

IN THE ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA

ART 2025/4916

BETWEEN

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

AFFIDAVIT

On 25 May 2026 I, Garrett McDonald of 134 Reed Street, Greenway 2900 in the Australian Capital Territory, General Manager, Cyber Security at Services Australia, affirm:

1. I am the Chief Information Security Officer (**CISO**) and General Manager, Cyber Security **Division** of Services Australia (**the Agency**). I have been in that role since 22 July 2024.

PART I PURPOSE OF THIS AFFIDAVIT

2. I am informed by Australian Government Solicitor (**AGS**) lawyers and believe that the Tribunal review concerns a challenge by the Applicant to a decision of the Agency dated 6 June 2025.
3. I am informed by AGS that on 3 March 2026, the Applicant revised the scope of his request to confine it to requesting the **source code** of the Android myGov **Code Generator app** that was publicly available at the time of the applicant's original FOI request (**Code Generator app source code**).
4. I make this affidavit to provide evidence relevant to the Agency's exemption claims under sections 33(a)(i) and 47E(d) of the FOI Act.
5. I am authorised to make this affidavit on the Respondent's behalf. I make this affidavit on the basis of my own knowledge, documents lodged in this proceeding and information which has been provided to me by employees of the Agency and AGS. Where I express an opinion, it is based on my background, experience and qualifications as described in this affidavit.

Lodged on behalf of the Respondent

Contact: Jessica Connolly

Prepared by: Jessica Connolly
AGS lawyer within the meaning of s 551 of the *Judiciary Act*
1903

File ref: 25010582
Telephone: 02 6253 7059
Facsimile: 02 6169 3054

Address for Service:
The Australian Government Solicitor
Level 5, 4 National Circuit, BARTON ACT 2600

E-mail: jessica.connolly@ags.gov.au

PART II MY EXPERIENCE AND BACKGROUND

6. I have been employed in the Australian Public Service since 2004 and have been employed at Services Australia (and its predecessors) since 2004. Prior to my employment in this role, I was employed at the Agency (and its predecessors) as General Manager, Chief Data Officer, Data and Analytics Division from March 2021 to July 2024 and General Manager, Experience and Data Services Division from July 2020 to March 2021.
7. I hold a Bachelor of Information Technology and have more than 30 years' experience within the Information Technology industry.
8. I have also held various acting and Senior Executive Service (**SES**) roles with the Agency at the National Manager and General Manager level.
9. In my role as CISO, I am responsible for:
 - 9.1. Protecting the Agency's networks and securing the Agency's data to mitigate current and future cyber security risks. This includes responsibility for the myGov Service and its associated networks and systems, such as the mobile and web-based access and the code generator app(s) (collectively referred to as the **myGov Service**).
 - 9.2. Working with the cyber security community, nationally and internationally, to share information, ensure best practice and enhance cyber security strategies.
 - 9.3. Ensuring compliance with national policy, standards, regulations and legislation.
 - 9.4. Facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives.
 - 9.5. Providing strategic-level guidance for the Agency security program.
10. The Division is responsible for protecting the payments and services the Agency delivers on behalf of the Commonwealth government to the Australian community. It also protects the information systems of our shared services clients, the Department of Veterans' Affairs and the National Disability Insurance Scheme. This includes protecting the Agency's networks and securing the Agency's data to mitigate current and future cyber security risks.
11. Since 2013, I have had a primary role in setting and guiding the architecture, design and implementation of the myGov Service. In my former role as National Manager, Applications Integration Services, I was the technology lead for the design and development of myGov and took myGov from business case through development, production implementation and operation.
12. I had various responsibilities for myGov in my roles as General Manager, Canberra Delivery Centre and General Manager, Experience and Data Services, including:

- 12.1. myGov apps development
- 12.2. moving from the original myGov to myGov 2 which the Respondent implemented in collaboration with the Digital Transformation Agency
- 12.3. developing the Digital Identity Exchange as part of the Digital Identity system, and
- 12.4. the analysis, design and development work that transitioned the platform from myGov 2 to myGov Blue.

PART III INFORMATION SECURITY AND GOVERNANCE IN THE AUSTRALIAN GOVERNMENT

13. The Protective Security Policy Framework (**PSPF**) sets out Australian Government policy across six security domains and prescribes what Australian Government entities must do to protect their people, information, and resources. This includes requirements for the cyber security of information, data, and technology. The PSPF is revised annually and available at: <https://www.protectivesecurity.gov.au/pspf-annual-release>.
14. The PSPF requires entities to authorise systems to operate using a risk-based approach to the implementation of the Australian Signals Directorate's (**ASD's**) Information Security Manual's (**ISM's**) cyber security principles, controls, and guidelines. The ISM is updated from time to time and is available at: <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism>.
15. While a risk-based approach to the implementation is required by the PSPF, a selection of controls is considered mandatory, known colloquially as the 'Essential Eight' (**E8**). The E8 consists of eight prioritised strategies designed to mitigate cyber security incidents and enhance the security posture of organisations. It is divided into tiered 'maturity levels' from Maturity Level 0 (ML0) to ML3.
16. The PSPF requires that entities implement each of the strategies within the E8 to ML2 and consider all remaining strategies within the ISM as required to achieve an acceptable level of residual risk.
17. To achieve compliance with the PSPF, including the implementation of the E8 to ML2 and consideration of the remainder of the ISM, the Agency maintains a suite of cyber security policies that reflects these requirements and ensures responsibility and accountability for delivering the outcomes are clearly assigned.
18. The PSPF also defines the role of the CISO, requiring that they oversee the entity's Cyber Uplift Program and the cyber security of the entity's technology resources. This includes responsibility for the Cyber Security Strategy and Uplift Plan and implementing the ISM and Strategies to Mitigate Cyber Security Incidents, and cyber security risks.
19. To enable the risk-based approach to control selection under the system authorisation capability, the System Authorisation Policy requires that System Owners consider risks

within the context of their system and that the residual risk is within defined tolerance levels to be authorised. This policy is central to the cyber security policy suite and is referenced throughout the suite to ensure that system authorisation is considered as part of policy implementation.

20. To ensure the CISO has the authority as defined within the PSPF and to ensure that cyber security policies are implemented by the organisation, the Agency Security Directive documents the Chief Executive Officer's (**CEO's**) expectations on implementing protective security in the Agency. It sets the strategic direction and outlines the Agency's security governance arrangements including appointing the CISO. The Directive assigns accountabilities and responsibilities for security risk management and implementing protective security controls across the agency.

PART IV MYGOV SERVICE

21. The myGov Service is run by the Agency. The myGov Service comprises the myGov public facing platform and all services, including associated electronic tools including applications such as the Code Generator app.
22. On myGov, users can create an account and link it to various government services of their choice. myGov users can then access those online services using their myGov credentials or their linked Digital Identity, removing the need to have separate accounts and credentials with each individual service. myGov also provides a centralised digital mailbox for participating services to send electronic correspondence to users who have linked their service account to their myGov account.
23. There are now 20 Commonwealth and state services which can be linked to a myGov account.

Annexed hereto and marked '**GM-1**' is the list of services as listed on the following myGov website as at 24 May 2026: <https://my.gov.au/en/about>

24. In January 2023, a panel of independent experts reviewed how well myGov is performing and delivered a myGov User Audit. In the Executive summary of that report, myGov is described as 'critical national infrastructure' (vol 1, page v). Finding 1 of that Audit report is that myGov is indispensable national digital infrastructure (vol 1, page 6).

Annexed hereto and marked '**GM-2**' is the Executive summary and Finding 1 of the 2023 User Audit report as available on the following myGov website as at 24 May 2026: <https://my.gov.au/content/dam/mygov/documents/audit/mygov-useraudit-jan2023-volume1.pdf>

25. A myGov account stores the following personal information of a myGov user:

25.1. email address

25.2. myGov password

- 25.3. myGov preferences
- 25.4. full name
- 25.5. date of birth
- 25.6. myGov inbox messages, which might include payment information, health information, taxable income and postal addresses.
- 25.7. records of activity on myGov, and
- 25.8. user account data, such as myGov customer authentication information which includes:
 - 25.8.1. myGov user ID
 - 25.8.2. email alias for authentication, and
 - 25.8.3. credentials, including:
 - 25.8.3.1. password
 - 25.8.3.2. secret questions and answers
 - 25.8.3.3. mobile number for SMS authentication
 - 25.8.3.4. code generator seed which is a unique value used by the code generator algorithm to generate a security code to be used alongside a password
 - 25.8.3.5. Digital Identity, and
 - 25.8.3.6. Passkey (for example, using a pin number or biometrics to unlock a cryptographic key stored on a device held by the user).

myGov authentication process

- 26. myGov can be accessed on a web browser at the myGov home page or through the myGov app.
- 27. myGov users must authenticate their account in order to access myGov, and its linked services. Authentication is one layer of security that is essential to protecting unauthorised entry into the myGov Service.
- 28. Once authenticated, a user can enter myGov and access their linked member service accounts.
- 29. myGov users authenticate using either single factor (username, password and secret questions and answers) or Multi-Factor Authentication (**MFA**). This is retained to

enable vulnerable Australians who are unable to access MFA options which require ongoing access to a mobile phone. This also supports myGov in meeting the Digital Transformation Agency's Digital Service Standard Criterion 3 which requires that agencies ensure that services are inclusive, accessible and useful for all.

30. After 6 March 2026, myGov users have four options for MFA:
 - 30.1. a password combined with a security code (one time password) sent via SMS to the registered mobile phone number
 - 30.2. a password combined with a security code generated via an authenticator app
 - 30.3. a passkey, or
 - 30.4. a Digital Identity which is part of the Australian Government Digital Identity System (AGDIS) such as the Australian Taxation Office's myID.
31. myGov users who elected to set up multi-factor authentication using the myGov Code Generator app would download and install the Code Generator app and pair it with their myGov account. The Code Generator app could then be used when logging in to myGov.

myGov Code Generator app

32. The myGov Code Generator app was available to download on iOS and Android mobile devices from 6 December 2017 to 6 March 2026. It is no longer available to download to new users.
33. When logging in to myGov, the user would enter their username and password, and a six-digit, time-based one-time password (**TOTP** also known as a **token**) which they generated using the Code Generator app. The TOTP is valid for 30 seconds and therefore considered a 'single use' code that authenticates the user as the owner of the myGov account. Further information about this is in my confidential affidavit.
34. Existing myGov Code Generator app users can continue to use the app however are being encouraged to transition to an alternative authentication method or choose to pair another authenticator with their account. Examples of other authenticator apps that could be used include 'Google Authenticator', Apple's Passwords app and '1Password'. The Agency intends to retire the myGov Code Generator App at some point in the future.
35. In my opinion, the fact that the Code Generator app is to be retired in the future does not eliminate the security risks that would be posed by the release of the source code. Further information about this is in my confidential affidavit.

PART V MYGOV CODE GENERATOR APP SOURCE CODE

What is 'source code'?

36. In general terms, 'source code' is a set of instructions written in a programming language which can be used by a computer to control the operation of a software program. Source code defines how a program or application functions. A description of the Code Generator app source code is contained in my confidential affidavit.
37. Another way of explaining the sensitivity of the Code Generator app source code is to explain it as the blueprint to a secure building. It provides valuable information about how you might break into the building. If a malicious actor has the blueprint, they can identify and exploit access points.
38. Disclosure of the Code Generator app source code would provide a level of information currently not in the public domain about the Code Generator app source code itself, and the myGov Service including the internal systems which need to process the TOTP code as part of authentication.
39. If the Code Generator app source code were disclosed, information within it could be used by malicious actors to identify vulnerabilities within the Code Generator app source code, the myGov Service and possibly the Agency's systems more broadly. By malicious actors, I mean state actors with interests antithetical to Australian interests, organised crime syndicates and hackers, each of which seek to utilise vulnerabilities to gain access to data, including identification information, relating to myGov users.
40. Details within the Code Generator app source code can potentially be used to identify vulnerabilities that could compromise myGov or other systems run by the Agency. This risk is significantly heightened with the introduction of Generative AI, which is increasingly capable of identifying and exploiting vulnerabilities within systems and applications.

PART VI DISCLOSURE OF THE MYGOV CODE GENERATOR SOURCE CODE WOULD, OR COULD REASONABLY BE EXPECTED TO CAUSE DAMAGE TO SECURITY

41. I now describe how access to the Code Generator app source code would, or could reasonably be expected to, cause damage to security.
42. Government digital services and critical infrastructure are priority targets for State-sponsored and State-aligned adversaries, particularly in the context of geopolitical tensions. While direct attribution of cyber activity is complex, public guidance recognises that patterns of behaviour, targeting and timing may indicate activity consistent with state-sponsored and state-aligned adversaries.
43. The Code Generator app source code, if disclosed, can potentially be analysed and used by malicious actors, including State actors, organised criminal syndicates and hackers, to:

- 43.1. Identify possible weaknesses in the algorithm which make it easier to correctly guess a TOTP and gain unauthorised access to a legitimate user's myGov account (particularly in combination with other items of information which may already be known, e.g. an email address).
 - 43.2. Build a counterfeit Code Generator app which legitimate myGov users might use to access their account. A malicious actor could use this process to obtain the TOTP and access the legitimate user's myGov account at the same time, because the TOTP is able to be used more than once for a short period of time. The legitimate user would be unaware, because the Code Generation app would function as expected from their own point of view.
44. In addition, disclosure of the Code Generator app source code could, or may reasonably be expected to:
- 44.1. Provide a window into other source code used in the Agency's digital services, including, importantly, other parts of the myGov Service, such as source code for the main public-facing myGov system.
 - 44.2. Afford greater insight into the threat detection systems and tools the Agency uses and permit malicious actors to use that information to devise ways to avoid detection. As a result, this would enhance the ability for malicious actors to fraudulently obtain access to myGov accounts.
 - 44.3. Facilitate the development or refinement of malicious tools or exploits to compromise myGov which could assist adversaries to bypass existing myGov safeguards or cyber threat detection mechanisms;
45. While it might be speculated that part of (or replica) Code Generator app source code is available in the public domain, for example, in open-source libraries, the actual Code Generator app source code is not in the public domain. Disclosure of the Code Generator app source code would confirm what is presently only the subject of speculation.
46. Additionally, disclosure of the Code Generator app source code may be significant to the application of 'mosaic analysis' which is a method by which an individual or entity can build up a coherent and comprehensive picture from individual pieces of information, including apparently innocuous or meaningless pieces of information. Mosaic analysis can be conducted by a broad range of individuals and entities, with varying degrees of sophistication, acting together or independently. Even where the disclosure of certain pieces of information may not of itself be sufficient to reveal a complete picture (in this case, of the Agency's platforms or the myGov Service), it may contribute to a growing mosaic.

47. Mosaic analysis is similar to putting together a jigsaw puzzle where you start with the edges and then use the image on the box to start putting together pieces that match through trial and error. The risks to the cyber security of a system due to this type of analysis is reinforced by ASD updating the ISM principles in March 2026 to introduce a principle titled 'GOV-10 – System exposure minimisation' which states:

Information about the design, configuration and operation of systems (infrastructure, operating systems, applications and data) is not publicly disclosed or shared externally unless necessary for commercial, legal, regulatory or security purposes, with any disclosure minimised, controlled and logged.

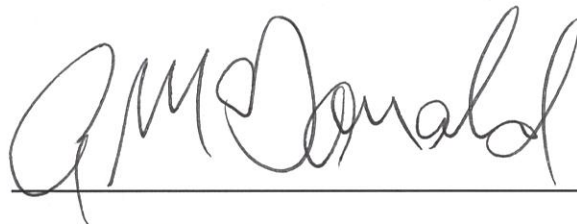
48. Additionally, Artificial Intelligence (AI) materially amplifies the threat landscape facing the Agency by lowering barriers to entry and accelerating the speed, scale, and sophistication of attacks. Threat actors are already using AI to generate highly convincing, phishing which is tailored to the individual recipient at scale; automate reconnaissance and vulnerability discovery; assist live network intrusion and lateral movement; and rapidly analyse stolen data to extract high-value intelligence. AI is also being used to evade traditional detection by dynamically changing attacker behaviour and tool signatures.
49. The emergence of Anthropic's 'Claude Mythos' brings an AI capability that demonstrates the risks AI could have on the security of systems. Anthropic claims Mythos has identified thousands of previously unknown vulnerabilities, including zero-days, across major operating systems, browsers and widely used software platforms. Such AI models could, with a relatively low barrier for entry, take advantage of any released source code to more easily and rapidly identify vulnerabilities in the code and develop working exploits for these vulnerabilities.
50. Once they have obtained access, I believe that a malicious actor may have the necessary information to carry out a range of actions within a myGov account, including for example:
- 50.1. download and view online letters relating to the legitimate user
 - 50.2. view the profile details of the legitimate user, including name, date of birth, address, phone number and email address
 - 50.3. update the personal details within the myGov account to send erroneous address, phone and email changes to linked member services, and
 - 50.4. take, and maintain, control of the myGov account by changing account preferences, changing the password, editing secret questions and answers and updating the associated email and mobile number. As a result, the legitimate user is unable to sign-in to their myGov account.
51. Further, if a malicious actor could gain access to a user's myGov account, they could also access any service linked to the myGov account. Depending on the particular services linked to a myGov account, the malicious actor could gain access to further sensitive and personal information from linked services such as:

- 51.1. customer identification numbers for the relevant linked service
 - 51.2. government payments and services the legitimate user receives, including documentation to support claims for payments or services (such as medical, legal, court and employment records)
 - 51.3. taxation information, including tax file numbers and tax assessment notices
 - 51.4. medical information, including medical imaging or doctors' reports, pathology results, doctors visited, immunisations, prescriptions and Medicare item codes which can identify medical conditions
 - 51.5. financial information, including bank details
 - 51.6. veterans' services information
 - 51.7. welfare information
 - 51.8. child support information.
52. Depending on the particular services linked to a myGov account, the actions a malicious actor could take in a linked service account include:
- 52.1. view and access government payments and services
 - 52.2. view and update sensitive details and personal information, such as contact information, medical details and financial details
 - 52.3. divert government payments intended for the legitimate myGov user to a bank account owned by the malicious actor by changing bank account details, and
 - 52.4. fraudulently apply for government payments or services to which they are not entitled, under cover of the legitimate myGov user's account, such as welfare payments and tax refunds, and have those payments directed to them.
53. National digital services, such as myGov, are targeted in this way because the large majority of Australians interact with government services online through myGov.
54. Given the volume of myGov users supported by the Agency, I believe a cyber attack would have a substantial adverse effect on Australian citizens through access to their personal and sensitive data and would result in substantial disruption to government services. This would in turn will erode public trust and confidence in Services Australia and government services more broadly and undermine the reputation of the Australian Government both nationally and internationally. From my duties and experience as CISO, including as chair and member of various cyber, security and related executive boards as I describe in paragraphs 6-10 in this affidavit, I believe a loss of trust and confidence, and any consequential social disruption to the delivery of essential government services would result in damage.

55. I explain further about other external threats and the activity the Agency currently experiences and how that could damage social cohesion and national security in my confidential affidavit.

PART VII SUBSTANTIAL ADVERSE EFFECT ON AGENCY OPERATIONS

56. If the Code Generator app source code was disclosed, it would require significant additional funding and resourcing to be allocated to maintaining and protecting the security of myGov to what I anticipate would be a significant increase in cyber attacks.
57. This would include redeploying staff from other significant projects to work on responding to cyber attacks which would have a substantial adverse effect on the ability of the Agency to manage, operate and protect myGov and other Government Services.
58. I provide further information about how disclosure of the Code Generator app would result in a substantial adverse effect on the Agency's operations in my confidential affidavit.



Garrett McDonald



Sonya Nordling,
Solicitor in the Australian Capital Territory
Services Australia

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

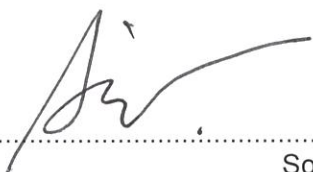
2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE GM-1

The following is the annexure marked GM-1 referred to in the affidavit of Garrett McDonald, affirmed at Canberra on 25 May 2026, before me:

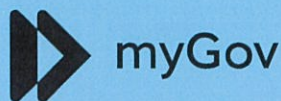

.....
Sonya Nordling
Solicitor in the Australian Capital Territory
Services Australia



Subscribe to get updates and access the 2026 Census through myGov.

[Dismiss](#) ✕

[Learn how to subscribe](#)



Menu ☰

[Home](#) > About myGov

About myGov

myGov is a simple and secure way to access government services online in one place.

On this page

[Access government services](#)

[Explore support](#)

[Give feedback](#)

[Stay connected](#)

[Get community resources](#)

myGov is run by Services Australia.

Access government services

With a myGov account, you can access services from:

- [Apprenticeships Services](#)
- [Australian Bureau of Statistics](#)
- [Australian Taxation Office](#)
- [Centrelink](#)
- [Child Support](#)
- [Department of Health Applications Portal](#)
- [Department of Veterans' Affairs](#)
- [HousingVic Online Services](#)
- [Individual Healthcare Identifiers service](#)
- [Medicare](#)
- [My Aged Care](#)

- [My Health Record](#)
- [National Cancer Screening Register](#)
- [National Disability Insurance Scheme](#)
- [National Redress Scheme](#)
- [State Revenue Office Victoria](#)
- [Unique Student Identifier \(USI\)](#)
- [Victorian Concessions and Allowances](#)
- [Workforce Australia](#)
- [Your Career](#)

You can choose which services you want to link to your myGov account. It also has a secure Inbox where you can get messages from some of your linked services.

You can access your myGov account through [this website](#) or the [myGov app](#).

Create a digital Commonwealth statutory declaration

You can [create a digital Commonwealth statutory declaration through myGov](#) using your Digital ID.

Explore support

You can [browse](#) or [search](#) for information about government payments, services and support on the myGov website without signing in to your account.

Give feedback

You can use our [short survey](#) to help us improve myGov.

Stay connected

Ask us questions and get tips about myGov on our [X](#) and [YouTube](#) social media accounts.

Get community resources

Our eKit helps intermediaries, community and advocacy groups tell people about myGov.

Learn more about our [community resources](#).

Help using myGov

Get help to create a myGov account, download the myGov app, link services and manage your account.



myGov terms of use

By having a myGov account, you agree to be bound by these terms of use.



Privacy and security

Find out what personal information myGov collects and what to do if you think someone is misusing it.



Accessibility

We're committed to providing an accessible and inclusive website anyone can use.



Copyright

If you want to share the content we've created, there are a few rules you need to follow.



Languages

Find information in more languages to help you use myGov services.



Contact myGov or your services

Find contact information if you need help with your myGov account or linked services.



Did you find this page useful?

Yes

No

Page last updated: 6 March 2026

About this site

Browse

About myGov

Raising kids

[Help using myGov](#)[Living arrangements](#)[Contact us](#)[Ageing](#)[Share feedback](#)[Work](#)[myGov User Audit](#)[Education](#)[Health and disability](#)[Terms of use](#)[Privacy and security](#)[Copyright](#)[Accessibility](#)[Languages](#)[Follow us](#)**myGov**

We acknowledge the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

**ADMINISTRATIVE REVIEW TRIBUNAL
MELBOURNE REGISTRY
INTELLIGENCE AND SECURITY JURISDICTIONAL AREA**

2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE GM-2

The following is the annexure marked GM-2 referred to in the affidavit of Garrett McDonald, affirmed at Canberra on 25 May 2026, before me:



.....
Sonya Nordling
Solicitor in the Australian Capital Territory
Services Australia



Critical National Infrastructure myGov User Audit

January 2023

Volume 1: Findings and recommendations

Contents

Definitions and glossary	ii
Foreword	iv
Executive summary	v
Introduction.....	1
Findings.....	6
The Panel's vision for myGov.....	18
Recommendations.....	19
Implementation	34

Attachments

- A Terms of Reference
- B Evolving the user experience
Delivering for government
- C Immediate funding priorities
- D Illustrative myGov performance framework

Definitions and glossary

DEFINITIONS

In this report, these terms are defined as follows:

Term	Definition
Enhanced myGov program	A two-year program established in 2021 to design and deliver an upgraded myGov website and improve usability and functionality.
govCMS	Content management and web hosting for government. Providing consistent tools for government to create and host websites that are secure, modern and accessible to the public.
Hub and spoke model	The term hub and spoke refers to a primary ICT system (such as a main user account) as the 'centralised location' or the 'hub', connecting to other systems to access detailed services via the 'spokes'.
Identity proofing levels (IP1, IP2, IP3)	The strength of a digital identity. A stronger digital identity proofing level requires verification of more identity documents. Basic digital identity – Identity proofing level 1 (IP1, IP1+) Standard digital identity – Identity proofing level 2 (IP2, IP2+) Strong digital identity – Identity proofing level 3 (IP3)
member service	A digital service linked with myGov. As at December 2022, there are 15 member services that can be accessed through myGov: ATO, Centrelink, Child Support, DVA, Health Applications Portal, Housing Victoria, Individual Healthcare Identifier, Jobsearch, Medicare, My Aged Care, My Health Record, National Cancer Screening Register, National Redress Scheme, NDIS, Victoria State Revenue
myGovID	Australian Government identity provider managed and operated by the ATO.
Tell Us Once capability	An optional capability offered through myGov to enable a user to update their personal information once, and have that information updated across all member services linked to their myGov account.

GLOSSARY

ABS	Australian Bureau of Statistics
ACMA	Australian Communication and Media Authority
AEC	Australian Electoral Commission
AGD	Attorney-General's Department
API	application programming interface
APS	Australian Public Service
ATO	Australian Taxation Office
ANAO	Australian National Audit Office
DSS	Department of Social Services
DTA	Digital Transformation Agency
DVA	Department of Veterans' Affairs
GDP	Gross Domestic Product
ICT	information and communications technology
NDIS	National Disability Insurance Scheme
NSW	New South Wales
OECD	Organisation for Economic Co-operation and Development
PORO	Proof of Record Ownership
TDIF	Trusted Digital Identity Framework
UX	User Experience
WA	Western Australia
WCAG	Web Content Accessibility Guidelines

Foreword

The myGov User Audit Expert Panel is pleased to submit our report to government.

The Panel was commissioned in September 2022 to oversee the audit and make recommendations to shape the future direction of myGov. During the course of the audit, two initial improvements were made to the usability of myGov including transitioning to a new, contemporary technology platform and the release of the myGov app in December 2022.

Despite these improvements, over the course of the audit the Panel heard there is a significant opportunity to improve user experience, particularly within the member services linked through myGov, and make myGov a world-class, trusted and citizen-centric digital service delivery platform serving all Australians.

The report is set out in two parts. Volume 1 details the Panel's 10 findings on the current and future state of myGov, and 10 recommendations to government to fulfil myGov's potential.

Volume 2 of the report contains detailed analysis across user experience, functions and performance of myGov, the potential features of a desired future state for myGov to meet the needs and expectations of Australians, and potential actions to get there. Detailed analysis has focused on:

- delivering intuitive, tailored services through myGov
- ensuring no one is left behind in digital service delivery
- keeping people and their information safe
- the requirements for myGov to operate on a modern technology platform
- the governance, accountability and funding arrangements to deliver the future myGov.

In addition to the recommendations made in Volume 1 of the report, Volume 2 provides further guidance government could consider in prioritising delivery of improvements to myGov.

Input from individual users of myGov, peak bodies, industry and all levels of government has informed the Panel's deliberations. The Panel thanks all those who contributed to and engaged with the audit, particularly within short timeframes. The support of the Secretariat is also appreciated.

While there are many issues that can be easily addressed to improve the satisfaction of Australians with myGov, several of the recommendations set out in this report are ambitious and the Panel recognises achieving the vision for myGov will not be easy.

It will require discipline across government to deliver truly connected services for the benefit of Australians, a long-term commitment to invest in myGov as a key piece of national infrastructure and building a foundation of trust in myGov by all Australians.

**David Thodey AO (Chair), Professor Edward Santow, Professor Emily Banks AM,
Commissioner Julie Inman Grant, Amit Singh**

myGov User Audit Panel

Executive summary

myGov is critical national infrastructure.

The nation's energy grid, roads, schools, and hospitals are indispensable to our country and its people. Previous generations built this national infrastructure to be safe, reliable, and readily available to all. We must now do the same for the digital infrastructure that Australians rely on to access government services.

myGov has many strengths and also some serious shortcomings. The right mix of technology, cooperative government arrangements and community protections is required to make myGov the kind of national infrastructure that truly meets the needs of Australians.

Over the last 5 years, the number of myGov users has more than doubled. Australians are conducting up to 1.4 million sessions in myGov each day – more than triple what it was 3 years ago. The proportion of users who are satisfied overall with myGov has improved from 40 to 45%, but this is still too low. myGov provides many tangible benefits for the nation. Australians get better services, saving them time and effort. Taxpayers gain savings which can be applied to creating even better services. The economy benefits from increased productivity. And all Australians benefit from potentially higher levels of cyber security when dealing with government – provided we get the settings right.

Recent improvements in myGov have come on the back of a two-year investment in the Enhanced myGov program. This investment runs out in June 2023.

The Enhanced myGov program has shown what a well-crafted and implemented development program can achieve. Independent economic analysis commissioned by Services Australia estimated that completing the program over 4 years would deliver net benefits of \$3.2 billion over 10 years.

The Enhanced myGov program has put in place much needed building blocks for a better myGov. The new platform is scalable, more secure and more flexible. The user-interface is more intuitive and easier to navigate. The new myGov app is easy to use and provides faster access to services for users.

While positive, these changes fall well short of the long-expressed vision of providing a primary digital front door to government for Australians. They are a starting point. The government has an opportunity to build upon these foundations and provide world-class services for all Australians.

Future development of myGov needs to focus strongly on its users – the Australian people. myGov must be easy to use, secure, leave no one behind and deliver smart, tailored services that meet people's needs. Funding, governance and planning arrangements need to appropriately reflect myGov's role as a critical piece of national digital service delivery infrastructure.

For myGov to develop as it should, behaviours within government also need to change. Too often in the past, myGov development has been hampered by agencies pursuing their own agendas. These separate perspectives are important but should not dominate at the expense of bringing things together for Australians.

As a nation, we have been here before and failed. The promise of myGov has been promoted by government many times in the past. The failure has not been in articulating myGov's promise. It has been in developing and implementing the detailed, long-term plan needed to bring that promise into reality.

The Panel's 10 recommendations represent a blueprint for investing in myGov as critical national infrastructure for all Australians.

Given the importance of myGov and the issues and opportunities we have highlighted, the Panel also encourages the Government to demonstrate its practical commitment by publishing its response to the audit and an implementation plan by 1 July 2023.

Box 1: Summary of recommendations

The Panel's 10 recommendations to Government

1. Confirm myGov as the 'go to' place for people to access services online from the Australian Government and communicate to all Australians.
2. Ensure myGov leaves no one behind and upholds Australians' human rights.
3. Legislate myGov as national service delivery infrastructure.
4. Provide ongoing annual funding of myGov at the same level as sustainment funding in 2021–22 and the Enhanced myGov program and establish a 'myGov development fund' to resource onboarding of new services and improvement of existing linked services.
5. Publish during 2023 a rolling 5-year roadmap for developing myGov, updated annually.
6. Accelerate development of Australia's national digital identity ecosystem, prioritising the protection of security, privacy, safety and other human rights with a view to government digital identity being safe, easy to use and secure.
7. Introduce by mid-2023 citizen-centred governance and operational arrangements for myGov and myGovID to overcome government siloes and drive inclusion and performance.
8. Partner with the states and territories on a five-year plan to make it easy for people to find and do what they need to across all levels of government.
9. Design and build myGov in alignment with a refreshed and enforced Australian Government Architecture, incorporating the Design System and the Service Standard.
10. Services Australia develop and adopt a new world-class approach to service and support to government agencies utilising myGov.

Introduction

WHAT IS MYGOV?

myGov is the government's front door for digital services and supports individuals to access the services of participating government agencies.

Launched in May 2013, it provides Australians with secure online access to a range of government services in one place. myGov operates on a "hub and spoke" model where myGov provides a central secure website and smartphone app for users to access services (the hub) and member services/agencies provide most of the available services through their own digital systems (the spokes). Some services are delivered in the myGov "hub" itself, however, the number of services available in this way is currently limited.

The 15 government services available in myGov

myGov provides access to:

- Australian Taxation Office
- Centrelink
- Child Support
- Department of Health Applications Portal
- Department of Veterans' Affairs
- Housing Victoria Online Services
- Individual Healthcare Identifiers service
- Medicare
- My Aged Care
- My Health Record
- National Cancer Screening Register
- National Disability Insurance Scheme
- National Redress Scheme
- State Revenue Office Victoria
- Workforce Australia

Services Australia leads implementation and delivery of myGov with the DTA having overarching policy responsibility for myGov and digital identity. Over time, myGov has gone from a strategically important ICT system to an indispensable part of the Australian Government service delivery ecosystem. Over its 9 years, myGov has continued to incrementally evolve, introducing new features and services.

For most people, digital services are ubiquitous across all areas of their lives including when interacting with governments. Today, delivering a digital service as good as or better than traditional channels is core business, not an optional extra.

WHERE DID MYGOV COME FROM?

The goal of joined-up online services for citizens is not new. In government, discussions on citizen-centred digital services have been occurring since the 1990s. However, myGov itself did not come into existence until 2013. This was 3 years after the 2010 *Ahead of the Game* report recommended making access to government services more convenient for Australians through automation, integration and better information sharing.

The vision has always been ambitious. Successive governments have promised a central digital entry point, information and services tailored to individual needs, and a way for people to see and manage their affairs with government.

However, until recently, progress has been slow.

When launched, myGov included 1.3 million user accounts (transitioned from australia.gov.au) and 3 Australian Government entities providing 5 member services.

People were able to securely access a range of Australian Government services online, in one place. The services myGov itself provided to Australians were:

- **login** – a single username to access (member) services
- **inbox** – more timely communications from services via a digital mailbox
- **Tell Us Once** – the ability to notify multiple services about changes of details.

Between 2013 and 2020, new services and features were gradually introduced including state and territory government services (August 2016), allowing the use of the myGov login to access agency services directly (October 2017) and introduction of two-factor authentication through the myGov code generator (December 2017). In parallel, myGovID (a digital ID incorporating biometric checks) was launched in October 2019 as the replacement to AUSkey, the authentication tool for businesses used by the Australian Tax Office (ATO). myGovID was integrated into myGov in late 2020 to give users an alternative log in option.

In 2022, the Enhanced myGov program has delivered a step change improvement in the underlying myGov platform, transitioning myGov to new, contemporary technology comprising:

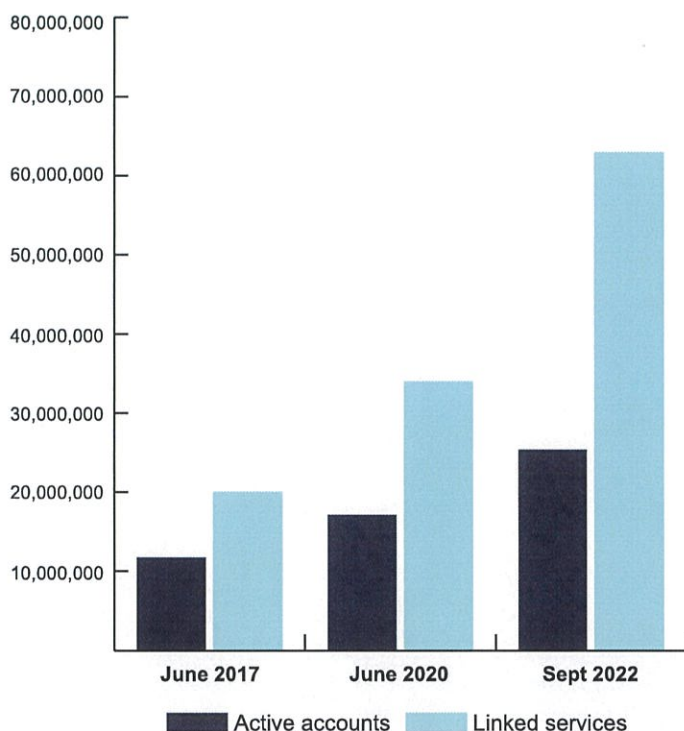
- software and infrastructure, leveraging a combination of public and private cloud hosting to provide high performance, resilience and security
- a microservices architecture based on scalable and flexible APIs
- a Content Management System (CMS) enabling information about services to be published through myGov
- a Digital Experience Platform (DXP) enabling the tailoring of services and information to meet the needs of individuals
- a Customer Journey Analytics tool producing data and insights which can be used to improve services.

The recently released myGov app is also a big step forward. The app delivers functionality and user experience closer to that provided by the private sector including:

- an easy way to login to myGov using the biometrics on a mobile device
- a secure digital wallet
- access to the myGov Inbox
- access to member services without needing to sign in again
- a central list of tasks
- push notifications such as alerts about new messages received in the myGov inbox which include the name of the agency and a short summary.

The growth in usage of myGov is considerable, especially since 2020 when the first wave of the COVID-19 pandemic led to a substantial increase in Australians accessing government services.

Active user accounts and linked services



Active user accounts

The number of active myGov accounts has grown significantly in recent times. Starting from a base of 11.7 million active accounts in June 2017, the number of accounts reached 25 million in September 2022.

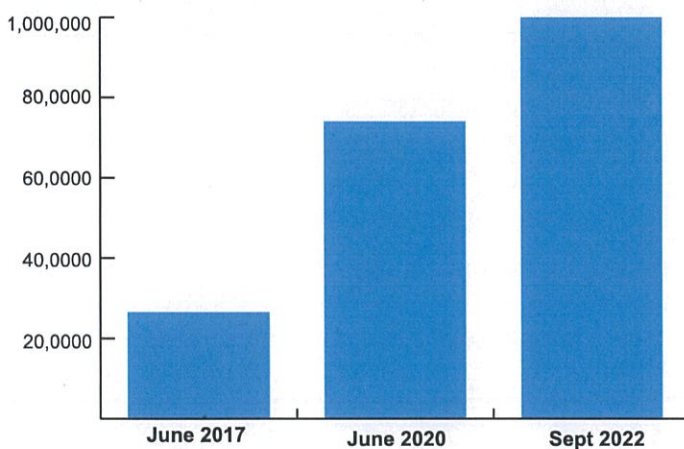
While one person can have multiple accounts, in general terms the number of accounts provides a sense of the scale of individual myGov users.

Linked services

The number of linked services in myGov has equally grown. The base number of 20 million linked services in June 2017 grew to 63 million in September 2022.

This demonstrates that not only the number of users in myGov has grown, but so too has the number of services people are connected to (linking) within myGov. This tells us not only more people are using myGov, but also that they are connecting to more services when they do.

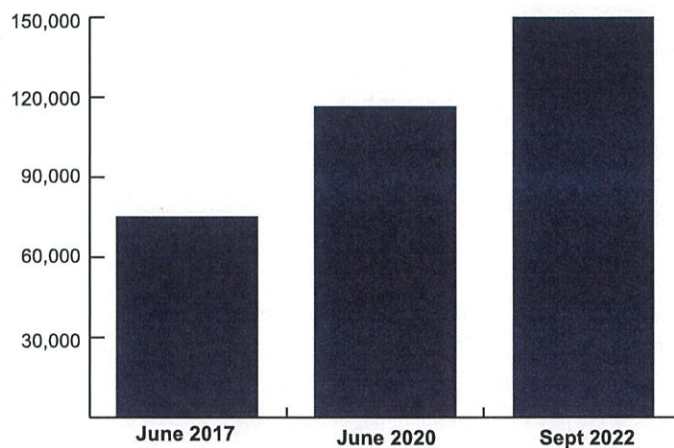
Daily logins



The number of daily logins saw a significant increase between June 2017 and June 2020, and further growth demonstrated in September 2022.

This demonstrates the sustained use of myGov by Australians following the rapid growth of logins to access COVID certificates in 2020 with more Australians than ever regularly logging in to myGov.

Tell us once updates (per month)



The number of people using the tell us once service has not seen the same growth, although higher than both the 2017 and 2020 snapshots.

Although further analysis is needed as to the drivers for this, evidence examined by the panel suggests this is due to both user awareness of the service and the limited number of agencies the tell us once service connects with, meaning there is lower value to users than other services.

THE PANEL'S APPROACH

The Terms of Reference (refer to Attachment A) set the aim and outcomes of the audit. The Panel was asked to consider the user experience, functions and performance of myGov in order to shape the future direction of myGov and its connection with government services.

The Panel's assessment is based on:

- desktop review of existing user research, analysis and data
- insights from over 700 survey responses, 91 submissions and the input from 66 participants in 12 focus groups conducted for the audit
- insights from 20 submissions from Australian Government agencies and state and territory governments
- 5 roundtables with peak bodies and industry experts
- 6 roundtable discussions with senior Australian Government and state and territory government officials.

The Panel assessed myGov by reference to four principles focused on **citizen value**.

- **Simple:** myGov should make it easy for citizens to engage with government, saving time and effort.
- **Beneficial:** myGov should promote well-being by connecting citizens quickly and seamlessly to the services they need.
- **Fair:** myGov should promote the human rights of all people and integrate with other services to ensure that all citizens can engage effectively with government.
- **Trustworthy:** citizens should be able to trust myGov to work when needed and that services will be delivered transparently, safely and securely.

And; two principles focused on broader **societal value**:

- **Efficient:** myGov should deliver better services for citizens at a reduced cost to taxpayers and with productivity-enhancing efficiencies across the economy.
- **Leading:** myGov should place Australia at the leading edge of quality digital service delivery globally and be an exemplar service within government.

Drawing on the evidence and principles, the Panel undertook detailed analysis of features of a great service experience for myGov, as well as the foundations of funding, planning, governance, accountability, and technology that would be needed to deliver that experience. While the procurement arrangements for the new myGov platform were not within the scope of the audit, the Panel notes the ANAO undertook analysis on these in early 2022. Volume 2 of the report provides the detailed analysis on the current state, features of a desired future state and actions required to realising the potential of a future myGov. From this detailed analysis, the Panel has distilled 10 findings and 10 recommendations in Volume 1.

The importance of trust

To build and maintain trust, myGov needs to work for people. It must be accessible, easy to use and secure. It must improve to meet evolving expectations. Each time a person has a positive experience when using myGov a little trust is gained. Conversely, each negative experience, reduces trust. Of the principles outlined above, the Panel considers trust to be foundational for Australians to have a positive and functional relationship with government.¹

The Government's demonstrated ability to securely collect, use and share data for Australians' benefit with prior, free and informed consent will build confidence and overcome concern and discomfort around government use of data.²

To earn the trust of Australians, government must also demonstrate responsiveness, reliability and commitment to values of openness, integrity and fairness.³ Efficiently coordinated services that serve and anticipate citizen needs are key. Doing so in a transparent and ethical way that holds government accountable is essential.

Australians having their say on myGov

The audit invited input from Australians through an online survey open from 13 October 2022 to 10 November 2022. Key findings from the 723 respondents were:

67% used myGov in the last week

10% spoke a language other than English as their primary language

75% thought government should do more for people who do not use online services

54% had their myGovID connected to their myGov account

20–40% reported negative experiences when using myGov

75% thought government online services need improving

50% of respondents did not know where to go for help if having problems

1 Behavioural Economics Team of the Australian Government (BETA), myGov User Audit Research Report, 2022 (unpublished)

2 *ibid.*

3 *ibid.*

Findings

FINDING 1



myGov is indispensable national digital infrastructure.

Australia's transport networks, hospitals, utilities and education systems are critical infrastructure relied on by Australians everyday as they go about their lives. Investing in roads, hospitals and schools is essential to serve Australians' basic needs, to drive economic growth and build a stronger Australia. So too, myGov is essential infrastructure that connects people to information and digital services leading to better health and social outcomes.

The *Infrastructure Australia Act 2008* defines nationally significant infrastructure as including transport, energy, communications, and water infrastructure 'in which investment or further investment will materially improve national productivity'. Social infrastructure is also considered, such as health, education, social housing and community facilities. As a guide, for a proposal to be considered nationally significant, it should concern a problem or opportunity that will have more than \$30 million per annum impact on the economy (nominal, undiscounted). Unquantified social benefit considerations are also taken into account.⁴

Providing high-quality, resilient, accessible and equitable digital infrastructure in an era of accelerating digitalisation has been identified as a key priority for Australia by Infrastructure Australia.⁵

Similarly, the Critical Infrastructure Resilience Strategy 2015 defines critical infrastructure as 'those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security'.⁶

Daily myGov usage has more than tripled in the past 5 years. myGov now supports more than 1.1 million sessions on an average day, with daily rates often exceeding 1.4 million. More people use myGov each day than use public transport⁷. Daily myGov usage is also greater than the average number of *monthly* hospital admissions in Australia.

In 2017, there were 11.7 million myGov accounts. Today, there are more than 25 million. Almost 20 million Australians have a digital COVID-19 vaccination certificate, and almost 4.6 million have downloaded their International COVID-19 Vaccination Certificate – all through myGov.

myGov is part of most Australians' lives and unlocks the value of government policies. With this comes an important caution. myGov's strong recent performance has raised the stakes. When performing well, myGov drives positive outcomes for Australians, the economy and government. If myGov fails to deliver, the impacts are severe, with those who need help the most significantly and disproportionately affected.

⁴ Infrastructure Australia, Infrastructure Glossary [website], accessed December 2022, <<https://www.infrastructureaustralia.gov.au/Infrastructure-glossary>>

⁵ Infrastructure Australia, *2021 Australian Infrastructure Plan*, 2021

⁶ Cyber and Infrastructure Security Centre, Defining critical infrastructure [website], accessed December 2022, <<https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/defining-critical-infrastructure>>

⁷ Australian Bureau of Statistics, Australia's Journey to Work [website], 2022, accessed December 2022, <<https://www.abs.gov.au/articles/australias-journey-work#public-transport>>

The myGov experience mirrors what is happening in the private sector. In Australia, one study found that Australian businesses undertook 10 years' worth of technology adoption and transformation during the pandemic alone.⁸ It also reflects global trends. Internationally, digital increased from 20% of customer interactions in 2018 to 58% in 2020 across the private and public sectors.⁹

The challenge for government used to be how to create demand for digital services. No longer. The challenge now is how to meet rapidly growing demand for high-quality, safe and secure digital services. There is rightly a higher standard for government digital services. That is why approaching myGov as a piece of indispensable infrastructure, and not just another IT project, is key in meeting this new challenge.

Other countries are also building this infrastructure for their citizens. The Panel commissioned a review of global best practice from the Boston Consulting Group (BCG) (refer to Volume 2, Attachment A). This evidence was used to inform the Panel's recommendations and to benchmark Australia's progress.

From this review it is clear no nation has fully realised the 'promise' of connected digital service delivery. Each national path reflects history, culture, and investment and technology choices. Nevertheless, BCG discerned 4 features of high-quality government digital service offerings:

1. single whole-of-government entry points that have the highest adoption and satisfaction combine navigation, information and transactions
2. citizens increasingly expect omni-channel experiences in line with best practice private offerings (e.g. chatbots, virtual assistance, telephony, mobile, online)
3. best practice portals eliminate redundancy by promoting Tell Us Once
4. portal design and development leverage a contemporary open and modular architecture with embedded digital identity.

FINDING 2

Recent investments have built the foundations to deliver on myGov's promise, but myGov will not fulfil its potential without further investment and discipline to ensure adoption of new capabilities across government.



myGov today is changing thanks to a temporary \$200 million boost provided in 2021–22 for the two-year Enhanced myGov program.¹⁰ This temporary boost came on top of business-as-usual sustainment funding in the order of \$38 million per year. This brought annual funding for myGov to a total of close to \$138 million per year over the 2021–22 and 2022–23 financial years.

The program is delivering overdue improvements to myGov's underlying IT platform and the quality of the digital front door it provides Australians. Importantly, the new technology is based on open standards using an approach designed to allow services to come easily together in a single interface. Testing suggests that myGov can now support 500,000 concurrent users – 50 times more than it did previously.¹¹

The recently released myGov app is another a big step forward. myGov has been late to the app game, but the new app delivers functionality and a user experience close to that provided by the private sector.

⁸ Alphabeta Australia, *Australia's digital resilience: How technology strengthened Australian business during COVID and beyond*, 2020

⁹ McKinsey and Company, *How COVID-19 has pushed companies over the technology tipping point and transformed business forever*, 2020

¹⁰ Australian Government, *2020–21 Australian Government Budget – Budget Paper No. 2*, 2020

¹¹ Services Australia data (unpublished)