Chapter 2

Background and context

Referral

2.1 On 16 August 2017, the Senate referred the following matter to the Senate Finance and Public Administration References Committee (the committee) for inquiry and report by 4 December 2017:

Digital delivery of government services, with particular reference to:

(a) whether planned and existing programs are able to digitally deliver services with due regard for:

(i) privacy,

(ii) security,

(iii) quality and reliability, and

(iv) value for money;

(b) strategies for whole of government digital transformation;

(c) digital project delivery, including:

(i) project governance,

(ii) design and build of platforms,

(iii) the adequacy of available capabilities both within the public sector and externally, and,

(iv) procurement of digital services and equipment; and

(d) any other related matters.[1]

2.2 The Senate was granted an extension of time for reporting until 26 June 2018.[2]

Overview

2.3 The digital delivery of government services represents a major change in the way government administration has traditionally interacted with citizens. The opportunities provided by the technology are countered by significant challenges.

2.4 This chapter provides the current context for the inquiry, starting with the Gershon Report into the government's delivery of digital services undertaken in 2008, which provided recommendations for a governance framework. The Chapter also covers recent incidents where the government has failed to meet community expectations in undertaking a transformation to digital modes of delivery.

---

1 *Journals of the Senate*, No 54—Wednesday, 16 August 2017, p. 1732–1733.

2 *Journals of the Senate*, No 68—Monday, 13 November 2017, p. 2191; *Journals of the Senate*, No 84—12 February 2018, p. 2666; *Journals of the Senate*, No 95—8 May 2018.

Previous inquiries into government ICT

The Gershon Report

2.5 In April 2008, the Minister for Finance and Deregulation, the Hon. Lindsay Tanner, MP, engaged Sir Peter Gershon CBR FREng to lead an independent review of the Australian Government's use and management of information and communication technology (ICT).[3]

2.6 The key findings of the *Review of the Australian Government's Use of Information and Communication Technology* (the Gershon Report) focussed on issues of governance, capability, ICT spend, skills, data centres and sustainable ICT. The heart of the Gershon Reports's findings was that sub-optimal outcomes for the digital delivery of government services was as a result of weak governance of ICT at a whole-of-government level and very high levels of agency autonomy.

2.7 The Gershon Report noted that sustainable change needed leadership at the top levels to bring about cultural change, and funding of the enablers of change—one such enabler being to identify those with the appropriate level of skills:

> My recommendations involve a major program of both administrative reform of, and cultural change from, a status quo where agency autonomy is a longstanding characteristic of the Australian Public Service. Based on my experience of creating sustainable change in the United Kingdom public sector environment, there are two critical requirements which will determine the success of this reform program: firstly, sustained leadership and drive at Ministerial and top official levels and, secondly, ensuring the enablers of change are properly resourced, not only in funding terms but also with skills of the right calibre.[4]

2.8 At the time the Hon Lindsay Tanner MP said the Gershon Report would provide a new model for the effective and efficient use of ICT within the Australian government, with the rebalancing of the currently highly-decentralised ICT administration in Commonwealth departments and agencies. Minister Tanner also said the focus would be on efficient and effective ICT expenditure and management, and that the government would reduce the number of ICT contractors by 50 per cent phased in over 2009–2011, commenting that ICT Review Teams would work with

---

3 Department of Finance archived record: *Review of the Australian Government's Use of Information and Communication Technology*, by Sir Peter Gershon CBE FREng: https://www.finance.gov.au/archive/publications/ICT-Review/ (accessed on 18 April 2018).

4 Sir Peter Gershon CBE FREng, *Review of the Australian Government's Use of Information and Communication* Technology, August 2008, p. iii–iv. https://www.finance.gov.au/sites/default/files/Review-of-the-Australian-Governments-Use-of-Information-and-Communication-Technology_0.pdf (accessed on 18 April 2018). Sir Peter Gershon is a former Chief Executive of the UK Treasury who undertook a similar review on behalf of the UK government in 2003–2004.

agencies to deliver reductions to agency 'business as usual' (BAU) ICT budgets, saving around $400 million annually once fully implemented.[5]

2.9 The government later extended the timeframe for the reduction of ICT contractors within the Australian Public Service (APS) from two years to three, to allow for the bulk of the reductions to occur after the development of a strategic ICT workforce plan and whole-of-government ICT career pathway.[6]

Audit of Australian Government ICT

2.10 In November 2013, the newly elected Coalition Government initiated an audit across all government departments and agencies focussing on spending, capital expenditure (capex) and outcomes achieved—*Audit of Australian Government ICT*. The audit was in support of the government's *e-Government and Digital Economy* policy agenda.[7] The objectives of the audit were:

- To assess the extent to which the government's investment in ICT, over the last three years (2010–11, 2011–12 and 2012–13), has achieved value for money.
- To make recommendations for improvement, with the aim of optimising outcomes from existing and future investments.[8]

2.11 The Department of Finance contracted a private sector consultant to conduct a desk review of ICT Benchmarking results and other relevant data holdings, and to identify options for government to derive better value for money from its ICT Business as Usual (BAU) spending.

2.12 The audit found that the value for money from BAU investment across the APS as a whole was reasonable, but that there is room for further improvement.[9]

---

5 Alan Coleman, 'Gershon ICT review to be implemented "in full"', *Government News*, 25 November 2009; https://www.governmentnews.com.au/2008/11/gershon-ict-review-to-be-implemented-in-full/ (accessed on 18 April 2018).

6 Department of Finance Archive, *Review of the Government's Use of Information and Communication Technology*, Publication Summary, https://www.finance.gov.au/archive/publications/ICT-Review/ (accessed 18 April 2018).

7 Department of Finance, *Audit of Australian Government ICT Public Report*, December 2014, released under the *Freedom of Information Act 1982*, FOI15/124 Document 1, p. 3, available at: https://www.finance.gov.au/sites/default/files/FOI%2015-124%20Document.pdf (accessed 13 June 2018.

8 Department of Finance, *Audit of Australian Government ICT Public Report*, December 2014, released under the *Freedom of Information Act 1982*, FOI15/124 Document 1, p. 3, available at: https://www.finance.gov.au/sites/default/files/FOI%2015-124%20Document.pdf (accessed 13 June 2018.

9 Department of Finance, *Audit of Australian Government ICT Public Report*, December 2014, released under the *Freedom of Information Act 1982*, FOI15/124 Document 1, pp. 4, 5, available at: https://www.finance.gov.au/sites/default/files/FOI%2015-124%20Document.pdf (accessed 13 June 2018.

2.13 The audit also involved a review of the status and outcomes of 31 major ICT-enabled projects underway during the past three years and that met the ICT Two Pass Review process criteria. These projects included 23 projects underway at the time of the audit, and eight completed projects.

- The audit analysis indicated that the majority of the 31 projects reviewed generally had appropriate governance and risk management mechanisms in place, but that there was scope for improvement in monitoring and tracking benefits, particularly during and after project implementation.
- There was concern that workforce issues such as skills shortages could pose risk to project delivery, and that agencies needed to more proactive in managing resources, and to take a more critical approach when analysing and treating workforce risk. Managing workforce risk at a whole-of-government level, as well as at agency level, would likely lead to better project outcomes.[10]

2.14 The audit noted the APS's adoption of digital channels had seen strong growth in online and mobile services. Over the period of this analysis, the APS had substantially increased the range and penetration of online services to customers, all of which were supported by BAU investment.

The history of the Digital Transformation Agency

The Digital Transformation Office

2.15 On 23 January 2015, a joint statement by the then Prime Minister, Hon. Tony Abbott MP, and the then Minister for Communications, the Hon. Malcolm Turnbull MP announced the establishment of a Digital Transformation Office (DTO) within the Department of Communications so that government services could be delivered digitally:

> The DTO will comprise a small team of developers, designers, researchers and content specialists working across government to develop and coordinate the delivery of digital services. The DTO will operate more like a start-up than a traditional government agency, focussing on end-user needs in developing digital services.[11]

2.16 On becoming Prime Minister in September 2015, Hon Malcolm Turnbull announced that the DTO would be transferred to the Prime Minister and Cabinet portfolio. The Prime Minister, who had secured $255 million to implement an

10 Department of Finance, *Audit of Australian Government ICT Public Report*, December 2014, released under the *Freedom of Information Act 1982*, FOI15/124 Document 1, pp. 4, 6. available at: https://www.finance.gov.au/sites/default/files/FOI%2015-124%20Document.pdf (accessed 13 June 2018.

11 Media Release: Joint Statement the Hon. Tony Abbott, MP, Prime Minister and the Hon Malcolm Turnbull MP, Minister for Communications *Establishment of a Digital Transformation Office*, 23 January 2015, available at: https://www.malcolmturnbull.com.au/media/digital-transformation-office-to-make-it-easier-to-connect (accessed 13 June 2018).

electronic service delivery agenda in the May 2015 budget, drove the establishment of the DTO, which was modelled on the UK's government Digital Service.[12]

The creation of the Digital Transformation Agency

2.17 The DTO was replaced by the Digital Transformation Agency (DTA) in October 2016.

2.18 Unlike the DTO, the DTA was not empowered to act as a start-up. Acting CEO Ms Nerida O'Laughlin explained the difference to this committee in an estimates session in February 2017:[13]

> The DTO was there to be a disruptor, to think about things differently, to go into agencies and challenge them…
>
> It was a confined role to transforming government digital services and service delivery. It was quite a different role to what I see as my role and the broader role of the organisation. Of course when you are going in and trying to disrupt people you get push back. DTO did quite a considerable amount of work, really good work, with departments and agencies around things like exemplar projects, of which they delivered any number. I expect the experience was varied, but in the time I have been in this role I have found strong cooperation across departments and agencies.

2.19 The DTA acquired additional functions. It continued the capability building, design and delivery roles of the former DTO, but the DTA's remit was been significantly broadened to include whole-of-government ICT policy, strategy and procurement, as well as the creation of a new whole-of-government assurance function.[14]

2.20 The DTA's first tasking was to review all significant government ICT projects to provide greater transparency and oversight of the government's $6.2 billion in annual ICT expenditure. The DTA ws expected to bring specific expertise in user centred design, technology and delivery to departments' and agencies' ICT projects, and to provide government with greater assurance that agencies are making the right technology choices. Furthermore, the projects should contribute to its transformation agenda and deliver real benefits.[15]

---

12 Paris Cowan, *Turnbull refuses to let go of DTO Turnbull refuses to let go of DTO: Takes pet agency with him to PM&C*, itnews, 22 September 2015 at 9.35 AM, available at: https://www.itnews.com.au/news/turnbull-refuses-to-let-go-of-dto-409453 (accessed 13 June 2018).

13 Ms Nerida O'Loughlin, Interim Chief Executive Officer, Digital Transformation Agency, *Official Estimates Hansard*, Monday 27 February 2017, pp. 194-195.

14 Ms Nerida O'Loughlin, Interim Chief Executive Officer, Digital Transformation Agency, *Official Estimates Hansard*, Monday 27 February 2017, p. 184.

15 Dr Steven Kennedy, Deputy Secretary, Innovation and Transformation, Department of the Prime Minister and Cabinet, *Official Estimates Hansard*, 27 February 2017, p. 185.

The DTA's current role

2.21 At the committee hearing in Canberra on 21 March 2018, Dr Lesley Seebeck, Chief Investment and Advisory Officer, Digital Investment Management Office, DTA, advised the committee that the DTA has an oversight and advisory role. It has oversight of all ICT projects worth greater than $10 million that are either being developed, or that are going through a significant transition, or that provide a service that affects a significant number of Australians. The DTA will also become involved where it has been specifically asked to help build capability. Dr Seebeck stated that the DTA does not get involved with everyday expenditure and resourcing of ICT operations across government, including outages:

> We see these as matters before business owners. Similarly, with the delivery of projects, we're there to assist, help and guide, but essentially, accountability lies with the agencies themselves.[16]

2.22 At the hearing in Canberra on 7 May 2018, the DTA further clarified its role. Dr Seebeck advised the committee of the transfer of the DTA's internal cyber security team to ACSC as part of the government's machinery of government changes. The DTA's role in cyber security will be to ensure departments' and agencies' project proposals take account of good cyber security practices.[17]

2.23 Dr Seebeck further advised that the DTA has no formal interface between the DTA and the Office of the Australian Information Commissioner, and similarly the DTA has no role in data policy or in access to government data.[18] Mr Peter Alexander, Chief Digital Officer, DTA, advised that the DTA's interest in data is in its management of the government's data sharing website, data.gov.au, and in looking at how data can better serve citizens and business.[19] Dr Seebeck advised one of the key elements of the DTA is the focus on user centredness, 'which is traditionally not the way government has tended to operate'.[20] Mr Alexander stated:

> Going to your question, and building on Dr Seeback's point, we are absolutely focused on users of government services; that is kind of the mission of the Digital Transformation Agency. And it really is the mission of digital transformation to think about the end user of a particular service. That is the purpose of government—to serve the people of Australia, to serve the businesses of Australia, to defend Australia, to protect our borders

16 Dr Lesley Seebeck, Chief Investment Officer and Advisory Officer, Digital Investment Management Office, Digital Transformation Agency, *Committee Hansard*, 23 March 2018, p. 9.

17 Dr Lesley Seebeck, Chief Investment Officer and Advisory Officer, Digital Investment Management Office, Digital Transformation Agency, *Committee Hansard*, 7 May 2018, p. 4.

18 Dr Lesley Seebeck, Chief Investment Officer and Advisory Officer, Digital Investment Management Office, Digital Transformation Agency, *Committee Hansard*, 7 May 2018, p. 4.

19 Mr Peter Alexander, Chief Digital Officer, Digital Transformation Agency, *Committee Hansard*, 7 May 2018, p. 5.

20 Dr Lesley Seebeck, Chief Investment Officer and Advisory Officer, Digital Investment Management Office, Digital Transformation Agency, *Committee Hansard*, 7 May 2018, p. 5.

> or whatever it might be…So our strategic input and our engagement with agencies is to have them think about the way they are doing their business and to guide them, build their skills and partner with them…
>
> To build on the [DTA CEO's] earlier point about platforms: we are thinking about the way we deliver, duplication across agencies and how we make space for better transformative thinking by taking away some of the more operational business of government. Platforms around identity, around notifications—things we do in our service delivery space. Payments—regularly. How do we build those into a common platform so that agencies then can build excellence in their services and transform them to solve the problems of their users rather the problems of the structure of government? We are doing a lot of work in that space with all the big service delivery agencies and exemplars with lots of smaller agencies as well. So we're absolutely in that strategic space. That guides the work we do. We apply security as built-in practice. The way we use data and the way we apply privacy principles is absolutely core to that.[21]

2.24 Mr Randall Brugeaud, Acting Chief Executive Officer, DTA, advised the committee that its role has evolved to be more expansive than that originally envisaged for the DTO:

> I would say that the accountabilities of the DTA are actually broader than those of the original DTO. Given the recent machinery of government changes, the DTA now has accountability for a range of capability programs, entry level programs and mentoring. It also now has accountability for whole of government coordinated procurement—administration of existing panel arrangements to move to a more strategic and consolidated footing. Investment management and providing advice on these major programs is also an important role for the DTA. The traditional digital delivery, the platforms, and doing common things in common ways and providing those central platforms for government, are still within the set of accountabilities that sit with the DTA.[22]

Leadership

2.25 The digital transformation portfolio has gone through a number of changes in responsibility.

2.26 Senator the Hon Mitch Fifield was the Minister Assisting the Prime Minister for Digital Government from 21 September 2015 until 18 February 2016. He was replaced by Hon Angus Taylor MP, as the Assistant Minister for Cities and Digital Transformation from 19 February 2016 until 20 December 2017. He was replaced by the now incumbent Hon Michael Keenan MP, the Minister Assisting the Prime Minister for Digital Transformation on 20 December 2017.

---

21 Mr Peter Alexander, Chief Digital Officer, Digital Transformation Agency, *Committee Hansard,* 7 May 2018, p. 6.

22 Mr Randall Brugeaud, Acting Chief Executive Officer, Digital Transformation Agency, *Committee Hansard*, 7 May 2018, p. 5.

2.27 The DTO/DTA has also undergone significant leadership turnover. Mr David Hazelhurst served as interim CEO of the DTO from its creation until July 2015. Mr Paul Shetler, previously the head of Britain's Government Digital Service, was head hunted by Mr Turnbull in his previous capacity as Minister for Communications to act as CEO of the DTO. Mr Shetler commenced his role with the DTO in July 2015, but resigned shortly after being demoted to the role of Chief Digital Officer when the DTO was replaced by the DTA.[23]

2.28 Ms Nerida O'Loughlin, a career public servant, replaced Mr Shetler as CEO of the revamped DTA.[24] On 5 April 2017, the Assistant Minister for Cities and Digital Transformation, Hon Angus Taylor MP announced the appointment of Mr Gavin Slater, as the new CEO of the DTA. Mr Slater was previously a member of the Group Executive Team of the National Australia Bank (NAB) responsible for digital transformation across the NAB's customer service businesses. Mr Slater replaced Ms O'Loughlin.[25]

2.29 On 22 June 2018, Mr Slater announced that he would be stepping down at the end of the month after less than a year and half in the role. He will be replaced by Mr Randall Brugeaud. Mr Brugeaud is currently the Chief Operating Officer of the Australian Bureau of Statistics. He served as acting CEO of the DTA for a period earlier this year when Mr Slater took leave to undertake a management course at Harvard.

Recent Incidents

2.30 The current inquiry has arisen in response to a number of serious incidents where different government departments and agencies have suffered significant failures in their ICT systems which have had a direct and detrimental impact on the Australian public.

2.31 Though diverse in their nature, the incidents all have in common underlying infrastructure and design fragility of their digital systems. These failures have the potential to cause harm to individuals as well as to undermine the public's trust in the Australian government's capacity to transition to a digital administration and economy.

---

23 Jenny Wiggins, *Why Malcolm Turnbull's digital transformation guru Paul Shetler had to quit*, Australian Financial Review, 27 January 2017 at 4.00PM, available at: http://www.afr.com/business/turnbulls-digital-public-service-appointee-paul-shetler-on-what-went-wrong-20170124-gtxhjd (accessed on 13 June 2018).

24 Noel Towell, *Digital Transformation Agency boss Paul Shetler resigns*, 20 November 2016, 7.16 pm, available at: https://www.smh.com.au/public-service/digital-transformation-agency-boss-paul-shetler-resigns-20161130-gt0tot.html (accessed on 13 June 2018).

25 Department of the Prime Minister and Canbinet, *Appointment of CEO of the Digital Transformation Agency*, media release, 5 April 2017, available at: https://ministers.pmc.gov.au/taylor/2017/appointment-ceo-digital-transformation-agency (accessed 14 June 2018).

2.32 The following is a brief summation of four case studies and other incidents. The case studies are examined more fully in Chapter 4.

Australian Taxation Office 'outages'

2.33 In December 2016 and February 2017, the Australian Taxation Office (ATO) experienced a series of 'unplanned systems outages' due to hardware failure of its Storage Array Network (SAN).[26]

2.34 In mid-2017, the Australian National Audit Office (ANAO) undertook a performance review of the ATO. The ANAO found that the ATO's responses to the system failures and unscheduled outages were largely effective, this being despite inadequacies in the ATO's business continuity management planning relating to critical infrastructure.

2.35 The ANAO found that the ATO does not have service commitments specifically relating to the availability of ICT systems but does specify system outage tolerances in its major contracts with ICT service providers. To monitor the impact of ICT service outages on satisfaction with its services, the ANAO recommended the ATO develop service standards that are aligned with system outage tolerances in its contracts with ICT service providers.[27]

Department of Human Service—'robo-debt'

2.36 In July 2016 the Department of Human Services' (DHS) Online Compliance Intervention (OCI) program experienced significant public criticism when welfare debt recovery letters based on data matched and data mined information provided by the ATO were automatically generated (colloquially called 'robo-debt').[28]

2.37 This incident was subject to two separate inquiries. In June 2017, the Senate Community Affairs References Committee published a report, *Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative*. The wide-ranging report resulted in 21 separate recommendations for the better management of the debt recovery processes. The Senate committee's central finding was that the OCI program's design

26 Australian Taxation Office, *Submission 9*, pp. 3 and 5; Community and Public Sector Union (PSU Group), *Submission 16*, p. 13.

27 Australian National Audit Office Report No 29 of 2017–2018, 20 February 2018, pp. 7–8, https://www.anao.gov.au/work/performance-audit/unscheduled-taxation-system-outages (accessed on 18 April 2018).

28 Department of Human Services, *Submission 13*, p. 12; Commonwealth Ombudsman, *Centrelink's automated debt raising and recovery system*, Report No 02/2017, April 2017 *Submission 12*, p. 1; Community and Public Sector Union (PSU Group), *Submission 16*, p. 15.

was flawed by a fundamental lack of procedural fairness, a flaw which filtered throughout the OCI debt recovery process.[29]

2.38 In April 2017, the Commonwealth Ombudsman published its report into the robo-debt incident. The Commonwealth Ombudsman found the OCI to be a complex automated system, the design and implementation of which failed to sufficiently mitigate risk by involving customers and external stakeholders in the design and testing stages.[30] Similar to the Senate committee's findings, the Commonwealth Ombudsman noted the requirement that automated decision making systems be consistent with the administrative law values of lawfulness, fairness, rationality, openness, transparency and efficiency, as set out in the Australian Government, *Better Practice Guide on Automated Assistance in Administrative Decision-Making* (February 2007).[31]

Department of Human Service's—'sale of Medicare card numbers on the darkweb'

2.39 On 4 July 2017 *The Guardian Australia* reported that a darknet trader had been selling Medicare patient's card details 'on request', and had sold at least 75 records since October 2016 by 'exploiting a vulnerability' in the government system.[32] Medicare cards have a primary function of being a means to claim medical benefits. However, Medicare card numbers have a secondary function as one form of proof of identity under the Document Verification Service scheme adopted by the

29 Senate Community Affairs References Committee, *Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative*, June 2017, p.119, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Community_Affairs/SocialWelfareSystem/Report (accessed on 18 April 2018).

30 Commonwealth Ombudsman, Centrelink's automated debt raising and recovery system: A Report About the Department of Human Services Online Compliance Intervention System for Debt Raising and Recovery, April 2017, http://www.ombudsman.gov.au/__data/assets/pdf_file/0022/43528/Report-Centrelinks-automated-debt-raising-and-recovery-system-April-2017.pdf (accessed on 18 April 2018).

31 Australian Government, Better Practice Guide on Automated Assistance in Administrative Decision-Making (February 2007), https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf (accessed on 7 May 2018).

32 Paul Farrell, *'The Medicare machine: patient details of "any Australian" sold on darknet', The Guardian Australia*, https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet, (accessed 15 August 2017). The 'darknet' is the World Wide Web content that exists on overlay networks which use the internet, but which require specific software configurations or authorisations to access. Due to the high level of encryption websites are not able to track the location and IP of the users, just as the users are not able to get this information about the host. The regular internet is called the 'clearnet' because it does not use encryption.

Australian Government to combat financial fraud. The Medicare card is accepted as one form of proof identity, and can therefore be a means of appropriating identity. [33]

2.40 On 9 August 2017, the Senate Finance and Public Administration References Committee referred the issue of the compromised Medicare card incident for inquiry and report by 16 October 2017. The committee remarked that it was concerned that the Medicare card numbers security breach came to light through a media organisation investigation rather than the department, and that DHS had failed to promptly notify affected individuals once the breach had been identified. The committee did not comment further in light of DHS's referral of the security breach to the Australian Federal Police.[34]

2.41 The issue of potential identity fraud arising from stolen Medicare card numbers had previously been raised at the Senate Community Affairs Legislation Committee's Senate Estimates hearing on 22 October 2015.[35] At the hearing the DHS confirmed 369 instances of possible identity theft from individuals; a small number of instances arose in 2014, with the remainder occurring progressively over the first half of 2015.

2.42 On 10 July 2017, Dr Peter Shergold, a former Secretary at the Department of the Prime Minister and Cabinet, led an independent review to examine access by health professionals to Medicare card numbers by using the Health Professional Online Services system or by telephoning DHS. The review found that while there had been no risk to patients' health records as a result of the reported sale of the Medicare card numbers, it noted that inappropriate access to Medicare card numbers might reduce public confidence in the security of government information holdings, such as the My Health Record system.[36]

---

33 The Document Verification Service (DVS), managed by the Department of Home Affairs, is a system that allows organisations, including businesses with a reasonable need to use a government identifier, to take information from a person's identity document with the person's consent, and compare that record against the corresponding record of the document's sponsoring agency. The checks are conducted in real-time to inform decisions that rely on the confirmation of a person's identity. The DVS is a key tool for organisations that are seeking to prevent dealings with any person who may be using fraudulent identities.
See: https://www.dvs.gov.au/How-the-DVS-works/Pages/default.aspx (accessed on 31 May 2018).

34 Senate Finance and Public Administration References Committee, *Circumstances in which Australian's personal Medicare information has been compromised and made available for sale illegally on the 'dark web'*, October 2017, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/medicareinformation/Report,

35 Community Affairs Legislation Committee, *Proof Committee Hansard*, Estimates, 22 October 2015, pp. 108–110.

36 Professor Peter Shergold AC, *Final Report: Independent Review of Health Provider's Access to Medicare Card Numbers, September 2014*, p. 2. https://www.humanservices.gov.au/organisations/health-professionals/subjects/independent-review-health-providers-access-medicare-card-numbers (accessed on 31 May 2018).

2.43 The review made 14 recommendations for immediate practical improvements to the security of Medicare card numbers. The report noted that because the Medicare card can be used to help verify an identity, it is therefore susceptible to theft for identity fraud and other illicit activities. Illegally obtained Medicare card numbers could also potentially be used for fraudulent Medicare claims or to enable ineligible individuals to access Medicare funded health services.[37]

Department of Human Services—child support replacement system

2.44 In 2013, the government began the process to replace the ageing child support IT system known as Cuba. This system processes payments of '$3.5 billion from separated parents to financially support the welfare of over 1.2 million children'.[38] From the very start of this process, a number of flags were raised, with concerns about the adequacy of the tendering process and whether sufficient time was being allocated to build the replacement system and migrate customer information.

2.45 The delivery date of mid-2016 passed with the replacement known as PLUTO not complete. Finally, the project was delivered in mid-2017; however, a significant number of faults were identified with the new system. In early 2018, the Community Affairs Committee were told that although PLUTO was now operational, a significant number of functions were still being undertaken in the old Cuba system. The effect being that some information was being entered twice. Instead of a new replacement system, it appears that DHS has ended up with a hybrid system that has created more work for staff and is less reliable than the original system.

Australian National Audit Office Cyber Security Follow-up Report.

2.46 In June 2014, the ANAO Report No. 50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems* was tabled in Parliament. The report examined seven Australian Government entities' and their implementation of the mandatory strategies in the Australian Government Information Security Manual (Top Four mitigation strategies). The Top Four mitigation strategies are:

- application whitelisting: designed to protect against unauthorised and malicious programs executing on a computer. This strategy aims to ensure that only specifically selected programs can be executed;
- patching applications: applying patches to applications and devices to ensure the security of systems;
- patching operating systems: deploying critical security patching to operating systems to mitigate extreme risk vulnerabilities; and
- minimising administrative privileges: restricting administrative privileges provides an environment that is more stable, predictable, and easier to

37 Professor Peter Shergold AC, *Final Report: Independent Review of Health Provider's Access to Medicare Card Numbers, September 2014*, p. 10. https://www.humanservices.gov.au/organisations/health-professionals/subjects/independent-review-health-providers-access-medicare-card-numbers (accessed on 31 May 2018).

38 Department of Human Services, *Submission 13*, p. 14.

administer and support as fewer users can make changes to their operating environment.[39]

2.47 The audit found that none of the seven entities was compliant with the Top Four risk mitigation strategies and none was expected to achieve compliance by the Australian Government's target date of 30 June 2014.[40]

2.48 On 24 October 2014, the Parliamentary Joint Committee of Public Accounts and Audit held a public hearing to examine Report No. 50. Three of the seven audited entities—the ATO, DHS, and the Department of Home Affairs (Home Affairs[41])—appeared before the hearing to explain their plans and timetables to achieve compliance with the 'Top Four' mitigation strategies. Each of these major Australian Government agencies are significant users of technology. All three agencies collect, store and use data, including national security data and personally identifiable information that can be used to identify, contact, or locate an individual such as date of birth, bank account details, driver's licence number, tax file number and biometric data. [42]

2.49 Each of the three agencies gave assurances to the Joint Committee of Public Accounts and Audit that compliance with the Top Four mitigation strategies would be achieved during 2016.[43]

2.50 The ANAO assessed that, of the three entities, only DHS was compliant with the Top Four mitigation strategies. DHS also accurately self-assessed its compliance against the Top Four mitigation strategies and met its commitment to the Joint Committee of Public Accounts and Audit of achieving compliance during 2016.[44]

2.51 Similarly, of the three agencies, only DHS was classed as cyber resilient. Cyber resilience is the ability to continue providing services while deterring and

---

39 Australian National Audit Officer Report, *Cyber Attack: Cyber Attacks: Securing Agencies' ICT System*, ANAO Report No. 50 2013–14, published on 24 June 2014, p. 14. https://www.anao.gov.au/sites/g/files/net4181/f/AuditReport_2013-2014_50.pdf

40 Australian National Audit Officer Report, *Cyber Attack: Cyber Attacks: Securing Agencies' ICT System*, ANAO Report No. 50 2013–14, published on 24 June 2014, p. 17. https://www.anao.gov.au/sites/g/files/net4181/f/AuditReport_2013-2014_50.pdf

41 Formerly the Australian Customs and Border Protection Service which became part of the Department of Immigration and Border Protection.

42 Joint Committee of Public Accounts and Audits, *Review of the Auditor-General's reports Nos 42, 43, 48, 50 and 52, (2013–14), Official Committee Hansard*, 24 October 2014, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/Review_of_Auditor-Generals_Reports_32-54_2013-14 (accessed 4 June 2018).

43 Joint Committee of Public Accounts and Audits, *Review of the Auditor-General's reports Nos 42, 43, 48, 50 and 52, (2013–14)*, pp. 14–23, *Official Committee Hansard*, 24 October 2014, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/Review_of_Auditor-Generals_Reports_32-54_2013-14 (accessed 4 June 2018).

44 The Auditor General, ANAO Report No 42 2016–2017, *Cyber Security Follow-up Audit*, pp. 7–8, https://www.anao.gov.au/sites/g/files/net4181/f/ANAO_Report_2016-2017_42.pdf (accessed on 19 April 2018).

responding to cyber-attacks. Cyber resilience also reduces the likelihood of successful cyber- attacks. To progress to being cyber resilient, the ANAO found that both the ATO and Home Affairs needed to improve their governance arrangements and prioritise cybersecurity. [45]

Australian Bureau of Statistics eCensus denial of service

2.52 On 9 August 2016, the Australian Bureau of Statistics (ABS) closed the 2016 *Australian Census of Population and Housing (eCensus)* form to new submissions by the public due to four separate instances of distributed denial of service resulting from a failed geoblocking strategy.[46] The Office of the Cyber Security Special Adviser (OCSSA) published a report on the cyber security issues arising from the e-census cyber incident. The executive summary made the following observation:

> The Australian Government's new paradigm of online engagement and services for Australians is not coming. It's already here.
>
> Government's response to the eCensus events of 9 August 2016 provides an opportunity to change the conversation about cyber security: to one of trust and confidence in the government's digital transformation agenda, where 'digital first' is the overwhelming preference for Australians, underpinned by tangible security and adherence to privacy.
>
> The 2016 eCensus tells us that more of the same is not enough: there is a new imperative to embrace cyber security as a core platform for digital transformation. And when we make the necessary changes we will increase the chance to deliver on the promise of Australia's Cyber Security Strategy, to strengthen trust online and better realise Australia's digital potential.[47]

Department of Home Affairs

2.53 In November 2014, Home Affairs inadvertently published a database containing detailed sensitive personal information of approximately 10 000 asylum seekers on its website, where it remained publicly available for eight days. The

---

45 The Auditor General, ANAO Report No 42 2016–2017, *Cyber Security Follow-up Audit*, pp. 7–8, https://www.anao.gov.au/sites/g/files/net4181/f/ANAO_Report_2016-2017_42.pdf (accessed on 19 April 2018).

46 Special Adviser to the Prime Minister on Cyber Security, (now the National Cyber Security Adviser) *Review of the Events Surrounding the 2016 eCensus: Improving Institutional cyber security culture and practices across the Australian Government*, 13 October 2016, p. 3, http://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5/upload_pdf/Review%20of%20the%202016%20eCensus%20-%20final%20report.pdf;fileType=application%2Fpdf#search=%22publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5%22 (accessed on 10 October 2017).

47 Office of the Cyber Security Special Adviser, (now the National Cyber Security Adviser) *Review of the Events Surrounding the 2016 eCensus*, at p. 3, http://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5/upload_pdf/Review%20of%20the%202016%20eCensus%20-%20final%20report.pdf;fileType=application%2Fpdf#search=%22publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5%22 (accessed on 19 April 2018).

privacy breach has resulted in ongoing litigation which to date has cost the government approximately $1 million in legal fees.[48]

The NAPLAN online failure

2.54 NAPLAN is an annual assessment for all students in years three, five, seven and nine. It tests the types of skills that are essential for every child to progress through school and life. The tests cover skills in reading, writing, spelling, grammar and punctuation, and numeracy. The assessments are undertaken every year in the second full week in May. Federal, state and territory education ministers had agreed that NAPLAN will move online over a two-three year period. This means moving NAPLAN from the current paper-based tests to computer-based assessments.[49]

2.55 The NAPLAN online tests were recently undertaken by approximately 200 000 students in New South Wales. At their first NAPLAN online test year 5 students at Annandale North Public School found the [undo] button didn't work, and that one of their group was initially unable to log on and was still completing the test when others students had completed the test. Also, some students' headphones didn't work on the school-issued laptops or in the test.

2.56 A trial of the online tests was initially planned for 2017. The trial was abandoned by all states and territories due to technical issues, including power failures, browser issues, freezes and broken internet connections. [50]

The Australian Apprenticeship Management System

2.57 On 18 May 2018, the Department of Education and Training notified the public that it had ceased work on the Australian Apprenticeship Management System (AAMS) project. The project was intended to deliver a new ICT system to replace the current Training and Youth Internet Management System (TYIMS) which supports Australian Apprenticeships. The departmental statement advised that work had ceased on the AAMS project rather than continue to invest in a system which ultimately may

---

48 Office of Australian Information Commissioner, *Department of Immigration and Border Protection unlawfully disclosed personal information of asylum seekers*, Media Release, 12 November 2014, https://www.oiac.gov.au/media-and-speeches/media-releases/dibp-unlawfully-disclosed-personal-information-of-asylum-seekers (accessed on 9 October 2017); ABC News, *Immigration Department's asylum seeker data breach costs taxpayers nearly $1m in legal fees*, 13 July 2017, http://www.abc.net.au/news/2017-07-13/asylum-seeker-data-breach-costs-$1-million-in-legal-fees/8705326 (accessed on 10 October 2017).

49 NAPLAN National Assessment Program, available at: https://www.nap.edu.au/home (accessed 15 June 2018).

50 Pallavi Singhai, *First NAPLAN online test brings nerves and some technical glitches*, Sydney Morning Herald, 15 May 2018, available at: https://www.smh.com.au/education/first-naplan-online-test-brings-nerves-and-some-technical-glitches-20180515-p4zfem.html (accessed 14 June 2018).

not have met the current business needs or future requirements of Australia's apprenticeship and traineeship system.[51]

2.58 An amount of $20 million has been spent so for on the AAMS with no outcome. The project has been discontinued. The AAMS is in the DTA's 'engaged category' but because the DTA's role is confined to oversight, it has not involved itself ascertaining why the sponsoring department had determined not to proceed with the project or continue to investment in something that was not 'fit for purpose', despite the DTA's role in to ensure effective ICT investment.

2.59 The DTA did not appear to be aware to whom it should be reporting, its accountability mechanisms, or its formal reporting obligations. The DTA maintained that accountability for the AAMS rested solely with the Department of Education and Training, not the DTA.[52]

The Biometric Identification Services Project

2.60 In 2016 a Biometric Identification Services project was established by the Australian Criminal Intelligence Commission (ACIC) to replace the national automated fingerprint identification system, as well as adding facial recognition, palm prints and foot prints capability.[53] The ACIC contracted NEC Australia to deliver the project at a budgeted $52 million, It appears costs have blown out to more than $100 million.[54]

2.61 A PriceWaterhouseCoopers report in late 2017 recommended the NEC Australian contract be overhauled, the project simplified and the timeline for delivery changed:

> There is a low confidence in likelihood of delivery, which requires focus to achieve turnaround.
>
> Poor communications, operational silos, limited collaboration and a failure to estimate the project's complexity had blown it off-track.[55]

---

51 Department of Education and Trainng, Departmental statement on AAMS project closure. 18 May 2018, available at: https://www.education.gov.au/departmental-statement-aams-project-closure (accessed 15 June 2018).

52 Finance and Public Administration Legislation Committee, *Senate Estimates Hansard*, 21 May 2018, pp. 101–110.

53 Sally Whyte, Chaos at bungled biometric identity project as costs, timeframe blow out¸ Canberra Times, 13 June 2018, available at: https://www.canberratimes.com.au/politics/federal/chaos-at-bungled-biometric-identity-project-as-costs-timeframe-blow-out-20180613-p4zl8k.html (accessed 5 June 2018).

54 Denham Sadler, *NEC staff walked from identity gig*, *InnovationsAus*, 12 June 2018, available at: https://www.innovationaus.com/2018/06/NEC-staff-walked-from-gig (accessed on 13 June 2018).

55 Sally Whyte, Chaos at bungled biometric identity project as costs, timeframe blow out¸ Canberra Times, 13 June 2018, available at: https://www.canberratimes.com.au/politics/federal/chaos-at-bungled-biometric-identity-project-as-costs-timeframe-blow-out-20180613-p4zl8k.html (accessed 5 June 2018).

2.62 In June 2018 the ACIC suspended the project. NECAustralia was also the contractor for the failed AAMS system recently cancelled by the Department of Education and Training.[56]

2.63 In parallel with the ACIC biometrics project, the May 2018 budget allocated $92.4 million to the DTA for the next phase of the Govpass digital identity system.[57] Govpass is being developed by the DTA with the purpose of creating a digital identity for Australian citizens that is recognised and trusted by online government services. The benefit of this digital identity is that it gives more Australians the option to complete their government business online, rather than visiting a shopfront.[58]

2.64 The DTA has declined to comment on how the ACIC's biometric capabilities project aligns with the DTA's own verification services project. Nor is it clear how the ACIC and DTA's projects fit with the proposed Home Affairs hub allowing the exchange of biometric data between jurisdictions.[59]

56 Sally Whyte, Chaos at bungled biometric identity project as costs, timeframe blow out¸ Canberra Times, 13 June 2018, available at: https://www.canberratimes.com.au/politics/federal/chaos-at-bungled-biometric-identity-project-as-costs-timeframe-blow-out-20180613-p4zl8k.html (accessed 5 June 2018).

57 Denham Sadler, *NEC staff walked from identity gig*, *InnovationsAus*, 12 June 2018, available at: https://www.innovationaus.com/2018/06/NEC-staff-walked-from-gig (accessed on 13 June 2018).

58 Australian Public Service Commission, Govpass - your digital identity for government services, available at: https://www.apsc.gov.au/govpass-your-digital-identity-government-services (accessed 15 June 2018).

59 Denham Sadler, *NEC staff walked from identity gig*, *InnovationsAus*, 12 June 2018, available at: https://www.innovationaus.com/2018/06/NEC-staff-walked-from-gig (accessed on 13 June 2018).