet comes risk'.[37] The NCSA noted that the Cyber Security Centre's *Threat Report* of 2016 revealed the nature and extent of the threat against Australian Government networks. The NCSA stated:

> As Government services move online there is a new imperative to embrace cyber security as a core objective of digital transformation.[38]

4.35 The NCSA also referred to the need for a culture of security, noting that 'there is a prevailing tick box compliance culture'; that agencies consider themselves secure if there is compliance with prescribed security procedures, whereas 'compliance does not equal security'.[39] The NCSA further stated that 'security must be "baked in" to design and delivery' of digital services.[40]

4.36 Mr MacGibbon observed:

> There is no such thing as a totally secure connected system, nor is there a totally stable connected system. Rather than looking at a binary secure or insecure state, I think we really need to enter into a world of asking about resilience and risk management.[41]

4.37 On the issue of the management of risk, Mr Mike Burgess, Director, Australian Signals Directorate (ASD), observed that the issue of risk-management of cyber intrusions is a reasonably new circumstance:

> I'm not familiar with the SFIA framework [Skills Framework for the Information Age] from a management-of-your-cybersecurity-risk point of view, and it's fair to say there is no decent framework internationally recognised on how to manage cybersecurity risk effectively, because this risk is really a young thing, insofar as the internet is really only 10 years old

36 See, for example, National Cyber Security Adviser, (formerly the Office of the Cyber Security Adviser), *Submission 6;* Department of Defence, *Submission 7;* Mr Ian Brightwell, *Submission 17*.

37 National Cyber Security Adviser, formerly the Office of the Cyber Security Special Adviser, *Submission 6*, p. 1.

38 National Cyber Security Adviser, formerly Office of the Cyber Security Special Adviser, *Submission 6*, pp. 1–2.

39 National Cyber Security Adviser, formerly the Office of the Cyber Security Special Adviser, *Submission 6*, p. 2.

40 National Cyber Security Adviser, formerly Office of the Cyber Security Special Adviser, *Submission 6*, p. 2.

41 Mr Alastair MacGibbon, National Cyber Security Adviser, *Committee Hansard*, 14 March 2018, p. 43.

> in the benefit we're seeing in society, even though it's been around longer, and there isn't yet a decent body of practice.[42]

4.38 The NCSA offered this warning to governments and the public at large:

> Security of personal and financial information is not solely the government's responsibility. The government can only protect what it possesses... Everyone must take responsibility for their online security.[43]

4.39 The ASD advised that one of its functions prescribed by legislation is to provide material, advice and other assistance to Commonwealth and state authorities on matters relating to the security and integrity of information managed digitally.[44] Under the Attorney-General's Protective Security Policy Framework ASD sponsors the Information Security Manual (ISM), which assists government agencies to apply a risk-based approach to protecting their information and systems:

> The controls in the ISM are designed to mitigate the most likely and highest severity security threats to Australian government agencies.[45]

4.40 The ASD's *Strategies to Mitigate Cyber Security Incidents* and the *Essential Eight* provide a prioritised list of practical actions government agencies can take to make their information systems and online services more secure. The ASD stated:

> …the advice that ASD provides to Australian Government agencies, when applied by an agency head as the system owner, should result in digital services that have been designed with due regard to security.[46]

4.41 Dr Nick Tate, Vice-President, Membership Boards, Australian Computer Society (ACS), considered cyber security to be a significant concern in light of attacks now being conducted by nation-states as well as organised crime. He stated that there is a need for dedicated cyber security task forces for all major departments and a national focus on the issue. In this regard, Mr Mike Burgess, Director, ASD, stated:

> There is, however, good advice out there coming from my agency [about risk management], but what's missing is: how do senior executives know the value of their data and ensure they understand who's got access to it, where it is, who's protecting it and how well it's protected from a data security point of view?[47]

4.42 In response to a question from Senator McAllister, Mr Burgess advised that the management of risk is not the issue of having skilled people, but rather it is an

---

42 Mr Mike Burgess, Director, Department of Defence, *Committee Hansard*, 14 March 2018, p. 50.

43 National Cyber Security Adviser, formerly Office of the Cyber Security Special Adviser, *Submission 6*, p. 4.

44 Department of Defence, *Submission 7*, p. 1.

45 Department of Defence, *Submission 7*, p. 1.

46 Department of Defence, *Submission 7*, p. 2.

47 Mr Mike Burgess, Director, Department of Defence, *Committee Hansard*, 14 March 2018, p. 50.

issue of the skill of the chief executive and his or her management team, in identifying and managing the risk effectively.[48]

4.43 Mr Ian Brightwell, who appeared in his private capacity, recommended that agencies separate the roles of CIO [Chief Information Officer] and CISO [Chief Information Security Officer], with each having separate reporting line to the Chief Executive Officer to ensure difficult security decisions are elevated outside the ICT area of an organisation.[49] As to the CIO role, Mr Brightwell said that CIO should not be lower than one level down from the CEO or agency head level because the responsibility rests at the CEO level:

> Because the role of the CISO, I would argue, is largely around audit control and ensuring all the controls for security are in place. Largely, it's the CIO who has the job of implementing those cyber controls and the CISO is going to look at those and look at other controls managed by other levels. You've got to have them as far away from the people doing the job so they can effectively be responsible for reporting their efficacy in implementation. If they're one and the same person, no-one is ever going to find out failure.[50]

4.44 The ATO advised that it maintains an expert in-house capability to conduct cyber-security resilience testing against ATO assets. The ATO testing team are industry certified and have knowledge of ATO systems.[51] Mr Ramez Katf, Second Commissioner and Chief Information Officer, ATO, further advised that the ATO has established a security operations centre to specifically address cyber-security threats.[52]

4.45 DHS advised that it has established a Cyber Security Operation Centre and has significantly enhanced its cyber security monitoring, security threat intelligence, rapid detection and security incident response capability. Mr Charles McHardie, Acting Chief Information Officer, DHS, reported that in March 2017 the ANAO had assessed DHS as being cyber-resilient across all its operations.[53]

Privacy

4.46 Submissions identified privacy as a significant issue for the successful transformation of government services. Submissions from government privacy specialists dealt with the need to embed privacy principles and protections at the design stage of infrastructure and software, recognising and accepting that protecting citizens' privacy is a critical enabler to the government's transition to the digital

---

48 Mr Mike Burgess, Director, Department of Defence, Committee Hansard, 14 March 2018, p. 48.

49 Mr Ian Brightwell, *Submission 17*, pp. 7–8.

50 Mr Ian Brightwell, *Committee Hansard*, 14 March 2018, p. 9.

51 Australian Taxation Officer, answer to written question on notice, received 18 April 2018.

52 Ramez Katf, Senior Commissioner and Chief Information Officer, Australian Taxation Office, *Committee Hansard*, 23 March 2018, p. 16.

53 Mr Charles McHardie, Acting Chief Information Officer, Department of Human Services, *Committee Hansard*, 23 March 2018, p. 28.

delivery of government services. A number of submissions representing citizens' interest have raised the critical issue of the need for a more sophisticated approach to digital identity in light of data analytics.

4.47 The CPSU noted that there is a real risk that the transformation of digital delivery could be derailed because of community concerns about privacy and digital rights. The CPSU highlighted widespread community concern about the ABS' collection and storage of names in the 2016 census.[54]

4.48 COTA Australia (COTA) noted that older people have a strong belief in the importance of the privacy of their personal information. In order to engage this cohort, governments must actively engender confidence that the systems are safe and that information is protected. COTA Australia recommended regular risk assessments and periodic audits of privacy protection procedures, with all breaches being reported to Parliament.[55]

4.49 The Federation of Ethnic Communities' Councils of Australia (FECCA) and COTA also highlighted that confidentiality is an issue with older Australians, people with disability, and culturally and linguistically diverse (CALD) communities where they may be reliant on third parties to whom they must disclose sensitive personal information if they are to engage with government agencies on line, through which process their privacy is breached, and the third party may be placed in the position of a conflict of interest.[56]

4.50 The NCSA has acknowledged that trust and confidence in operating online are the salient factors to successful digital transformation:

> …the potential for digital transformation and digital delivery of government services depends upon the extent to which the Australian people can trust and feel secure online.[57]

4.51 The OAIC recommended the use of privacy impact assessments (PIAs) to provide a systematic assessment of a project that identifies the impact the project might have on the privacy of individuals.[58] The OAIC also advised the development of the *Australian Public Service Privacy Governance Code* (Code) which is to come into effect on 1 July 2018. The Code will set out specific requirements and practical steps an agency must take to comply with Australian Privacy Principles 1.1 (APP) (those include reasonable practices, procedures and systems in place to comply with APPs). The Code requires an agency to undertake a PIA on 'high privacy risk' projects.[59]

---

54 Community and Public Sector Union (PSU Group), *Submission 16,* p. 12.

55 COTA, Australia *Submission 14*, pp. 3–4.

56 Federation of Ethnic Communities' Councils of Australia, *Submission 3,* p. 4; COTA Australia, *Submission 14*, p. 5;

57 Office of the Cyber Security Special Adviser, *Submission 6,* p. 1.

58 Office of the Australian Information Commissioner, *Submission 1,* p. 2.

59 Office of the Australian Information Commissioner, *Submission 1,* p. 3.

4.52 DHS has advised that its operational framework is guided by its Operational Privacy Policy, and its policy is to undertake PIAs for all significant digital services.[60]

Digital identity

4.53 A number of submissions considered the security of a digital identity to be a significant enabler in the transition to digital government.

4.54 SCOA Australia said that a major issue contributing to the way data is used is the ability to positively and uniquely identify individuals.[61] SCOA Australia advocated the introduction of a unique individual identifier on the basis that current identifiers are no longer sufficient.[62] SCOA Australia contended that the lack of a strong identifier has a significant cost, often unheralded:

> Organisations will attempt to data match and data mine large data sources irrespective, with the matching attempt on name, address, birthdate and other descriptive data. The twins, Mary and Margo Smith, therefore spend their lives being mistaken for each other, especially if they share a house and an occupation.[63]

4.55 On this point, Ms Ward referred to a Productivity Commission report that considered data and datasets as a value to the economy and the community.[64] In that context, Dr Tate, ACS, drew attention to the potential dangers of the government's open data initiatives to privacy using apparently de-identified data. Dr Tate observed that data linking tools are such that it is difficult to keep data anonymous. Furthermore, Dr Tate considered there is a need for a framework for de-identification of government data, especially medical data:

> …it is possible to take data from a whole range of different sources, not just medical ones, but often sources you wouldn't expect, and put them together and say, 'Hang on, now we can possibly work out who these are'. I don't know how extensive it is. But the initial work on that has certainly shown that it's possible…[65]

4.56 The ATO noted that taxpayers can now choose voice biometric authentication and cloud authentication and authorisation to establish proof of identity.[66] The ATO also stated that it will continue to invest heavily in securing taxpayer information through robust identity authentication and authorisation platforms:

---

60 Department of Human Services, *Submission 13*, p. 27.

61 SCOA Australia, *Submission 2*, p. 2

62 SCOA Australia, *Submission 2*, p. 2.

63 SCOA Australia, *Submission 2*, p. 3.

64 Ms Teressa Ward, Assistant Director-General, National Archives of Australia, *Committee Hansard*, 14 March 2018, p. 38.

65 Dr Nick Tate, Vice-President, Membership Boards, Australian Computer Society, *Committee Hansard*, 14 March 2018, p. 33.

66 Australian Taxation Office, *Submission 9*, p. 8.

> Increasingly the risk of identity theft in online and digital interactions needs to be anticipated, monitored and mitigated as fraudsters become more sophisticated in their operations.[67]

4.57 The ATO advised that it is continuing to invest heavily in securing taxpayer information through robust identity, authentication and authorisation platforms. It flagged the Tax File Number as a main identifier. It has also introduced the option of voice biometric authentication; and the use of cloud authentication and authorisation; and the linking of an Australian Business Number with myGov accounts.[68]

4.58 The DTA stated that it is working with agencies, other jurisdictions and the private sector to develop the GovPass program, to produce a common model for verifying data that can be used across government:

> To complement the GovPass program, the DTA has developed the Trusted Digital Identity Framework, a comprehensive set of rules, policies and standards that will set a nationally consistent approach to accredit, govern and operate identity across the digital economy…The framework will be extended to address non-digital identity for individuals to allow alternate pathways for those unable to complete identity verification digitally.[69]

4.59 Mr Peter Alexander, Chief Digital Officer, DTA, advised that myGov has now has 12.5 million active accounts. He further advised that the DTA is looking to change the authentication process for myGov to build in the 'Tell Us Once' service, and payment and notification utilities. He also advised that the Trusted Digital Identity Framework is nearing completion; it will be a common framework across government which covers use of identity for digital services; the use of non-digital identities in a digital world for those without a digital identity to interact with government, and also an 'acting on behalf of others' authorisation.[70]

4.60 On 7 May 2018, Mr Gavin Slater, Chief Executive Officer, DTA advised the committee that the DTA had received $60M in the recent budget to work with agencies for the next phase on the development of a digital identity.

> By October a system will be up and running that will allow people to apply for and receive their tax file number. Over the following 12 months the capability will be rolled out to a number of other high-volume government services, giving more than 400 000 people the opportunity to test this capability.[71]

---

67 Australian Taxation Office, *Submission 9*, p. 7. See also Digital Transformation Agency, *Submission 10*, p. 6. See also: Department of Human Services, *Submission 13*, pp. 23– 24; Australian Taxation Office, *Submission 9*, pp. 16–17.

68 Australian Taxation Office, *Submission 9*, pp. 7–9.

69 Digital Transformation Agency, *Submission 10*, p. 6. See also: Department of Human Services, *Submission 13*, pp. 23–24; Australian Taxation Office, *Submission 9*, pp. 16–17.

70 Mr Peter Alexander, Chief Digital Officer, Digital Transformation Agency, *Committee Hansard*, 7 May 2018, p. 10.

71 Mr Gavin Slater, Chief Executive Officer, Digital Transformation Agency, Senate Finance and Public Administration Legislation Committee, *Estimates Hansard*,21 May 2018, p. 101.

The diversity of users and their needs

4.61 Submissions emphasised the diversity of needs and circumstances of the Australian community which must be accommodated in the design, delivery, and ultimately, the acceptance by the public of government delivering services online. A number of submissions expressed dissatisfaction with the government's performance in the delivery of online services.

4.62 A number of submissions focussed on the need for inclusiveness, and particularly the need for the government to maintain traditional methods of dealing with citizens to accommodate sectors of society who are not digitally literate.[72] Submissions concerning website design focussed on the user perspective and the need for user-friendly websites through consistency in screen presentation and language across the whole-of-government sector.

Public expectations of government in digital transformation

4.63 A number of submissions have expressed dissatisfaction in the government's delivery of digital services. Mr Chris Hamill, private citizen, observed:

> …I think it's fair to say the government does not have a great track record when it comes to 'going digital'…
>
> It makes no sense to build a digital service for the nation, if that digital service can't *handle* the nation.[73]

4.64 COTA Australia has made a similar point, expressing concern over the quality and reliability of systems used to deliver government services:

> COTA views customer experience as a key quality domain in online services. In turn, this is comprised of response time, user friendliness, ease of access and availability and responsiveness of customer support. Feedback that COTA has received indicates that current online government services have far to go in this area of performance'.[74]

4.65 Many submissions stated that the success of digital delivery of government services is critically dependent upon the government's capacity to provide a secure and user-friendly service, accessible by all sections of the community, and especially the most vulnerable who are the most likely recipients of government services.[75]

---

72 See, for example: SCOA Australia, *Submission 2*, p. 3; Federal Ethnic Communities Councils of Australia, *Submission 3*, p. 1; Mr Chris Hamill, *Submission 8*, p. 1; Australian Communications Consumer Action Network, *Submission 11*, p. 6; COTA Australia, *Submission 14*, p. 3.

73 Mr Chris Hamill, *Submission 8*, p. 8.

74 COTA, Australia, *Submission 14*, p. 5.

75 See, for example: Office of the Australian Information Commissioner, *Submission 1*, p. 1; Federation of Ethnic Communities' Council Australia, *Submission 3*, p. 2; Mr Chris Hamill, *Submission 8*, pp. 3–5; Australian Communications Consumer Action Network, *Submission 11*, p. 6; COTA Australia, *Submission 14*, p. 3; Community and Public Sector Union (PSU Group), *Submission 16*, p. 3.

4.66 Submissions identified categories of vulnerable Australians, and the barriers each group faces in interacting with the government on line. The categories identified as vulnerable are older Australians;[76] CALD communities[77]; people with disability;[78] people on low incomes;[79] rural and remote communities;[80] remote and Indigenous communities;[81] homeless people;[82] and small business.[83]

4.67 COTA contended that digital inclusion is just as important as privacy and security:

> It is just as important (and challenging) to understand and address inclusion as it is to ensure privacy and security when building government digital platforms, service delivery models and business practices. Given that many government programs are specifically targeted to disadvantaged and vulnerable, it is essential that delivery to be fit-for-purpose.[84]

4.68 The barriers all categories face are a lack of computer literacy, and affordability issues.[85] Homeless people and those in rural and remote Australia face the additional barrier of availability of internet access, and network availability and coverage is an issue for those in remote Australia.[86] A lack of services have led to poor literacy and access for CALD and Indigenous people.[87]

---

76 See, for example: Mr Chris Hamill, *Submission 8*, p. 1; Australian Communications Consumer Action Network, *Submission 11*, pp. 45–49; COTA Australia, *Submission 14*, p. 3.

77 See, for example: SCOA Australia, *Submission 2*, p. 3; Federation of Ethnic Communities' Councils of Australia, *Submission 3*, pp. 1–4; Australian Communications Consumer Action Network, *Submission 11*, pp. 17–26.

78 See, for example: SCOA Australia, *Submission 2*, p. 3; Mr Chris Hamill, *Submission 8*, p. 1; Australian Communications Consumer Action Network, *Submission 11*, pp. 26–33; COTA Australia, *Submission 14*, p. 9.

79 See, for example: Mr Chris Hamill, *Submission 8*, p. 1; Australian Communications Consumer Action Network, *Submission 11*, pp. 33–38; COTA Australia, *Submission 14*, p. 9.

80 See, for example: SCOA Australia, *Submission 2*, p. 3; Australian Communications Consumer Action Network, *Submission 11*, pp. 39–43; Tangentyere Council Aboriginal Corporation, *Submission 19*, p. 7.

81 See, for example: SCOA Australia, *Submission 2;* p. 3; Australian Communications Consumer Action Network, *Submission 11;* pp. 49–56.

82 See, for example: Australian Communications Consumer Action Network, *Submission 11*, pp. 57–60; Tangentyere Council Aboriginal Corporation, *Submission 19*, p. 7.

83 Australian Communications Consumer Action Network, *Submission 11*, pp. 61–68.

84 COTA, Australia, *Submission 14*, p. 3.

85 Australian Communications Consumer Action Network, *Submission 11*, p. 13.

86 Australian Communications Consumer Action Network, *Submission 11*, p. 16.

87 See, for example: SCOA Australia, *Submission 2*, p. 3; Federation of Ethnic Communities' Councils of Australia, *Submission 3*, p. 2; Australian Communications Consumer Action Network, *Submission 11*, pp. 17 and 52.

4.69 Older people are reluctant to engage in the online world, having significant concerns with security and privacy.[88] COTA observed:

> COTA hears from many older Australians that they hold strong belief in the importance of their personal, financial and medical information. Recent research reinforces this with the finding that older people are more likely than younger people to take steps to protect their personal information.
>
> Issue related to privacy and security can create anxiety for many older Australians…To engage this cohort in the transition to digital systems government must actively engender confidence that the systems are safe and information is protected.[89]

4.70 COTA Australia noted that Australians over age 65 are increasingly vulnerable to scams, particularly those involving the loss of money, as well as an emerging trend of threat-based and impersonation scams representing to be from government agencies.[90]

The retention of traditional methods of engagement with citizens

4.71 SCOA Australia and COTA noted that government processes must recognise that there will always be Australians who cannot or will not use an automated process to interact with government.[91] Mr Hamill advocated the need to maintain traditional methods of service delivery concurrently with digital delivery, on the basis that there are many Australians who cannot or will not engage in digital government for a range of practical reasons.[92]

4.72 COTA referred to the importance of inclusiveness. It supported the DTA's Digital Service Standard's recognition of the importance of digital inclusion:

> The Australian Government has acknowledged the importance of digital inclusion in its Digital Service Standard, stating that the services 'need to ensure they are accessible to all users regardless of their ability and environment'. This high-level principle acknowledges government responsibility to all citizens and recognises it is increasingly evident that digital exclusion can further exacerbate the social and economic exclusion experienced by vulnerable Australians.[93]

4.73 ACCAN expressed a similar view that:

> As traditional points of contact such as shopfronts and call centres give way to the Government's new digital channels, millions of digitally disconnected consumers will need to spend more time engaging with the government –

88 Australian Communications Consumer Action Network, *Submission 11*; COTA Australia, *Submission 14*, pp. 3–4.

89 COTA Australia, *Submission 14*, p. 3.

90 COTA Australia, *Submission 14*, p. 4.

91 See, for example: SCOA Australia, *Submission 2*, p. 3, COTA Australia, *Submission 14*, p. 11.

92 Mr Chris Hamill, *Submission 8*, p. 1.

93 COTA Australia, *Submission 14*, p. 7

> exacerbating their social exclusion and the impacts of Australia's digital divide. Without taking positive action to eliminate barriers to universal digital access, the Australian Government risks alienating millions of vulnerable consumers who are effectively denied the opportunity to engage with crucial services such as healthcare, welfare and social housing – all of which are increasingly mediated by the internet.[94]

4.74 COTA also recommended the Australian government ensure appropriate, sustainable and adequately resourced legacy systems, including face-to-face, phone and paper based communications at no extra cost to the consumer are in place for people who are unable to access digital services.[95] SCOA Australia noted that 86 year old Mrs Smith who has never used a computer must be catered for.[96] ACCAN similarly supported the retention of non-digital points of contact until there is universal access to digital technology in Australia,[97] as does Mr Hamill, who observed that the non-digital alternatives should not be:

> …unreasonably inefficient, slow or unreliable, compared to their digital versions.[98]

4.75 The CPSU argued that the community choice of service delivery must be mandatory noting that government and agencies maintenance of the option of face-to-face and other delivery methods is 'vital' on the basis that not all members of the community want to, or are equipped to access government services digitally.[99] In an answer to a question on notice, Mr Tull, Assistant National Secretary of the CPSU expressed concern that government business processes have been designed to push citizens onto online services:

> The role of DHS staff has been changing from helping the most vulnerable and disadvantaged Australians, to implementing business processes that many in the community perceive are designed to make access to financial support from the government as difficult as possible.[100]

4.76 In its submission, the Tangentyere Council Aboriginal Corporation stated that the transfer from the existing Centrelink portal to myGov needs to be halted:

> Future service delivery should not oblige individuals with poor literacy and numeracy; limited English; poor computer literacy; limited access to information technology; and limited internet to access Centrelink services via the internet. Individuals should not be obliged to create email addresses or purchase mobile phones unless they have the capacity to use and

---

94 Australian Communications Consumer Action Network, *Submission 11*, p. 6.

95 COTA Australia, *Submission 14*, p. 11.

96 SCOA Australia, *Submission 2*, p. 3.

97 Australian Communication Consumer Action Network, *Submission 11*, p. 5.

98 Mr Chris Hamill, *Submission 8*, p. 1.

99 Community and Public Sector Union (PSU Group), *Submission 16*, p. 11.

100 Community and Public Sector Union, answers to questions on notice, 14 March 2018 (received 4 April 2018).

> maintain these devices and services in a sustainable manner that is not open to exploitation. Centrelink in particular needs to continue to operate Centrelink agencies in remote areas and for language speaking Aboriginal in a manner that is appropriate and accessible…[101]

4.77 Mr Murphy of DHS advised that the Welfare Payments Infrastructure Transformation program is not exclusively about digital:

> We fully recognise that for many people digital is a real, appropriate response but that a number of people, particularly those who are vulnerable, need to continue to have access to the services that the department provides day in and day out. Essentially, what we're also looking to do as part of this program is ensure that the people who need access to our experts, of whom we have many, are able to access those people in a very timely way.[102]

Website design

4.78 The issue of website design is closely inter-related with the public's expectations of government; that the user as the ultimate arbiter of the success of the new technology must be at the forefront of website design. Many submissions focussed on the confusion and frustration citizens face when they are required to provide the same information to different departments and agencies, all of which have different web designs, some of which are better than others. Submissions focussed on the need for a whole-of-government approach to website design and data collection.

4.79 SCOA Australia observed that, as data is the basis of policy, there must be a consistent approach to its collection, as well as the application of standard definitions:

> The data that Government uses should be defined, standardised, retained and maintained of a whole of Government basis by a central agency, most probably the ABS.[103]

4.80 FECCA advocated the use of consistent icons and layouts across all government websites to enable easier navigation of different agencies' websites by users.[104] Mr Hamill recommended that the layout of digital services be designed to resemble the traditional versions consumers are used to, both in terms of style and formats, noting that the less computer literate can become confused if the format deviates from what they are used to.[105]

4.81 The Commonwealth Ombudsman commented that:

> A key lesson from the [DHS Online Compliance Incident – robot-debt] experience is that the design of the online platform may have a significant bearing on the launch of a new process.

---

101 Tangentyere Council Aboriginal Corporation, *Submission 19*, p. 11.

102 Mr John Murphy, Deputy Secretary, Department of Human Services, *Committee Hansard*, 23 March 2018, p. 47.

103 SCOA Australia, *Submission 2*, p. 2.

104 Federation of Ethnic Communities' Councils of Australia, *Submission 3*, p. 3.

105 Mr Chris Hamill, *Submission 8*, p. 3.

> Seemingly micro-level issues of design may have significant consequences…What icon should be used? Should the phone number appear prominently on each web page? This may determine whether people access help at the critical points or instead give up in frustration...[106]

4.82 The RACGP noted that standard terminology, including the use of structured data and national interoperable standards are vital to the safe sharing of digital information.[107]

4.83 In relation to DHS's 'Cuba' child care payments operating system replacement project,[108] Ms Bridger, General Manager, Child Support and Redress, DHS, advised that a key lesson learnt by DHS during the project was that users must be very tightly intertwined with not only the program or design, but also the testing, trialling and iteration of any initiative. She further advised that recent experience of having the users involved allowed requirements to be acquitted more quickly.[109]

4.84 Mr Charles McHardie, Acting Chief Information Officer, DHS advised that DHS had recently established a new position of Chief Citizen Experience Officer to look after design change from the public perspective.[110]

4.85 The DTA stated that it is developing a whole-of-government design system in collaboration with a community from across the government

> The design system works like a catalogue of reusable design components, including code, that can be used freely by agencies.
>
> This brings consistency to the design of government websites and services…This empowers agencies to transform their services efficiently, bringing usability, accessibility and consistency to the forefront.[111]

Data storage security

4.86 Submissions indicated that data collection and data storage are a very sensitive issue for users, the concerns being demographically based.

4.87 COTA noted that older Australians are concerned about data security where data is held at third party data 'cloud' centres).[112] 'Cloud' is a term used to describe a global network of servers, each with a unique function. The cloud is not a physical entity. It is a vast network of remote servers around the globe which are hooked together and meant to operate as a single ecosystem. These servers are designed to

---

106 Commonwealth Ombudsman, *Submission 12*, p. 3.

107 Royal Australian College of General Practitioners, *Submission 15*, p. 5.

108 Cuba is discussed further in Chapter 4.

109 Ms Maree Bridger, General Manager, Child Support and Redress, Department of Human Services, *Committee Hansard*. 23 March 2018, pp. 29–30.

110 Mr Charles McHardie, Acting Chief Information Officer, Department of Human Services, *Committee Hansard*, 23 March 2018, p. 31.

111 Digital Transformation Agency, *Submission 10*, p. 23.

112 COTA, Australia, *Submission 14*, pp. 3–4.

either store and manage data, run applications, or deliver content or a service... Instead of accessing files and data from a local or personal computer, it is accessed online from any internet-capable device—the information will be available anywhere …and anytime it is needed.[113]

4.88 COTA recommended regular audits to ensure centres meet performance levels relating to security, with all breaches of security being reported to the Australian Parliament and the Australian National Audit Office.[114]

4.89 FECCA accepted the need to collect data for digital delivery of government services, and encouraged data collectors to use secure storage methods, noting that transparency and accountability will garner further trust.[115]

4.90 SCOA Australia stated that data should be retained and maintained on a whole-of-government basis by a central agency, but also makes the additional point about the location of cloud storage:

> Are Australians concerned about whether their tax data is stored in Canberra or in Dallas?[116]

4.91 AusAccess advocated that proper protection of data held by the Australian government means cloud computing centres that are for government data only; are within Australian borders; are Australian owned, and staffed by Australians who have a security clearance.[117] AusAccess recommended that the decision to grant 'protected status' to a multinational cloud service provider should be elevated to a cabinet or parliamentary level, taking the view that:

> The data of Australians held by government *should never be subject* [emphasis in the original] to the actions of any foreign government.[118]

4.92 The AIIA noted the complexity and lack of transparency of the Information Security Registered Assessor Program (IRAP) arrangements administered by the ASD. Under the IRAP arrangement, ASD will certify an assessor who, once certified, is qualified to assess the implementation, appropriateness and effectiveness of an organisation's systems and security controls. The AIIA stated:

> …current arrangements are complex, time consuming and costly and most critically not transparent or responsive to industry attempts to be more actively engaged in the process. While this has obvious impacts on industry, more importantly, it is inhibiting the operation of an effective and

113 *What is the cloud?* https://azure.microsoft.com/en-us/overview/what-is-the-cloud/ (accessed 5 June 2018).

114 COTA, Australia, *Submission 14*, pp. 3–4.

115 Federation of Ethnic Communities' Councils' of Australia, *Submission 3*, p. 4.

116 SCOA Australia, *Submission 2*, p. 3.

117 AusAccess, *Submission 20*, p. 3.

118 AusAccess, *Submission 20*, pp. 3.

> competitive cloud market across government and undermining the government's broader procurement agenda.[119]

4.93 The DTA explained that it is developing a secure cloud strategy to increase government understanding and adoption of cloud services:

> The strategy will address a number of areas to encourage government adoption of cloud, such as promoting cloud in a government context, building confidence in compliance and streamlining assurance processes, creating shared capabilities, guiding agencies to transition to the cloud, and working with industry to make cloud offerings more comparable and easier to adopt.[120]

4.94 In an answer to a question, the ATO has advised that it uses cloud storage, however, the ATO was adamant that it would never put its cloud services in an overseas data centre. The ATO stated that it maintains absolute control over the data centres the cloud services are offered from. The ATO confirmed that its contracting arrangements are that data be physically stored somewhere in Australia.[121]

4.95 The ATO advised that three of its eight applications are available by cloud and are benefitting from improved availability. The ATO stated that it continues to leverage cloud to improve availability of key applications, and will continue to work with the DTA on future cloud policies of strategies.[122]

4.96 DHS similarly confirmed that its cloud services are located onshore in Australia:

> We as a department are a very small consumer of cloud based services. We have a very large on-premise [storage] in both of our large data centres here in Canberra. All of our customer data is kept on shore in both of those data centres. They are what are known as ASIO T4 accredited data centres, so they can handle data up to the secret national security classification. The only cloud services we are using are some add-ons to assist things such as website representations et cetera. We are not moving any customer data offshore.[123]

4.97 Mr McHardie further advised that it has embarked on a program to be able to access cloud based services, known as the 'elastic private information cloud' program (EPIC). The program has been established so that DHS can shift load across its low, mid and mainframe platforms in a more dynamic fashion, but also allows DHS to start

---

119 Australian Information Industry Association, *Submission 5*, p. 5.

120 Digital Transformation Agency, *Submission 10*, p. 10.

121 Mr John Dardo,, Chief Digital Officer and Deputy Commissioner, Digital Delivery, Enterprise Solutions and Technology, Australian Taxation Office, *Committee Hansard*, 21 March 2018, p. 9.

122 Australian Taxation Office, *Submission 9*, p. 6.

123 Mr Charles McHardie, Acting Chief Information Officer, Department of Human Services, *Committee Hansard*, 23 March 2018, p. 27.

the work which will enable DHS to access more cloud based services where appropriate:

> It may be to use some cloud based storage, because it's very cost effective. But you should only consume it if you've done a proper risk based assessment and you know exactly where that data is going to be stored. The DTA may want to say a bit more about that approach.[124]

4.98 Mr Peter Alexander, Chief Digital Officer, Digital Division, DTA referred to the security and privacy regime currently in place through both the ASD's Information Security Manual, concerning how data is stored, the Australian privacy principles concerning the storage of people's private and personal data. The obligation imposed by that guidance is that agencies must 'control' the data:

> …Control then has implications on knowing where it's stored, not putting it in the cloud, when we're talking about people's individual data. But we also have a set of security requirements.[125]

4.99 Mr Alexander further advised that the DTA has built a cloud strategy set of principles and policies for what agencies can use cloud, and how they do it. The DTA is also examining whole-of-government hosting. DTA intends to collect data on what departments and agencies are currently doing to obtain an overall picture of Australian government hosting arrangements. The DTA sees great advantages in obtaining cloud technology and public cloud services, but notes those things come with risks around privacy and security.[126]

124 Mr Charles McHardie, Acting Chief Information Officer, Department of Human Services, *Committee Hansard*, 23 March 2018, p. 27.

125 Mr Peter Alexander, Chief Digital Officer, Digital Division, Digital Transformation Agency, *Committee Hansard*, 23 March 2018, pp. 27–28.

126 Mr Peter Alexander, Chief Digital Officer, Digital Division, Digital Transformation Agency, *Committee Hansard*, 23 March 2018, p. 28.