

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

ART 2025/4916

BETWEEN

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

FURTHER AFFIDAVIT

On 25 August 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 make this further affidavit to respond to certain matters in the affidavit of (Fraser Tweedale affirmed 29 July 2026) (**Tweedale affidavit**), the report of Dr Teague dated 24 July 2026 and the report of Professor Serwylo dated 31 Jul 2026 and the Statement of Facts, Issues and Contentions of the Applicant (**ASFIC**). I adopt abbreviations used in my prior open affidavit in this matter affirmed on 25 May 2026.
3. 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.

PART II INFORMATION SECURITY AND GOVERNANCE IN THE AUSTRALIAN GOVERNMENT

4. At [61.2] of the ASFIC, the applicant contends that 'Australian Government policy has embraced the position that source code developed for delivery of digital services should be publicly disclosed'.

Lodged on behalf of the Respondent

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

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

Contact: Jessica Connolly

File ref: 25010582

Telephone: 02 6253 7059

Facsimile: 02 6169 3054

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

5. Based my role and understanding of the Commonwealth technology and security environment, and information in my closed affidavit, I can say that that it is not the policy position of the Australian Government to encourage or mandate the public disclosure of source code developed for delivery of digital services.

The Commonwealth digital environment

6. The Digital Transformation Agency (DTA) is an executive agency of the Commonwealth, within the Finance portfolio, which provides strategic and policy leadership on whole-of-government and shared information and communications technology (ICT) and digital service delivery.
7. The DTA's 'Digital Experience Policy' is supported by the following four standards:
 - 7.1. Digital Service Standard (DSS);
 - 7.2. Digital Inclusion Standard;
 - 7.3. Digital Access Standard; and
 - 7.4. Digital Performance Standard.

The Digital Experience Policy is available at: <https://www.digital.gov.au/policy/digital-experience>

8. Currently, the DSS consists of 10 criteria. See: <https://www.digital.gov.au/policy/digital-experience/digital-service-standard>.
9. Criterion 5 is "Build trust in design".

Annexed hereto and marked 'GM-1' is a copy of Criterion 5, as accessed on 20 August 2026.

10. Under the heading "How to apply criterion 5", there are four principles, including:
 - 10.1. "Implement security measures". Criterion 5 requires that services be "secure by design" and requires agencies to "use the Information Security Manual, the Essential Eight and other resources from the Australian Cyber Security Centre to thoroughly assess the service's threats, posture and protections."
 - 10.2. "Be Accountable for the service". Criterion 5 that services "undertake periodic audits" of the service, data-handling practices, security incidents and compliance with whole-of-government policies. It further requires that results are used to improve and keep the service fit for purpose (further referring to Criterion 10 "Keep it relevant").
11. Further high level guidance provided by the DTA to "build trust in design" includes ensuring that security measures are up to date to protect against new and emerging threats, and implementing a layered security strategy.

12. The DSS on-refers to whole-of-government information security policies which I have previously referred to in my prior open affidavit affirmed on 25 May 2026 (the ISM and the E8) as being policies that govern information security in the Australian Government, as well as other resources from the ACSC.

13. Included in the ISM are the following cyber security principles:

GOV-10 – System exposure minimisation: 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.

GOV-14 – Legacy system management: Systems (infrastructure, operating systems, applications and data) that are not capable of meeting cyber security requirements are managed using compensating controls, along with enhanced monitoring and assurance activities, to maintain an acceptable level of residual risk until they can be decommissioned or replaced.

The ISM cyber security principles are available at: <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-principles>

14. Based on the above principles and statement, which I believe to be current and correct, government agencies are required to maintain systems and practices that reduce system exposure which includes maintaining confidentiality in relation to information including source code.

15. In my prior open affidavit affirmed on 25 May 2026 I referred to the 2023 myGov User Audit report at [24]. In December 2023, the Government released its response to the myGov User Audit report. In response to recommendation 9, which included a recommendation that Government should “design and build myGov ‘in the open’” including wherever possible to publish ‘most of its source code’, the Government response said at page 18:

Following advice from the Australian Signals Directorate’s Australian Cyber Security Centre, Government does not support the recommendation to publish open-source code due to cyber security concerns of such an approach.

Annexed hereto and marked ‘GM-2’ is the Government response to the 2023 myGov User Audit report as available at: <https://my.gov.au/en/audit>

PART III THE APPLICANT’S CONTENTIONS

16. I have read the Applicant’s Statement of Facts, Issues and Contentions (**ASFIC**) filed in this proceeding dated 31 July 2026.

Three step model

17. At [23]-[24] of the ASFIC, the applicant conceptualises the respondent’s case as proceeding in three steps and says that the applicant does not dispute steps 2 and 3 but says the respondent has not established step 1 (that harm would result from the disclosure). I maintain the view that disclosure of the source code would cause, or

could reasonably be expected to cause damage to the security of the Commonwealth, and have a substantial adverse effect on the agency.

18. From my experience, the Applicant's three step model (referred to at ASFIC [23]) does not account for the motivations of a malicious actor and the value they see in any given piece of information, the discovery of a vulnerability, the ability to compromise an account or ability to gain access to another system.
19. The "MITRE ATT&CK" is an internationally recognized tool used by cyber security professionals to standardise descriptions of how a malicious actor operates and is informed by real world compromises. MITRE ATT&CK is self-described on its website as:

a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
20. MITRE ATT&CK is a structured method for describing adversary behaviour. It defines 15 techniques, 254 tactics and several hundreds of procedures. These tactics, techniques and procedures (**TTPs**) are described on the website.

MITRE ATT&CK can be accessed at: <https://attack.mitre.org/>
21. A malicious actor in planning to compromise a digital service will seek a variety of information to support their malicious activity. Examples of the types of information a malicious actor may be interested in includes procurements, as built documentation (indicating deficiencies in the service), integration or engagement channel pathways (indicating potential avenues to compromise an application or system), and stakeholders (indicating potential targets). Threat actors can combine information they have collected from other breaches with further information gained.
22. In my experience, source code is highly sought after by threat actors as it can be used for a variety of purposes (including various TTPs).

Counterfeit applications

23. Contrary to the contention at [44] of the applicant's ASFIC, counterfeit applications can bypass various barriers. There are public examples where malicious actors have managed to get counterfeit applications added to both the Apple App Store and the Google Play store including authenticator apps, as well as banking and other financial management apps.
24. Further, counterfeit apps or other malicious apps can be deployed to steal information. The MITRE ATT&CK lists procedures setting out where a malicious actor has successfully bypassed the application sandbox to gain access to privileged functions of Android devices, including enabling access to information the sandbox is supposed to protect. Specific examples include:

- 24.1. Gooligan – “is a malware family that runs privilege escalation exploits on Android devices and then uses its escalated privileges to steal authentication tokens ...”
- 24.2. HummingBad – “is a family of Android malware that ... has the ability to obtain root access on older, vulnerable versions of Android.”
- 24.3. Pegasus for Android – “is the Android version of malware that has reportedly been linked to the NSO Group.”

See further ‘Exploitation for Privilege Escalation’, technique T1404:
<https://attack.mitre.org/techniques/T1404/>

- 25. Critically, once the application sandbox is breached, malicious actors can deploy specialised malicious apps specifically designed to exfiltrate sensitive information such as credentials, TOTP, banking or financial information and other sensitive information that may be on a phone.
- 26. An example of an Android information stealer app is ‘Infamous Chisel’. The ACSC has published their analysis of this app to assist organisations to understand the risks they face, indicators of compromise and avenues to attempt to mitigate being exploited.

The report is available at: <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/infamous-chisel>

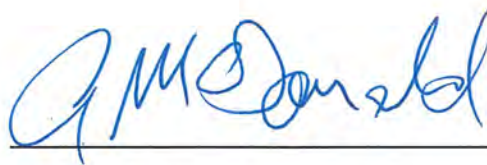
Cyber security industry practice

- 27. Penetration testing (known as “pen testing”) is often categorised based upon the level of knowledge the penetration tester knows about a system, as follows:
 - 27.1. **Black-box penetration testing** (close-box penetration testing) is perhaps the most challenging and realistic form of penetration testing. As the name suggests, black-box penetration testing involves assessing the security of an IT environment or system without any prior knowledge of its inner workings.
 - 27.2. **White-box penetration testing** (open-box penetration testing) is the opposite of black-box penetration testing. During a white-box test, pentesters have full knowledge of and visibility into the target IT environment.
 - 27.3. **Grey-box penetration testing** sits somewhere between black-box and white-box testing. In a grey-box pentest, the testers may have limited or partial knowledge of the target of their attacks. Depending on the type of test, grey-box pentesters may know a little about the entire system or a lot about only part of the system.
- 28. As the source code has not been released into the public domain there is presently limited to no information beyond the application package which would enable a malicious actor to understand the application. In this scenario, malicious actors are essentially limited to attempting ‘black-box’ penetration of an application or system. This approach increases the difficulty of compromising a system and identifying

vulnerabilities, and is part of a layered approach to cyber security and defensive capabilities.

AFFIRMED at Canberra in the
Australian Capital Territory

On 25 August 2026



Garrett McDonald

Before me



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 further affidavit of Garrett McDonald, affirmed at Canberra on 25 August 2026, before me:


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



Digital Service Standard

Digital Service Standard

Criterion 5 – Build trust in design

Making sure the service is useful, easy, inclusive, transparent and stable will build users' trust and confidence in government.

Your responsibilities

To successfully meet this criterion, agencies will need to:

- adopt transparent data handling
- implement security measures
- maintain a reliable service
- be accountable for the service.

When to apply

Apply Criterion 5 throughout Beta to protect users' digital rights and ensure robust security measures are in place.

As cyber threats become more prevalent and sophisticated, adhere to this criterion across the Service design and delivery process.

Questions for consideration

- How are users informed about the collection, use and storage of data?
- How will informed consent be obtained from users?

Was this
page
helpful?



Which encryption and authentication mechanisms will provide the most robust security?

How does the service comply with data protection legislation and policies?

What processes are in place to prevent misinformation?

How is the service built to be resilient against cyber threats?

What assurances are in place to promote ethical use of data?

How to apply criterion 5

Adopt transparent data handling

Consider privacy, consent and control: Safeguard user data by adhering to the Australian Privacy Principles and the Privacy Act 1988. Always get explicit, informed consent before collecting a user's data and provide a means to update or delete it. Allow users to report inaccurate data and respond with how it has been rectified. Notify users about their responsibilities to protect their data, such as not sharing their password with others.

Eliminate ambiguity in the user interface: Provide validating feedback and progress tracking as users interact with the service. Design to eliminate the need for error messages in the first place. When creating error messages, make them understandable and actionable. Tell users what information they need before they start a task and, where appropriate, allow them to pause and resume at their own pace.

Establish trust and provenance: The widespread availability of AI and machine learning tools, including generative models and deepfake technologies, makes it possible for anyone to convincingly create and/or modify media with minimal effort, low cost, and increased realism. Where appropriate, consider how to embed provenance information to help establish and maintain trust. Resources such as Content Credentials: Strengthening Multimedia Integrity in the Generative AI Era should be consulted.

Was this
page
helpful?

Implement security measures

Secure by design: Use the [Information Security Manual](#), the [Essential Eight](#) and other resources from the [Australian Cyber Security Centre](#) to thoroughly assess the service's threats, posture and protections. Plan for the requirements and [system hardening](#) that will support the service throughout design, build, operation and decommissioning.

Maintain a reliable service

Available and consistent: Make the service available, stable and consistent for users in different places and time zones, at different times, on different days. Schedule maintenance for a predictable period of downtime, and give notice to users well ahead of time.

Be accountable for the service

Embrace contestability: Offer clear avenues for users to submit complaints, contest decisions or report issues, including security data and cyber concerns. To increase the likelihood of useful feedback, make avenues anonymous by default and identifying by choice wherever possible. To demonstrate that feedback has been addressed or will inform future action, provide users with timely and transparent responses. Responses should be tailored to the feedback.

Undertake periodic audits: Audit the service, data-handling practices, security incidents and compliance with whole-of-government policies. Use an independent review to test assumptions and identify issues that may be taken for granted. Use these results to improve and keep the service fit for purpose ([Criterion 10 'Keep it relevant'](#)).

Was this
page
helpful?

Guidance to build trust in design

Ensure security measures are up to date

Prioritise service security measures and have processes in place to ensure that they are efficient and current. Use methods or tools such as:

Conduct regular and comprehensive security audits to identify vulnerabilities in the digital service. This includes penetration testing and assessments to keep security measures robust and up to date.

Regularly update software, hardware and security protocols to protect against new and emerging threats. This includes prompt application of patches, updates and security fixes.

Implement ongoing security training for staff on best practices, include phishing recognition attempts and secure handling of sensitive data.

Establish and regularly update an incident response plan to prepare for potential security breaches. Outline steps for detecting security incidents, responding to them and recovering.

Establish processes for preventing misinformation

Prioritise the accuracy of information provided. Put processes in place for regular checks and updates. Use methods or tools such as:

Establishing clear guidelines for content moderation to prevent misinformation. This includes procedures for reviewing and verifying information before it is published.

Implement reporting mechanisms so users can flag misinformation or content they believe is inaccurate. This encourages user engagement and helps maintain the integrity of information provided.

Was this
page
helpful?

Maintain processes for regular content updates and corrections when information inaccuracies are identified. Transparent correction processes build trust.

Ensure the service is resilient against cyber threats



Have processes in place to make sure the service is resilient and updated against current and imminent cyber threats. Use methods or tools such as:

Implement a layered security strategy that includes firewalls, intrusion detection systems and encryption to create multiple anti cyber barriers.

Develop and test disaster recovery and business continuity plans to ensure the service runs quickly to recover from cyber incidents, including data breaches or denial-of-service attacks. Continuously monitor and assess emerging cyber threats. This involves subscribing to threat intelligence services and keeping abreast of industry developments.

Educate users about cybersecurity best practices, such as using strong passwords and recognising phishing attempts. An informed user base enhances overall security.

Document your findings



Document your findings and recommendations to apply criterion 5:

Ensure timely updates of software and hardware to protect against the latest threats and implement ongoing training programs for staff on security best practices.

Establish and regularly update an incident response plan outlining procedures for handling security breaches.

Create guidelines for content moderation to prevent misinformation.

Was this
page
helpful?

Make sure the data is collected and documented in a centralised knowledge repository.

Links



[Protect yourself | Cyber.gov.au](#)

[Cyber Security | Australian Signals Directorate \(asd.gov.au\)](#)

[Information security | Protective Security Policy Framework](#)

[Preventing data breaches: advice from the Australian Cyber Security Centre | OAIC](#)

[Update your devices | vic.gov.au \(www.vic.gov.au\)](#)

[Cyber incident management plan | vic.gov.au \(www.vic.gov.au\)](#)

[Cyber Security | Australian National Audit Office \(ANAO\)](#)

[ACSC Emergency Response Guide \(cyber.gov.au\)](#)

[Cyber Security Incident Response Planning: Practitioner Guidance | Cyber.gov.au](#)

Criterion 6 – Don't reinvent the wheel

[Next page](#)

Was this
page
helpful?

Connect with the digital community

Share, build or learn digital experience and skills with training and events, and collaborate with peers across government.

[Join the Digital Profession](#)

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

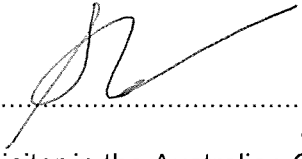
2025/4916

FRASER TWEEDALE
Applicant

CEO, SERVICES AUSTRALIA
Respondent

ANNEXURE GM-2

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


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



Australian Government

Response to the myGov User Audit Report

Independent Audit 'Critical National
Infrastructure – myGov User Audit'

October 2023



The Australian Government acknowledges 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.

Contents

Introduction.....	4
Foreword	5
Summary of Responses	6
Recommendation 1	10
Recommendation 2	11
Recommendation 3	12
Recommendation 4	13
Recommendation 5	14
Recommendation 6	15
Recommendation 7	16
Recommendation 8	17
Recommendation 9	18
Recommendation 10	19

Introduction

myGov is one of the most heavily used digital platforms in Australia, providing a centralised entry point for people to access critical government services. It has become an indispensable piece of Australian national digital infrastructure, serving as a fundamental link to connect people to government.

myGov started as a secure authentication solution for a few government services and has grown to become one of the most heavily relied upon government platforms, with approximately 26 million active accounts, 3.3 million app users and more than 782,000 sign ins per day. Currently, it provides secure and rapid access to a range of government services, some whole-of-government content, and a number of supporting capabilities, such as the inbox.

The myGov User Audit commenced in September 2022 and was conducted by an independent audit panel. The aim of the audit was to review the current state and possibilities for myGov and make recommendations to shape its future direction.

The independent audit panel consulted with users, industry, and peak bodies, and engaged all tiers of government to inform their findings.

The critical national infrastructure–myGov User Audit report (the report) was publicly released by Senator the Hon Katy Gallagher, Minister for Finance and Minister for Women and the Public Service, and the Hon Bill Shorten, Minister for the National Disability Insurance Scheme and Minister for Government Services, on 31 January 2023.



Volume 1 of the report contains the panel's 10 findings and 10 recommendations. These go to the heart of systemic issues and set the pathway to fulfil myGov's potential as critical national infrastructure.



Volume 2 of the report contains detailed analysis and guiding actions to meet Australians' needs and expectations for digital government services.

In the 2023–24 Budget, Government invested a further \$134.5 million to operate and maintain the myGov platform.

Foreword

We welcome the myGov User Audit Report (the report) which presents us with an opportunity to fundamentally reshape the way government services are delivered.

Thank you to the independent panel chaired by Mr David Thodey AO, with Professor Edward Santow, Professor Emily Banks AM, Commissioner Julie Inman Grant and Mr Amit Singh, for their comprehensive review and thought-leadership.

myGov is a recognised government brand and is part of most Australians' lives. Today there are more than 26 million myGov accounts with more than 782,000 sign ins per day and 3.3 million app users.

It has become an indispensable national infrastructure delivering essential digital public services to support people through their lives, including during emergencies and disasters.

Clearly, we need to implement the future of digital government service delivery through myGov.

The 10 findings and recommendations of the report go to the heart of systemic issues holding us back. We agree we need to address these issues to unlock the value of government policies and simplify government services.

Like many other countries in the world, the Australian government aims to create a digital ecosystem where services are connected, secure and seamless.

Our response to the report is part of setting a clear pathway to achieve that ecosystem in lockstep with the Data and Digital Government Strategy and Digital ID work.

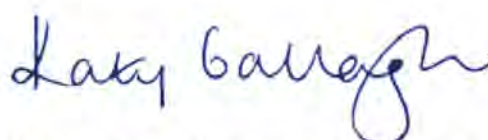
The establishment of a dedicated team to make early progress towards the strategy and implementation of myGov as a primary front door shows we understand the need for well thought-out implementation, and whole-of-government action to deliver on the government's position.

We are committed to establishing the foundations and to investing in and scaling myGov to deliver the world class digital services Australians expect.



Minister Bill Shorten

Minister for the National Disability Insurance Scheme,
Minister for Government Services



Senator the Hon Katy Gallagher

Minister for Finance,
Minister for Women,
Minister for the Public Service

Summary of Responses

MYGOV AUDIT RESPONSE OVERVIEW

POSITION

Recommendation 1

Agreed

Confirm myGov as the 'go to' place for people to access services online from the Australian Government and communicate with all Australians.

To support citizens to navigate government services and to drive efficient and effective digital investment, Government agrees to a unified and pragmatic whole-of-government approach to myGov as a primary front door. Government will define a decision-making framework in consultation with whole-of-government input to provide clear guidelines for agencies to determine where their service fits into the broader delivery of government services to curb the proliferation of new front doors, consolidate the existing digital ecosystem, and identify opportunities to reuse systems and reduce duplicative investment.

Government notes that seamless and connected services are constrained by government organising structures which makes achieving the full extent of this recommendation difficult and costly.

Removing barriers to implementation will be further explored by Government in progressing work under recommendations 3 and 7. Government has commenced work towards this recommendation, however there is a need to increase whole-of-government oversight of investments in the digital service delivery ecosystem.

Recommendation 2

Agreed

Ensure myGov leaves no one behind and upholds Australians' human rights.

Government will develop a Digital Inclusion Standard that ensures services are designed and delivered to leave no one behind. This new standard will set levels of acceptable delivery of digital services to Indigenous communities, designing and building services that are inclusive and accessible, and uphold human rights. Government agrees to ensure myGov is designed and delivered according to this standard.

Government has agreed through the Data and Digital Ministers Meeting to progress initiatives related to digital literacy, inclusion and connectivity across all tiers of government.

Government notes Services Australia has broad reaching infrastructure and capabilities including service centres, remote and regional support and telephony services that could be leveraged to support a collective approach in delivering to citizens.

Recommendation 3**Noted****Legislate myGov as national service delivery infrastructure.**

Government recognises the potential for legislating myGov as national infrastructure. The current legislative environment for myGov impedes service delivery, particularly around data and personal information that may hinder the realisation of the aspirations outlined in the Audit. Government will invest in further discovery work to inform decisions and actions toward this recommendation.

Recommendation 4**Agreed in-principle****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.**

Government agrees in-principle to fund myGov as national infrastructure with appropriate allocations to preserve and operate the service, ensuring it remains secure and contemporary. Noting \$134.5 million was committed in 2023–24 Budget to operate and maintain myGov for one year. Further analysis will be completed and brought back in the 2024–25 Budget context for ongoing operate and maintenance needs.

Recommendation 5**Agreed in-principle****Publish during 2023 a rolling 5 year roadmap for developing myGov, updated annually.**

Government agrees in-principle to develop a rolling roadmap that sets out new services and functionality through myGov that will be integrated and published for citizens, including, as part of the implementation plan for the Data and Digital Government Strategy. Major improvements and enhancements will be prioritised and overseen by the governance outlined in recommendation 7.

Recommendation 6**Agreed**

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.

Digital ID is a voluntary, secure and trusted way for Australians to use the government services they rely on. The expanded use of Digital IDs will ensure that in the future, government services are easier for citizens to access. Government supports accelerated development of Australia's national digital identity ecosystem and the introduction of legislation to support its broader rollout. Implementation of this recommendation will be guided by the outcomes of the Department of Finance led Digital Identity Taskforce. The Government has invested to sustain and develop the next stage of the Digital ID Program, as it transitions to an economy-wide Digital ID ecosystem with an independent regulator.

Recommendation 7**Agreed in-principle**

Introduce by mid-2023 citizen-centred governance and operational arrangements for myGov and myGovID to overcome government siloes and drive inclusion and performance.

Government will develop revised governance arrangements to support the future of myGov. The first step will be the establishment of an independently chaired advisory board that will provide expert advice to the Minister of Government Services to shape the future of government services.

Governance of myGov and myGovID will remain separate, with myGovID remaining part of the Digital ID Program, to consider whole of economy impacts, whilst myGov focuses on Government service delivery.

Recommendation 8**Agreed**

Partner with the states and territories on a 5 year plan to make it easy for people to find and do what they need to across all levels of government.

Government will continue to work with jurisdictions to deliver connected services for citizens. Government will establish a Commonwealth and state and territory working group, through the Data and Digital Ministers Meeting, to develop a plan. The plan would expand beyond the Audit's recommendation by covering digital service integration across all sectors, leveraging work on life events, digital identity and verifiable credentials, and a plan to develop interoperability standards. The plan will intersect with the roadmap for myGov as outlined in recommendation 5.

Recommendation 9**Agreed in-principle**

Design and build myGov in alignment with a refreshed and enforced Australian Government Architecture, incorporating the Design System and the Service Standard.

The Digital Transformation Agency has launched a refreshed platform to better navigate and apply the Australian Government Architecture to digital investments.

Government, through the Digital Transformation Agency, has developed a new Digital Service Standard to standardise the way digital services are designed, delivered and maintained, and better support agencies through enhanced guidance materials that accounts for varying levels of digital maturity. Adherence to these standards and policies will be monitored and governed under recommendation 7. The Standard is supported by a whole-of-government digital service performance framework, providing measurements to assess and improve the quality of Australian Government digital services, in line with its digital government vision and as part of the Data and Digital Government Strategy's measurement framework.

Recommendation 10**Agreed in-principle**

Services Australia develop and adopt a new world-class approach to service and support to government agencies utilising myGov.

To realise the vision for myGov, Government acknowledges the need for myGov to be the most responsive and contemporary part of the delivery system and make pragmatic changes to ensure myGov is offering contemporary support and solutions to agencies. Government will progress work to develop a new approach to enable the opportunity to build once and use many times to meet the needs of a range of service delivery challenges. It will also provide an opportunity to explore government services being delivered in new, non- traditional and flexible ways that avoids additional costs to Government through the development of duplicated and bespoke solutions and delivers a better service for Australians.

Government, through Services Australia, will review its current approach to operating and delivering across government agencies. This will be done in consultation with existing and potential new partner services focusing on ways to deliver value easily and quickly. Achieving a new world-class approach to service and support for agencies utilising myGov will be underpinned and further enabled under recommendations 4, 5 and 7.

Recommendation 1



Confirm myGov as the 'go to' place for people to access services online from the Australian Government and communicate with all Australians.

Government **agrees** to the recommendation.

Government notes services are still widely distributed across multiple websites and apps, meaning people have to navigate multiple sources of information built around complex government structures to access the support they need. Government will establish a Digital Access Standard through whole-of-government consultation that sets the decision-making criteria to promote digital consolidation, identify opportunities to reuse systems and reduce duplicative investment.

It is the Government's ambition that myGov provides a primary front door for individuals to access digital Government services as a future state. Simplifying and consolidating the broader service delivery ecosystem provides opportunity for economic, social and service delivery benefits. Further decisions by government will inform the future of myGov and its role.

Government has commenced work towards this recommendation, however there is a need to increase whole-of-government oversight of investments in the digital service delivery ecosystem.

Document execution makes interacting with government services easier

Government has commenced addressing the audit recommendations to make services simple through the delivery of a document execution function within myGov, meaning people no longer need to find someone to manually witness their statutory declaration. Moving forward, there is potential for this capability to be re-used across government services enabling a seamless user experience, such as for passport renewals.

Recommendation 2



Ensure myGov leaves no one behind and upholds Australians' human rights.

Government **agrees** to the recommendation.

Digital and online platforms are a huge part of our everyday lives, but 1 in 4 people in Australia are currently facing barriers to accessing or making best use of them
– Hon. Minister Amanda Rishworth

Government will develop a Digital Inclusion Standard that sets requirements for agencies to deliver inclusive and accessible government digital services to ensure services are designed and delivered to leave no one behind. These standards will set levels of acceptable delivery of digital services to all communities including Indigenous, those living with or caring for someone with a disability, and culturally and linguistically diverse.

Government acknowledges a greater emphasis on consultation with citizens, peak bodies, advocacy groups and front-line service delivery staff throughout the design and development of new government services and capabilities is required.

Government will explore avenues to reducing language and literacy barriers for people accessing a digital service. Government notes Services Australia has experience and significant broad-reaching infrastructure and capabilities, including service centres, remote and regional support and telephony services that could be leveraged to support a collective approach in delivering services to people. Government will consider further decisions needed in relation to ensuring people can switch to another channel if myGov does not work for them.

Government recognises there is an important role in improving digital literacy for all people in Australia, as a way to reducing barriers to access digital services. Government has agreed through the Data and Digital Ministers Meeting to progress initiatives related to digital literacy, inclusion and connectivity across Commonwealth, state and territory governments.

Government notes the outcomes of the Privacy Act Review will have implications for the delivery of this recommendation, including how government progresses consent and nominee arrangements.

Connecting vulnerable people to government services

Government has implemented a pilot to provide support to vulnerable people in Australia with complex circumstances to access essential government services. Services Australia is working alongside, and onsite, with community organisations to connect vulnerable customers who don't have access to apps and computers to claim payments and connect with government and community services based on their individual circumstances.

In the 2023–24 Budget, Government provided:

- \$10.0 million over 3 years for broadband and mobile services upgrades to support digital connectivity needs for First Nations people in Central Australia through the Regional Connectivity Program.
- \$0.3 million to provide mobile and internet for Wi-Fi connectivity in Alice Springs Town Camps through the Digital Connectivity Project.

Recommendation 3



Legislate myGov as national service delivery infrastructure.

Government **notes** the recommendation.

Government notes that a number of practical barriers remain in place that inhibit the vision for myGov to join-up service delivery for individuals. This includes the interplay between key parts of program legislation, secrecy provisions and statutory requirements that prevent end-to-end information sharing and connected experiences.

Government agrees to exploring pathways that will support the joined-up delivery of government services and will invest in further discovery work to investigate what, if any, are the legislative barriers in realising the potential of myGov, how legislation could further improve citizen's rights and confidence in digital services, and to inform government's decisions and actions toward this recommendation.

Technology and the digital world is accelerating and legislation has not kept pace

Government have finalised their response to the Privacy Act Review, aimed at strengthening and modernising Australian Privacy Laws. The outcomes of this review will have implications for future practices, procedures and systems for handling personal information.

Recommendation 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.

Government **agrees in-principle** to the recommendation.

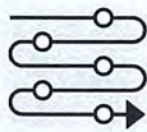
Government acknowledges that the investment made to date to enhance myGov has created a secure, scalable foundation to support the onboarding of new services and capabilities. The 2023–24 Budget invested \$134.5 million to operate and maintain myGov, ensuring it remains contemporary, secure and user-friendly.

Government will make a decision on appropriate ongoing funding for myGov in the 2024–25 Budget to preserve and operate the platform, ensuring it remains secure and contemporary.

Government invested more than \$2 billion for digital and ICT capabilities in the 2023–24 Budget

The Data and Digital Government Strategy highlights the need for new funding models to provide secure, ongoing funding to support whole-of-government digital and ICT delivery. Services Australia will explore funding options for onboarding and future improvements to myGov.

Recommendation 5



Publish during 2023 a rolling 5-year roadmap for developing myGov, updated annually.

Government **agrees in-principle** to the recommendation

Government agrees to develop a rolling roadmap for myGov that sets out services and functionality through myGov that will be reviewed every 12 months, and published to citizens as part of the broader government implementation plan for the Data and Digital Government Strategy. The roadmap will set out the strategic vision for myGov and will be informed by government priorities, policies, insights from customer research and feedback.

The Australian Government will deliver simple, secure and connected public services for all people and business through world class data and digital capabilities by 2030
– Data and Digital Government Strategy

Government's vision for the future of digital government services

Government has set their vision for the future of digital government services through the Data and Digital Government Strategy. The strategy confirms commitment for the Commonwealth to work collaboratively, and with all tiers of government, industry and academia to progress towards the 2030 vision.

Recommendation 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.

Government **agrees** to the recommendation.

Australia's approach to identity resilience needs to keep pace with our economic and social activities, and the changing nature of identity crime
– National Strategy for Identity Resilience.

Government notes that a Digital Identity (Digital ID) provides a secure way for people to access their online services. Creating and using a Digital ID is a voluntary, secure and convenient way for Australians to access government services they rely on. The Australian Government Digital ID provider is myGovID and can be used as credentials to sign in to myGov, reducing the need to remember usernames and passwords. Using a Digital ID to access services includes the ability to allow people to digitally confirm their identity when accessing services.

Government supports accelerated development of Australia's national digital identity system and the introduction of legislation to support its broader rollout. Implementation of this recommendation will be guided by the outcomes of the Department of Finance-led Digital ID Taskforce, including to progress Digital ID legislation. The Government has invested to sustain and develop the next stage of the Digital ID Program, as it transitions to an economy-wide Digital ID ecosystem with an independent regulator. The expanded use of Digital ID will ensure that, in the future, services will be able to choose to use Digital ID instead of collecting people's personal information, thereby helping to minimise the impact of future potential data breaches involving identity data.

Working together to protect people from identity crime

The National Strategy for Identity Resilience was released and demonstrates the commitment by the Commonwealth and state and territory governments to work together to better protect the people of Australia from identity crime. This strategy is an important part of the broader whole-of-nation cyber security efforts, including the development of the 2023–2030 Australian Cyber Security Strategy.

Recommendation 7



Introduce by mid-2023 citizen-centred governance and operational arrangements for myGov and myGovID to overcome government siloes and drive inclusion and performance.

Government **agrees in-principle** to the recommendation.

Future governance arrangements will be considered as part of long-term funding for myGov in the Budget process. Renewed governance arrangements will be designed to underpin a joined-up service delivery model through ongoing collaboration across government to put citizens at the heart of the decision-making process, and give a voice to partner services in myGov decisions. An interim Independent Advisory Board was established in December 2023 to provide expert advice to the Minister for Government Services on projects, policies and initiatives ensuring they are ethical, uphold human rights, have a focus on customer service and are beneficial to Australians and the economy.

In alignment with the Government's Digital ID program, Government agrees that governance of myGov and myGovID will remain separate, with myGovID remaining part of the Digital ID Program, to consider whole of economy impacts, whilst myGov focuses on Government service delivery.

Governance mechanisms are strong, however there is more to do

Government confirms through the Data and Digital Government Strategy that there are strong governance mechanisms in place to coordinate cross agency efforts with state and territory governments. This includes the inter-jurisdictional forums like the Data and Digital Ministers Meeting and cross-APS bodies such as the Secretaries' Digital and Data Committee.

Recommendation 8



Partner with the states and territories on a 5-year plan to make it easy for people to find and do what they need to across all levels of government.

Government **agrees** to the recommendation.

Government has partnered with states and territories to develop a life events model to make it easier for people of Australia to access the services they need across all levels of Government. Getting married, having a child, retiring or death of a loved are some examples where joining up information and services can help the experience people have with government.

The Commonwealth will lead the implementation of recommendations of the cross-jurisdiction program Life Events Review in collaboration with states and territories through the Data and Digital Ministers Meeting (DDMM), as part of a renewed National Life Events Program.

Data and Digital senior officials from the Commonwealth and all states and territories agreed in May 2023 to the establishment of a Data and Digital Ministers Meeting (DDMM) working group with representatives from all jurisdictions, to lead work to develop a 5-year plan that provides a coordinated approach to digital service delivery and joined-up experiences for people using them.

Government notes the scope of the state and territory plan would expand beyond myGov, as noted in the Audit's recommendation by covering digital service integration across all digital services, not just those limited to myGov. The plan would leverage existing Government efforts on life events, Digital ID and verifiable credentials. The plan will intersect with the roadmap for myGov as outlined in recommendation 5.

Working with states and territories to connect tiers of government services

The Birth of a Child trial is delivering a streamlined experience, in select sites, for birth mothers to enrol their newborn with Services Australia. The trial aims to reduce the burden of filling out forms and interacting with government by re-using data government already holds. The future of the trial intends to enrol newborns in Medicare, streamline family claims with Centrelink and assist in registering births with state-based Births, Deaths and Marriages registries. With consent, data is exchanged meaning birth mothers will no longer have to complete three forms, and interact with three government organisations to register their baby for services.

Recommendation 9



Design and build myGov in alignment with a refreshed and enforced Australian Government Architecture, incorporating the Design System and the Service Standard.

Government **agrees in-principle** to the recommendation.

Government has released a vision for scalable, secure and resilient architecture, through the Data and Digital Government Strategy.

Government continues to support the development of the Australian Government Architecture (AGA)—a collection of digital artefacts and guidance materials to align to the digital direction of government. Government will expand the AGA by incorporating new policies and standards that will improve interoperability and inclusion of digital services addressing gaps in the digital policy landscape.

Government will take the lessons learnt from the previous design system and consider how this can be refreshed to be used by partner services to support more seamless and connected services with myGov.

Government has updated the Digital Service Standard to set the requirements for how to design and build digital services for the community, business and employees that are user-designed, inclusive and measurable.

Following advice from the Australian Signals Directorate's Australian Cyber Security Centre, Government does not support the recommendation to publish open-source code due to cyber security concerns of such an approach.

Government notes a collective approach will strengthen safety and security, and reduce the risks of cyber-attacks, imitation, and phishing of sign in pages. A whole-of-government approach to reviewing and maintaining the security and resilience of myGov and its partner agencies will be progressed to support the expansion of myGov.

Strengthening Australia's cyber security position

On 3 July 2023, Australia's inaugural National Cyber Security Coordinator (the Coordinator) commenced. The Coordinator, together with the National Office of Cyber Security (NOCS) within the Department of Home Affairs, serves as a focal point for Australia's strategic response to cyber security threats, challenges and opportunities, and will work closely with industry and critical infrastructure owners and operators to build a cyber resilient Australia.

Government will soon release the 2023–2030 Australian Cyber Security Strategy, which commits to Australia being a world-leading cyber secure and resilient nation by 2030.

Prime Minister of Australia [website], accessed August 2023 <<https://www.pm.gov.au/media/appointment-national-cyber-security-coordinator>>

Australian Government Department of Home Affairs [website], accessed August 2023 <<https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy>>

Recommendation 10



Services Australia develop and adopt a new world-class approach to service and support to government agencies utilising myGov.

Government **agrees in-principle** to this recommendation.

The Government's ambition is to shift myGov to be the primary front door for government services, where possible and appropriate. Government acknowledges the need for myGov to be the most responsive and contemporary part of the delivery system, including making pragmatic changes to ensure myGov is offering contemporary support and solutions to agencies. Government will progress work to develop a new approach to enable the opportunity to build once and use many times to meet the needs of a range of service delivery challenges.

It will also provide an opportunity to explore government services being delivered in new, non-traditional and flexible ways that avoid additional costs to Government through the development of duplicated and bespoke solutions and deliver a better service for Australians. Initiatives such as the Digital Traineeship Program will ensure that Government is positioned with the skills needed to deliver digital services.

Government, through Services Australia, will review the current approach to development and operations and explore options and feasibility for a whole-of-government approach to the design, development and delivery of products for myGov.

Digital skills for the future of Australia's economy

Government has established a Digital Traineeship Program, with placements for 1000 digital trainees over the next 4 years. Further, Government is also exploring a digital and data internship program, and further initiatives to build the capability needed and attract and retain data and digital skills in the APS to meet the growing emerging skill need.

