AGENDA

Date: 23 February 2024, 9.00am – 12:00pm (AEDT)
Venue: NSW Parliament, 6 Macquarie St, Sydney NSW 2000
Chair: The Hon Bill Shorten MP, Minister for the National Disability Insurance Scheme, and Government Services

Item		Action	Lead
1	Welcome	Note	Minister Shorten (Cth)
2	Update on New Zealand's data and digital priorities	Note	Minister Collins (NZ)
3	National Strategy for Identity Resilience (paper) – update on immediate initiatives	Agree	Attorney-General (Cth)
4	DDMM 2024 Workplan	Agree	Minister Shorten (Cth)
Delivering a secure, convenient, voluntary and inclusive Digital ID and verifiable credential experience for citizens			
5	Digital ID and verifiable credentials (paper)	Agree	Minister Shorten (Cth)
6	Digital Inclusion (paper)	Agree	Minister Uibo (NT)
7	Cyber Security update (paper)	Note	Minister O'Neil (Cth)
Reforming cross-jurisdictional data and digital platforms, services and protocols			
8	Artificial Intelligence Assurance Framework update (paper)	Agree	Minister Dib (NSW) Minister Shorten (Cth)
9	Third National Data Sharing Work Program (paper)	Agree	Minister Shorten (Cth)
10	National Disability Data Asset and Australian National Data Integration Infrastructure update (paper)	Agree	Minister Shorten (Cth)
Transforming services around life events			
11	National Life Events Program (paper)	Agree	Minister Shorten (Cth)
12	Life event: Birth of a Child (paper)	Agree	Minister Steel (ACT) Minister Shorten (Cth)
Other business			
13	Communique (paper)	Agree	Minister Shorten (Cth)
14	Next meeting	Note	Minister Shorten (Cth)

Members

Cth	Senator the Hon Katy Gallagher The Hon Bill Shorten MP (a/g chair)	**SA**	The Hon Andrea Michaels MP
NSW	The Hon Jihad Dib MP	**TAS**	The Hon Madeleine Ogilvie MP
VIC	The Hon Gabrielle Williams MP	**ACT**	Mr Chris Steel MLA
QLD	The Hon Bart Mellish MP	**NT**	The Hon Selena Uibo MLA
WA	The Hon Stephen Dawson MLC	**NZ**	The Hon Judith Collins MP

Agenda Item 1: DDMM Actions Register

#	Action	Agenda item	Lead	Status
23 June 2023				
1	DDMM Senior officials to support finalisation of the Multilateral Data Sharing Agreement to the satisfaction of all parties.	Reforming cross-jurisdictional data and digital platforms, services, and protocols	All jurisdictions	**Completed.** Cth and seven jurisdictions have signed the Multilateral Data Sharing Agreement.
2	Commonwealth to report back at next DDMM on scope of work to implement recommendations of the Review of cross jurisdictional program of life events.	Transforming services around life events	Cth (DTA)	**Completed.** Paper to come forward at 23 February 2024 DDMM.
29 September 2023				
3	s47B [redacted]	Reforming cross-jurisdictional data and digital platforms, services and protocols	NSW	s47B [redacted]
4	Commonwealth to work with SA around access to data from the National Disability Insurance Scheme.	Reforming cross-jurisdictional data and digital platforms, services and protocols	Cth (Finance)	**In progress.** The National Disability Insurance Agency, with support from Finance, is working closely with SA on a resolution following a meeting on 8 December 2023.
5	All jurisdictions to notify the Commonwealth of any substantial issues with exposure draft Digital ID Bill and supporting Rules no later than 13 October 2023.	Delivering a seamless digital ID experience for citizens	All jurisdictions	**Completed.**

#	Action	Agenda item	Lead	Status
6	Commonwealth to work with jurisdictions to update Digital ID Roadmap.	Delivering a seamless digital ID experience for citizens	Cth (Finance)	**In progress.** A draft National Digital Identity Strategy to be prepared by mid-2024 with collaboration and input from all jurisdictions. This will establish the vision and strategy for digital ID in Australia and inform subsequent work on a more-detailed Roadmap.
7	Commonwealth to circulate details of any Senate Committee consideration of Digital ID Bill, once known.	Delivering a seamless digital ID experience for citizens	Cth (Finance)	**Completed.** Minister Gallagher wrote to Data and Digital Ministers on 21 December 2023 providing notice of the Senate Inquiry. Advice was also sent to Data and Digital Senior Officials on 12 January 2024.
8	Minister O'Neil and the Department of Home Affairs to have follow-up discussions with Tasmania about cyber security issues.	Delivering a seamless digital ID experience for citizens	Cth (Home Affairs)	**Completed.**
9	Digital Inclusion Working Group to consider the recommended actions for DDMM from the First Nations Digital Inclusion Advisory Group initial report.	Delivering a seamless digital ID experience for citizens	NT	**Completed.** Paper to come forward at 23 February 2024 DDMM.
10	Secretariat to publish the communique on the DDMM website.	Other business	Cth (Finance)	**Completed.** Communique published on 29 September 2023.
11	Secretariat to confirm details of out-of-session process for agreeing National Cabinet annual report.	Other business	Cth (Finance)	**Completed.**
12	Secretariat to confirm date of first in-person DDMM to be scheduled early in 2024.	Other business	Cth (Finance)	**Completed.**

23 February 2024

Agenda item 3: National Strategy for Identity Resilience: Update on immediate initiatives

RECOMMENDATIONS

That members:

a) **Agree** the proposed way forward to progress the immediate initiatives under the National Strategy for Identity Resilience.

KEY ISSUES

On 23 June 2023, the Data and Digital Ministers Meeting (DDMM) approved the National Strategy for Identity Resilience (the Strategy) and agreed that detailed plans and budgets for initiatives under the Strategy would be considered at future meetings, following the Government response to the myGov User Audit. The Government released its response to the myGov User Audit Report on 18 December 2023.

The immediate initiatives under the Strategy support a stronger, more secure and accessible digital economy, and are a step towards making a greater range of biometrically anchored and verifiable credentials available for the majority of Australians. This will enhance the accessibility of government and everyday services, while making online transactions safer.

The Commonwealth, states and territories have joint responsibility for the development and implementation of these initiatives. Each initiative is built to complement the other and to work together to strengthen identity resilience for all Australians, and support the growth of the digital economy.

The immediate initiatives under the Strategy are:

- *Update of the National Identity Proofing Guidelines*
- *Identity resilience education and awareness*
- *Cohesive national approach for responding to the identity security aspects of data breaches*.

Update of the National Identity Proofing Guidelines

The National Identity Proofing Guidelines (the Guidelines), released in 2016, provide guidance for government and private sector organisations on identity proofing, which is the process for establishing whether a person is who they say they are.

The Commonwealth, through the Attorney-General's Department, has consulted through the National Identity Resilience Group[1] and developed a plan for the update of the Guidelines to strengthen identity proofing practices, achieve greater national consistency in identity proofing, and to provide better support for agencies that undertake identity proofing. The following key areas of the Guidelines have been identified for update:

- *introduction of design principles* to articulate what the Guidelines are designed to do and set out a consistent approach to identity proofing
- *enhanced risk management framework* to demonstrate the link between undertaking a risk assessment and determining an appropriate identity proofing level

[1] The National Identity Resilience Group, with representatives at the SES Band 1 level from states, territories and relevant Commonwealth agencies with responsibility for identity security, was established in 2022 and underpins jurisdictional engagement for the National Strategy for Identity Resilience.

- *development of consistent national identity proofing processes* across jurisdictions for core credentials, including minimum proofing standards
- *consistent national identity proofing requirements* for both physical credentials and digital identity proofing, aligned with the Trusted Digital Identity Framework (TDIF). Pending passage of the Digital ID Bill through Parliament, the TDIF would be replaced with the Accreditation Rules.
- *simplified credential weighting* to simplify guidance on what identity credentials can be used in the proofing process and what weighting they should be given.

Identity Resilience Education and Awareness

The Optus and Medibank data breaches highlighted a lack of consistency on identity resilience and remediation messaging. It also highlighted that information was not centralised, and therefore made it difficult for Australians to access. A stocktake of existing online identity security resources undertaken by the Attorney-General's Department confirmed that many businesses, and Commonwealth, state and territory government agencies have their own websites on protecting identity information, however, there are challenges for Australians in navigating these different sources of information.

The first phase of this initiative will provide a central point for access to identity security education and awareness resources on a comprehensive, dedicated website, hosted by the Australian Government, and support consistent messaging on identity security, resilience and remediation. The website is designed as a tool to navigate sources of information rather than to replace them and provides a starting point for identity messaging, including links to jurisdictional information. The website will build on work completed by the NSW Department of Customer Service, ID Support NSW website, which was stood up in 2021 to support NSW residents with compromised credentials. The website also includes other Commonwealth and jurisdictional resources such as guidance for enhancing cyber security and combatting scams. The Attorney-General's Department has agreement from the Commonwealth and state government agencies whose identity security content will be referenced on the website.

There is further work to be done to coordinate the messaging and strengthen the connections between identity security and cyber resilience and scams awareness, to increase identity resilience. The next phase proposed under this initiative will involve the Attorney-General's Department working with relevant agencies to leverage existing programs and activities to improve education and awareness of the connections between identity resilience, cyber resilience and scams awareness. This includes improved outreach, and coordinating messaging, through the 2023-2030 Australian Cyber Security Strategy.

Cohesive National Approach for Responding to the Identity Security Aspects of Data Breaches

This initiative seeks to support rapid and efficient whole of government responses in the event of a cyber incident, and minimise further harm to individuals, business and government. A single, highly visible point of expertise, or Centre of Excellence, was originally envisaged to support the management of identity security aspects of data breaches at a Commonwealth level, and work with state and territory bodies. However, as detailed below, the Australian Government through the establishment of the National Office of Cyber Security in the Department of Home Affairs, has put in place arrangements to respond to the identity security aspects of data breaches to improve the timeliness and efficiency of remediation activities.

- The establishment of the National Cyber Security Coordinator, the National Office of Cyber Security and the Cyber Security Response Coordination Unit within the Department of Home Affairs provides national oversight for cyber security incident response and a single point of coordination for whole-of-government cyber incident consequence management. The Cyber Security Response Coordination Unit works closely with affected entities and governments to manage consequences following a data breach or cyber-attack.

- The Cyber Security Response Coordination Unit is formalising working groups which are convened on an incident-by-incident basis. The Identity Services and Security Working Group (the Working Group) will be the primary mechanism to coordinate identity remediation and consequence management following significant cyber incidents. The Working Group may also operate alongside the National Coordination Mechanism when the threshold for a National Coordination Mechanism is met.
- The Working Group will be co-chaired by the Attorney-General's Department and Services Australia and will work closely with states, territories and Australian Government agencies to de-conflict and support consequence management efforts.
- Additionally, the National Coordination Mechanism, including Australian Government, state and territory governments and industry and private sector stakeholders, is now being used to support whole-of-government responses to the consequences of cyber incidents. This change was formalised in the Australian Government Crisis Management Framework on 29 September 2023. To further support the National Coordination Mechanism, the Australian Cyber Response Plan and Australian Cyber Incident Consequence Management Plan are currently being developed.

In light of these actions, the Commonwealth proposes that this initiative be considered to be finalised, with further reviews and updates to be considered if needed, for example if required in response to a future cyber incident.

NEXT STEPS

1. The Attorney-General's Department will continue to work with states and territories to progress the Strategy's immediate initiatives, including by:
   - updating the National Identity Proofing Guidelines, including consideration of timeframes, costings and legislative implications
   - consolidating and providing consistent messaging on identity security, resilience and remediation for individuals and businesses on the IDMatch website
   - leveraging existing Commonwealth government awareness programs and activities to enhance identity resilience and security messaging, including seeking opportunities to more effectively coordinate messaging and strengthen the connections between identity security and cyber resilience and scams awareness.
2. As agreed at the June 2023 meeting, the Commonwealth will present detailed plans and budgets for initiatives at future Data and Digital Ministers Meetings, noting the Government response to the myGov Audit was delivered on 18 December 2023.

PREPARED BY: Commonwealth

23 February 2024

Agenda item 4: DDMM 2024 Workplan

RECOMMENDATIONS

That members:

a) **Endorse** the milestones and deliverables set out in the DDMM 2024 Workplan

KEY ISSUES

DDMM's annual Workplan outlines the key milestones and deliverables on three strategic priorities:

- Delivering a secure, convenient, voluntary and inclusive Digital ID and verifiable credential experience for citizens
- Reforming cross-jurisdictional data and digital platforms, services and protocols
- Transforming services around life events

PREPARED BY: COMMONWEALTH

Attachment A: DDMM 2024 Workplan

2024 DDMM Work Plan

Item		**Milestones and deliverables**
1	Delivering a secure, convenient, voluntary and inclusive Digital ID and verifiable credential experience for citizens	*National Cabinet tasking – delivering government services fit for the digital age through citizen-centric solutions* • Provide strategic oversight and drive intergovernmental collaboration to implement a federated ecosystem of digital identities and lift productivity across the community, business and government. ○ Update National Digital Identity Roadmap to demonstrate how all jurisdictions will contribute to delivery of interoperable national Digital ID (mid-2024). ○ Develop nationally consistent policy settings for verifiable credentials (mid-2024). *Digital Inclusion* • Explore initiatives to promote digital inclusion including community trust and individual consent, and improve digital ability across the Australian community, in collaboration with the First Nations Digital Inclusion Advisory Group and Regional Connectivity Ministers Roundtable (first half of 2024). *Identity resilience* • Implement short term initiatives and begin work on medium term initiatives under the National Identity Resilience Strategy. *Cyber Security* • Improve Australia's national resilience to cyber security threats and address the consequences of cyber security incidents.

2	Reforming cross-jurisdictional data and digital platforms, services and protocols	*Third National Data Sharing Work Program (6 months from March 2024 to Aug 2024)* • Develop nationally consistent data on family and domestic violence services to deliver better outcomes for service users and address cross-jurisdictional data challenges. • Develop a National Data Catalogue of public data assets. Agree national metadata standard to facilitate ingestion of state and territory metadata into the Australian government data catalogue. • In collaboration with Disability Reform Ministers, oversee the digital infrastructure, data integration approach and associated governance arrangements to deliver the National Disability Data Asset (NDDA), also known as the Australian National Data Integration Infrastructure (ANDII). Promote the elements of ANDII which can be used to streamline data sharing across other policy domains and coordinate cross-jurisdictional data integration. • Review of the third National Data Sharing Work Program and its outcomes (Sep/Oct 2024). *Government use of artificial intelligence* • Develop and agree a framework for a nationally consistent approach to the assurance of government use of artificial intelligence (mid-2024).
3	Transforming services around life events	*Life events: Birth of a child project* • Completion of the pilot phase and delivery of the birth registration service (calendar year 2024) and full evaluation thereafter. *Cross-jurisdictional life events program* • Develop and implement a five-year plan to make it easy for people to find and do what they need to across all levels of government. This plan will leverage findings from the review of the Cross-Jurisdictional Program of Life Events and work underway in jurisdictions.

Data and Digital Ministers Meeting

23 February 2024

Agenda item 5: Digital ID and verifiable credentials

RECOMMENDATIONS

That members:

a) **Discuss** and provide feedback on the key digital ID priorities proposed in this paper.

b) **Agree** that all jurisdictions will work together to progress a National Digital Identity Strategy, by mid-2024, to guide development of an updated National Digital ID Service Transformation Roadmap.

c) **Note** the update on the progress of Commonwealth Digital ID legislation.

d) **Note** the update on the Cross-Jurisdictional Verifiable Credentials Working Group.

KEY ISSUES

Commonwealth Digital ID legislation – implications for states and territories

On 30 November 2023 Commonwealth Digital ID legislation was introduced into the Australian Parliament. The legislation is intended to strengthen the existing voluntary accreditation scheme; provide legislative authority for the Australian Government's Digital ID System (AGDIS) to expand; strengthen privacy and consumer protections; as well as setting up a stronger governance framework including to establish the ACCC as the interim Digital ID regulator. The legislation has been referred to the Senate Economics Legislation Committee for inquiry with the Committee's report due on 28 February 2024.

The draft legislation supports the existing Commonwealth federated approach to Digital ID by providing a legal basis to expand the current AGDIS and broader Digital ID Accreditation Scheme. It is anticipated that the future of digital identity in Australia will increasingly be based upon the adoption of verifiable credentials and digital wallets. The challenge ahead for all jurisdictions is how best to integrate emerging approaches, such as state and territory driver licences, with existing approaches, such as the Commonwealth AGDIS and myGovID.

The Cross-Jurisdictional Verifiable Credentials Working Group is a first step in bringing the Commonwealth and the states and territories together to address this challenge.

The Commonwealth is continuing to engage with states and territories to work through outstanding issues raised in feedback on the draft legislation, for example law enforcement access to Digital ID information.

The immediate impact on states and territories upon commencement of this legislation is expected to be relatively minor. The use of Commonwealth Digital ID services will remain voluntary, and all services currently connected to the AGDIS can continue to use the AGDIS in the same way that they do now. The Commonwealth is working with states and territories to develop legislative instruments (transitional rules) to facilitate this process, subject to the passage of the primary legislation. State and territory entities onboarding services following the initial transition period can seek approval from the Digital ID regulator.

The commencement of legislation will create several medium and longer-term opportunities for states and territories. The AGDIS will be capable of onboarding accredited state and territory identity service providers and attribute providers alongside the existing Commonwealth identity provider (myGovID) and attribute provider (Relationship Authorisation Manager). Having both state and territory as well as Commonwealth digital IDs available through the AGDIS presents opportunities for mutual recognition of digital IDs and/or sharing of verified attributes, and will support citizen choice in how they access government services. Direct adoption is also an option for jurisdictions that may prefer not to develop their own digital ID.

The states and territories will have the option to access the Commonwealth accreditation scheme in lieu of establishing their own parallel processes. Further down the track there is also the potential for use of government digital IDs by people accessing services from private sector entities (should this be desirable).

Decisions of whether to seek accreditation for a digital ID service and whether to onboard a digital ID to the AGDIS will remain voluntary and will rest with each jurisdiction to determine.

Importantly the commencement of Commonwealth legislation should not interfere with established digital identity initiatives already implemented by states and territories, such as digital driver licences in South Australia, NSW, QLD, and Victoria, or development of state-based digital IDs.

Additional detail on the development of the legislation can be found at **Appendix A**.

Indicative digital ID priorities for 2024-25

In February 2023, Data and Digital Ministers Meeting (DDMM) agreed the current Digital ID Roadmap, bringing together input from the Commonwealth and all states and territories to show the range of digital ID activities planned for 2023-24. Development of the Roadmap was guided by four core design principles agreed by DDMM.

The Roadmap is intended to outline the shared outcomes and vision across jurisdictions as well as the key priority activities across the Commonwealth and the states and territories in coming years. Ahead of preparing an updated Roadmap there is a need to develop a National Digital Identity Strategy that will establish the vision and strategy for digital ID across the jurisdictions. While the necessary analysis to develop the Roadmap is dependent upon the direction set by the National Digital Identity Strategy and will occur in coming months, a number of likely priority activities have already been identified.

For the Commonwealth this will include activities to:

- establish and support the legislated AGDIS and Accreditation Scheme, including establishing the Digital ID Regulator, finalising rules and standards, transitioning current participants, and developing a Digital ID inclusion strategy;
- commence technical policy development and consultation to support future phases of the expansion of the AGDIS, which would enable onboarding of state and territory identity service providers and the use of myGovID to access private sector services (respectively);
- working across the Commonwealth and with states and territories to identify potential policy pilots that may help expand the Digital ID program across Australia (refer **Appendix B**);
- ongoing work to onboard additional states and territories to the Face Verification Service;
- work with jurisdictions to develop nationally consistent policy settings for verifiable credentials, including public and targeted consultation with participants and other key stakeholders; and
- progressing work to rename myGovID.

For the states and territories priority activities may include:

- ongoing review and development of digital identity strategies across multiple jurisdictions;
- developing policy advice in NSW and Tasmania on possible legislation for digital credentials;
- developing a state-based digital ID in NSW and perhaps other jurisdictions;
- exploring the feasibility of a digital driver licence for Western Australia and the Northern Territory;
- progressing the digital driver licence pilot in Victoria;
- exploring the potential for implementing other digital credentials in NSW and Victoria; and
- continued work with Austroads on pilots for interoperable digital driver licences.

Proposed approach to update the Digital ID Roadmap

The Digital ID Roadmap needs to be anchored by a clear, national vision for digital ID as well as being guided by an agreed strategy that contemplates the strategic objectives and outcomes common across all jurisdictions.

Since DDMM endorsed the Digital ID Roadmap there have been a range of developments relevant to digital ID across jurisdictions. These include activities such as the Commonwealth's introduction of Digital ID legislation to the Australian Parliament, passage of the related Identity Verification Services Bill, release of the National Strategy for Identity Resilience, the growing development and adoption of digital driver licences in state and territory jurisdictions, and continued developments in relevant emerging technologies including verifiable credentials.

The Digital ID Roadmap is due for a review to ensure it remains current and fit for purpose to demonstrate the relevant initiatives that contribute to a national interoperable digital ID system, and DDMM's tasking from National Cabinet to deliver government services fit for the digital age through citizen-centric solutions. In particular the Roadmap should be guided by an agreed vision and national strategy for digital ID and aim to capture shared digital ID outcomes that are sought by all jurisdictions. Additionally, the Roadmap should be transparent in differentiating between funded and unfunded initiatives to avoid potential confusion and misalignment of expectations.

Recognising this, we propose a top-down approach to update the Roadmap to reflect shared outcomes and vision across jurisdictions through the following approach:

1. commence with a face-to-face workshop with senior officials from all jurisdictions to discuss a shared national digital identity strategy that sets the parameters and objectives for the Roadmap;
2. bring back a draft National Digital Identity Strategy for DDMM endorsement in mid-2024 that sets the vision and strategy to guide development of a detailed Roadmap;
3. coordinate input from jurisdictions to prioritise and sequence planned activities to outline how the vision, strategy, and shared outcomes can be achieved (noting for some jurisdictions, including the Commonwealth, this will have dependencies on Budget funding processes);
4. review the format and focus of the document and reshape it so it remains fit for purpose.

The comeback with the updated National Digital Identity Strategy in mid-2024 will also outline the proposed approach to develop, iterate, and maintain the updated Roadmap, ensuring this is aligned with other processes (e.g. reporting to National Cabinet).

Verifiable credentials update

Since its establishment in September 2023, the Cross-Jurisdictional Verifiable Credentials Working Group has met four times in the last four months to progress work on establishing nationally consistent policy settings for verifiable credentials. Terms of reference for the group have been settled and high-level policy principles have been agreed. The working group has also undertaken an environmental scan of initiatives underway across jurisdictions to understand potential opportunities for alignment and collaboration.

The working group reconvened in January 2024 with an immediate focus on developing recommendations for a consistent approach to the key policy issue of trust frameworks to support interoperability of verifiable credentials across jurisdictions.

BACKGROUND

National Cabinet requires DDMM to maintain a Digital ID Roadmap, including reportable milestones. On 29 September 2023, Ministers commissioned the next update to the Digital ID Roadmap to ensure it continues to be fit for purpose as Digital ID transitions to a fully legislated regime.

At the 23 June 2023 meeting Ministers agreed to the establishment of a cross-Jurisdictional verifiable credentials working group, co-led by the Commonwealth, Queensland and Victoria, to shape the policy for verifiable credentials and guide implementation.

NEXT STEPS (INCLUDING ANY COMEBACKS)

1. Prepare a draft National Digital Identity Strategy with collaboration and input from all jurisdictions for presentation to DDMM in mid-2024.
2. The Commonwealth will continue to consult with states and territories on the Digital ID legislation and provide further updates on progress following the conclusion of the Senate Committee process, and more broadly on its Digital ID Program including any developments on policy pilots.
3. The Cross-Jurisdictional Verifiable Credentials Working Group will undertake a review of priority policy issues from January 2024, commencing with trust frameworks.

PREPARED BY: Commonwealth

Appendix A: Commonwealth Digital ID legislation update

Appendix B: Potential Commonwealth Digital ID policy pilots

Appendix A: Commonwealth Digital ID legislation update

On 30 November 2023 the Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023 were introduced into the Australian Parliament in the Senate. The Bills were referred to the Senate Economics Legislation Committee for inquiry and the deadline for public submissions to the Committee closed on 19 January 2024.

The Bills introduced into the Senate reflected feedback from public consultation on the draft legislation, which ran from 19 September to 10 October 2023. In total 112 formal submissions were received, as well as a number of informal submissions including feedback from some states and territories. The Senate Economics Legislation Committee is due to report on the Bills by 28 February 2024.

Consultation responses contemplated a range of matters including voluntariness of Digital IDs and the importance of alternative channels; privacy safeguards and law enforcement access to Digital ID information; the phased expansion of the AGDIS to states and territories and the private sector; mandatory versus voluntary accreditation for Digital ID providers; and the ability to use Digital IDs to meet Anti-Money Laundering and Counter-Terrorism Financing customer identification requirements.

On 21 December, Minister Gallagher wrote to each ministerial representative sitting on the DDMM with an update on key issues arising from the Digital ID consultation that are relevant for DDMM and the introduction of legislation to Parliament. This included the following key issues:

- **Law enforcement access to personal information:** Minister Gallagher proposed an approach for annual reporting to Parliament on law enforcement agency access to personal information held by accredited Digital ID service providers. The Commonwealth is now considering possible amendments to the Bill on this issue and will be engaging with jurisdictions in due course.
- **Phasing:** Feedback on the proposed phased expansion of the AGDIS indicated that phasing needs to allow jurisdictions and the private sector to invest in a reasonable timeframe. Minister Gallagher will undertake further consultation and engagement on phasing and other matters raised during consultation.
- **Charging arrangements:** Minister Gallagher confirmed that state and territory services will not be charged to use myGovID as relying parties within the AGDIS. This is consistent with current arrangements and reflects the substantial value and data that jurisdictions provide that supports the use of Digital IDs. The Commonwealth will review charging arrangements, including through consultation with jurisdictions, ahead of private sector Digital ID providers being able to join the AGDIS.
- **Transitional arrangements under the Digital ID legislation:** The Commonwealth Department of Finance has requested that departments in each jurisdiction responsible for services currently participating in the unlegislated AGDIS indicate whether they intend to transition to the legislated AGDIS. The Department is also working with relevant agencies to understand how this transition will be appropriately authorised, including the role of state and territory ministers, cabinets, and the National Cabinet. The Commonwealth will provide further detail via our continued engagement with jurisdictions at the official level, as well as subsequent meetings of the DDMM.

The Commonwealth also continues to consult with Queensland regarding the potential impacts of privacy safeguards in the legislation on operations of state agencies that may choose to become accredited as Digital ID service providers.

Appendix B: Potential Commonwealth Digital ID policy pilots

The Commonwealth is currently considering potential policy pilot activities and trials that could commence in 2024-25, such as:

- Working to ensure Digital IDs can be used for *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* purposes;
- Exploring policy interventions and additional communications activities to enhance the inclusivity of Digital ID and better understand what particular groups need to adopt and use Digital ID; and
- Exploring expanded use cases relevant to authorisation and nominees – such as individuals nominating others to act on their behalf, caring and disability use cases, powers of attorney and instances where businesses need to authorise another trusted business to act on their behalf.

These activities will be considered jointly between the Commonwealth and jurisdictions with a view to how they may potentially expand the Digital ID program across Australia, fostering opportunities to drive interoperability both across Australia's governments and between government and the private sector.

23 February 2024

Agenda item 6: Digital Inclusion

RECOMMENDATIONS

That members:

a) **Endorse** the proposed actions for three priority initiatives.

b) **Note** the two initiatives that will be referred to Commonwealth agencies for further consideration.

c) **Agree** that the Digital Inclusion Working Group continue to explore ways to improve digital inclusion.

KEY ISSUES

The Digital Inclusion Working Group (DIWG) reviewed the 22 digital inclusion initiatives identified and recommended by the First Nations Digital Inclusion Advisory Group (FNDIAG) in their initial report. Using structured prioritisation criteria the DIWG arrived at five significant initiatives and recommends the following actions:

Priority Initiative (FNDIAG Report)	Recommended action	Lead
Establish a National Device Bank to provide households with refurbished devices	Jurisdictions to explore existing local arrangements (eg local councils, community groups, commercial and recycling enterprises) and identify fresh opportunities to donate used government devices to these programs.	All jurisdictions (report to DDMM via DIWG)
Explore alternative technologies beyond traditional terrestrial solutions	DDMM and all jurisdictions to maintain a watching brief over emerging communications technologies, including LEO satellites, mesh wifi and public safety networks	DDMM/DIWG
Develop a national map of connectivity data in collaboration with states and territories	Jurisdictions to contribute to an integrated national connectivity map, leveraging work already in progress, to be developed in collaboration with the Communications Department and FNDIAG.	Commonwealth (Communications) with jurisdiction participation

Jurisdictions recognise there are practical and policy matters within each of their governments that will need to be addressed to support the design and delivery of these three initiatives.

The establishment of a national device bank recognises the leading role governments can play in encouraging reuse of devices and providing a means of digital connectivity to digitally disadvantaged groups. Governments recognise that many local initiatives are already in place and will seek to enhance these where practical.

Developing an integrated national connectivity map builds on work already in progress in many jurisdictions; it offers an opportunity to strengthen baseline data measures against Target 17 of the National Agreement on Closing the Gap and track progress towards achievement of that target.

The following two initiatives will require financial and feasibility consideration by Commonwealth agencies. It is appropriate to refer these initiatives to officials in the Finance and Communications agencies for further assessment and reporting back to DDMM.

Priority Initiative (FNDIAG Report)	Recommended action	Lead
Partner with telcos to provide grants for community Wi-Fi	DIWG to engage with Communications Department (DITRDCA) to initiate community wi-fi grants program, co-funded by states and territories. Funding commitments across all governments are yet to be determined.	Commonwealth (Communications)
Increase the Telephone Allowance to reflect contemporary use on telecommunications services	Refer to Department of Finance for further consideration. Will require coordination across jurisdictions for data collection.	Commonwealth (Finance)

The DIWG recognises that these and the remaining FNDIAG recommendations will continue to be progressed under the Communications Minister, through the FNDIAG. The DIWG will continue to collaborate with FNDIAG in pursuit of improved digital inclusion outcomes consistent with achieving Target 17 of the National Agreement on Closing the Gap.

The DIWG also recognises that although the challenges of digital connectivity and affordability across Australia are not solved, there is limited scope for the DIWG to explore further options in these areas. Instead, the focus of this group's digital inclusion efforts can shift towards other dimensions of digital inclusion, noting the complex relationships between all elements of inclusion.

The proposed implementation of a national digital identity scheme will demand a sharper focus on digital ability across the community. The DIWG intends to continue to explore other ways to improve digital inclusion, such as support for digital identity inclusion, maximising community trust, explaining individual consent, and improving collective digital ability for individuals and businesses.

BACKGROUND

At the June 2023 meeting, Ministers agreed the following:

Digital inclusion Ministers noted the goal of Target 17 of the National Agreement on Closing the Gap is for Aboriginal and Torres Strait Islander people to have equal levels of digital inclusion by 2026. Ministers agreed to explore options to advance digital inclusion for First Nations people in collaboration with the First Nations Digital Inclusion Advisory Group.

The DIWG has met regularly through 2023 to discuss, assess and prioritise these initiatives, with a focus on access to digital connectivity for First Nations people. This approach recognises that there are many cohorts across Australia that are digitally excluded to some extent and improving outcomes for First Nations people will improve inclusion for many other groups.

All jurisdictions and the Commonwealth (Finance, Communications) have been represented. The DIWG issued a standing invitation to the FNDIAG Chair and co-Chair, which has been taken up. The FNDIAG has also invited the DIWG Chair to its meetings. There is strong collaboration and alignment between these two bodies.

NEXT STEPS

1. Subject to DDMM endorsement, DIWG to engage with leads to commence work on initiatives
2. DIWG to continue to explore nationally significant digital inclusion initiatives to propose to Ministers.
3. DIWG to continue regular reporting to DDMM on project progress, including improved data measurement against Target 17 of the National Agreement on Closing the Gap.

4. DIWG members to engage within their jurisdictions to ensure maximum leverage of inclusion related initiatives and policies across different arms of government and the community sector.

PREPARED BY: NORTHERN TERRITORY

23 February 2024

Agenda item 7: Cyber Security update

RECOMMENDATIONS

That members:

a) **Note** the update on implementation of the *2023-2030 Australian Cyber Security Strategy*.

b) **Note** the update on the work of the National Cyber Security Coordinator.

KEY ISSUES

Implementation of the 2023-2030 Australian Cyber Security Strategy

- Since the release of the *2023-2030 Australian Cyber Security Strategy* (the Strategy) and associated Action Plan on 22 November 2023, Commonwealth agencies and departments have commenced implementation of the Strategy in alignment with Horizon 1.
  - Horizon 1 seeks to strengthen cyber foundations across 2023-25. The Commonwealth will address critical gaps in cyber security, build better protections for vulnerable citizens and businesses, and support cyber maturity uplift.
  - Building on this, Horizon 2 (2026-28) will scale cyber maturity across the whole economy. The Commonwealth will make further investments in the broader cyber ecosystem, continuing to scale up the cyber industry and grow a diverse cyber workforce.
  - Horizon 3 (2029-30) will advance the global frontier of cyber security. The Commonwealth will lead the development of emerging cyber technologies that adapt to new risks and opportunities across the cyber landscape.
- To remain current, the Action Plan will be reviewed every two years, with actions being updated, added and removed as required.
- On 19 December 2023, the Commonwealth released the *2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper* to facilitate industry consultation on two proposed areas of legislative reform: new legislated initiatives to address gaps in existing regulatory frameworks, and amendments to the *Security of Critical Infrastructure Act 2018* to strengthen protection of Australia's critical infrastructure.

Update on the work of the National Cyber Security Coordinator

- Deputy Secretary Hamish Hansford is acting in the role of the National Cyber Security Coordinator (the Coordinator), following Air Marshall Darren Goldie's recall to Defence on a workplace matter related to a previous role.
- The Coordinator and the National Office of Cyber Security (the Office) have supported several recent high-profile cyber incidents, including St Vincent's Health Australia (SVHA) and DP World Australia.
- The Office commenced coordinating a response to the SVHA incident on 20 December 2023.
  - As at 9 January 2024, SVHA advises that the incident has not impacted service delivery across its health care networks, and no patient data or personal identifiable information has been identified as impacted yet.

  - The investigation into the incident remains ongoing and SVHA has committed to keeping Home Affairs informed as its analysis develops.

- The Office led the coordinated response to the cyber incident impacting DP World Australia in early November. The incident impacted port services across four major Australian ports from 10 to 13 November 2023. The incident involved the exfiltration of data, including personal identifiable information from DP World employees.

- In early 2024, the Office finalised a Lessons-Learned Review of the coordination and consequence management response to the HWL Ebsworth cyber incident in 2023. Stakeholders in the HWL Ebsworth review process overwhelmingly noted the benefit of having a centralised function for significant cyber security incidents requiring consequence management.
- Key learnings from the Office's engagements (across all incidents) are being incorporated into sector-level incident response and consequence management playbooks. The playbooks are a key deliverable under the Strategy, and will assist government and industry to coordinate and collaborate during their incident response and consequence management phases.

National Office of Cyber Security Exercise Program

- Since being established on 1 May 2023, the Office has delivered six cyber security consequence management exercises, including major exercises with the Financial Services and Markets, Transport (Aviation), and Telecommunications sectors.

- The Office is actively working toward future exercises with the Financial Services and Markets, Data Storage and Processing, and Health Care and Medical sectors this year. Additional exercises are being scoped for other sectors.

BACKGROUND

Update on the work of the National Cyber Security Coordinator

The Office conducted three major exercises with critical infrastructure sectors in 2023:

- Financial Services and Markets – Banks and ASX (May 2023). This exercise focused on information sharing arrangements, communication channels, regulatory frameworks and consequence management activities that may be activated when responding to a cyber incident impacting critical assets and/or systems within the Financial Services and Markets sector.

- Aviation (June 2023). The exercise allowed participants to explore the respective approaches to crisis response between Sydney Airport Corporation, major airlines and government. Discussion included the use of legislation, frameworks and plans, board engagement and stakeholder considerations required to enable a joint response to significant cyber security incidents impacting Sydney Airport.

- Telecommunications (September 2023). The exercise explored the various information sharing arrangements, communication channels, regulatory frameworks and consequence management activities that may be involved in responding to a cyber incident impacting critical assets and/or systems within the Telecommunications sector.

NEXT STEPS

1. The Department of Home Affairs will continue to progress the implementation of the 2023-2030 Australian Cyber Security Strategy.

2. The 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper has gone out for public submissions. Consultation will close on 1 March 2024.
3. Targeted consultation will supplement the formal Consultation Paper. Town Halls, Deep Dives and bilateral engagements are being scheduled for February 2024.

PREPARED BY: COMMONWEALTH

23 February 2024

Agenda item 8: Artificial Intelligence Assurance Framework update

RECOMMENDATIONS

That members:

a) **Endorse** the Initial National Framework for AI Assurance (Attachment A).

b) **Agree** to next steps for development of a Final National Framework for AI Assurance.

KEY ISSUES

National AI Working Group

Following agreement at the 23 June 2023 DDMM meeting, the Commonwealth and all states and territories established the National Artificial Intelligence (AI) Working Group. The purpose of the Working Group, co-led by the Commonwealth and NSW, is to work towards a nationally consistent approach to the assurance of AI in government.

To develop the nationally consistent approach, Working Group members investigated the suitability of the NSW AI Assurance Framework as a foundation document to be adapted by each jurisdiction, including by self-assessing various elements of the Framework in terms of their applicability. Subsequently, a deep dive was held to enable discussion on challenges for national consistency, including where NSW processes were not directly applicable in all jurisdictions. This led to the proposed structure of the national approach to AI assurance to set out high level principles and processes as part of an initial framework with further detail to be developed for agreement by mid-2024.

As part of its remit to inform the alignment of national approaches, the National AI Working Group has also acted as a forum for members to share work underway in their jurisdictions towards safe and responsible use of AI. This includes:

- NSW Government shared their final version 2.0 of the NSW AI Assurance Framework, following updates to accommodate generative AI projects, improvements to usability and addressing longer-term policy impacts.
- The Queensland Government presented on their roll out of their QChat tool, which uses AI technology to ask questions and complete tasks within a Queensland Government context.
- The Tasmanian Government's development of interim guidance on use of AI technologies.
- The Public Record Office Victoria's development of guidance on record keeping for AI technologies which was published in November.
- The Commonwealth shared details on the plans and approach for the whole-of-government trial of Copilot for Microsoft 365, including the development of user guardrails.

Initial National Framework for AI Assurance

The National AI Working Group has developed an Initial National Framework for AI Assurance (the Initial Framework) which, if endorsed, will form the basis of the nationally consistent approach to assurance of AI in government. This is comprised of two main components: alignment to the Australian AI Ethics Principles; and a high-level set of assurance processes which would be implemented across the Commonwealth and all states and territories.

Alignment to the Australian AI Ethics Principles provides a flexible base for AI assurance. This will allow Commonwealth, state and territory frameworks to develop over time, in line with the quickly evolving nature of AI technology, while ensuring nationally consistency.

The second component of the Initial Framework sets out key overarching assurance processes which have been agreed as feasible for each jurisdiction to implement as independent AI assurance processes. This seeks to ensure that each jurisdiction is addressing the same important areas of AI assurance, including governance, assessment of human, societal and environmental impacts, reviewing transparency mechanisms, assessing data and information governance, assessing cybersecurity and privacy considerations, and obtaining legal advice for projects meeting a certain risk threshold.

Next steps towards development of the Final National Framework for AI Assurance

1. **Initial implementation:** Subject to endorsement of the Initial Framework, individual Working Group members will begin work in their jurisdictions to implement the Initial Framework while the Working Group builds out the Final National Framework for AI Assurance (the Final Framework). Jurisdictions will make best efforts to align to the Initial Framework as closely as practicable, while exercising judgement on integration with existing systems and processes and any necessary adjustments for their context and circumstances.
2. **Development of Final National Framework:** Concurrently, the Working Group will work towards a Final Framework for agreement at the mid-year meeting of the DDMM. This will include:
   a. Consultation with members on whether any initial lessons learned from implementation of the Initial Framework can be addressed in the development of the Final Framework.
   b. Exploration of inclusion of additional assurance processes and further guidance on implementation of processes. For example this might include AI project risk rating categorisation and identification, a recommended structure for establishing an AI assurance review body and other areas where national guidance may be of use.
   c. Coordination of approval pathways to enable agreement to the Final Framework. See Attachment B for a proposed timeline for a Final National Framework for AI Assurance.

BACKGROUND

At the 29 September 2023 DDMM meeting, Ministers agreed to continue working towards a nationally consistent approach to the safe and ethical use of artificial intelligence by governments. Ministers agreed principles which commit jurisdictions to collaborate, align approaches to ethical use of artificial intelligence by governments and continually improve in response to technological developments.

NEXT STEPS

1. Jurisdictions to work towards implementation of the Initial Framework.
2. The National AI Working Group to build on the Initial Framework to develop a Final National Framework for AI Assurance.
3. The Commonwealth and NSW to comeback to DDDM in mid-2024 with outcomes on the Final National Framework for AI Assurance.

PREPARED BY: COMMONWEALTH and NSW

Attachment A: Initial National AI Assurance Framework

Attachment B: Proposed timeline for a Final National Framework for AI Assurance

Initial National Framework for AI Assurance

A nationally consistent approach is a key step towards safe and ethical use of artificial intelligence by governments in Australia. Working towards a nationally consistent approach will ensure that the application of AI projects in government is subject to a similar standard of risk assessment across jurisdictions. It will also reduce duplication and resources spent from developing individual processes and initiatives in isolation.

This document sets out principles and best practice processes as the base elements for an Initial National Framework for AI Assurance for governments in Australia. This document should be used to inform the development of jurisdictions' independent AI assurance processes, through following the recommendations outlined, while exercising judgement on adjusting to context where appropriate. Jurisdictions are expected to implement these processes and principles agreed by states, territories and Commonwealth representatives of the National AI Working Group to achieve consistency in their respective jurisdictions.

Australia's AI Ethics Principles

Australia's AI Ethics Principles are proposed to be used for the national base approach. This will enable a flexible base for AI assurance that will allow national frameworks to develop over time in line with the quickly evolving nature of AI technology. Jurisdictions are encouraged to adapt these principles to their existing frameworks and ethics principles, as well as issuing additional guidance to support interpretation in their individual contexts.

Australia's AI Ethics principles are:

- **Human, societal and environmental wellbeing**: AI systems should benefit individuals, society and the environment.
- **Human-centred values**: AI systems should respect human rights, diversity, and the autonomy of individuals.
- **Fairness**: AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.
- **Privacy protection and security**: AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.
- **Reliability and safety**: AI systems should reliably operate in accordance with their intended purpose.
- **Transparency and explainability**: There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI, and can find out when an AI system is engaging with them.

- **Contestability**: When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
- **Accountability**: People responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

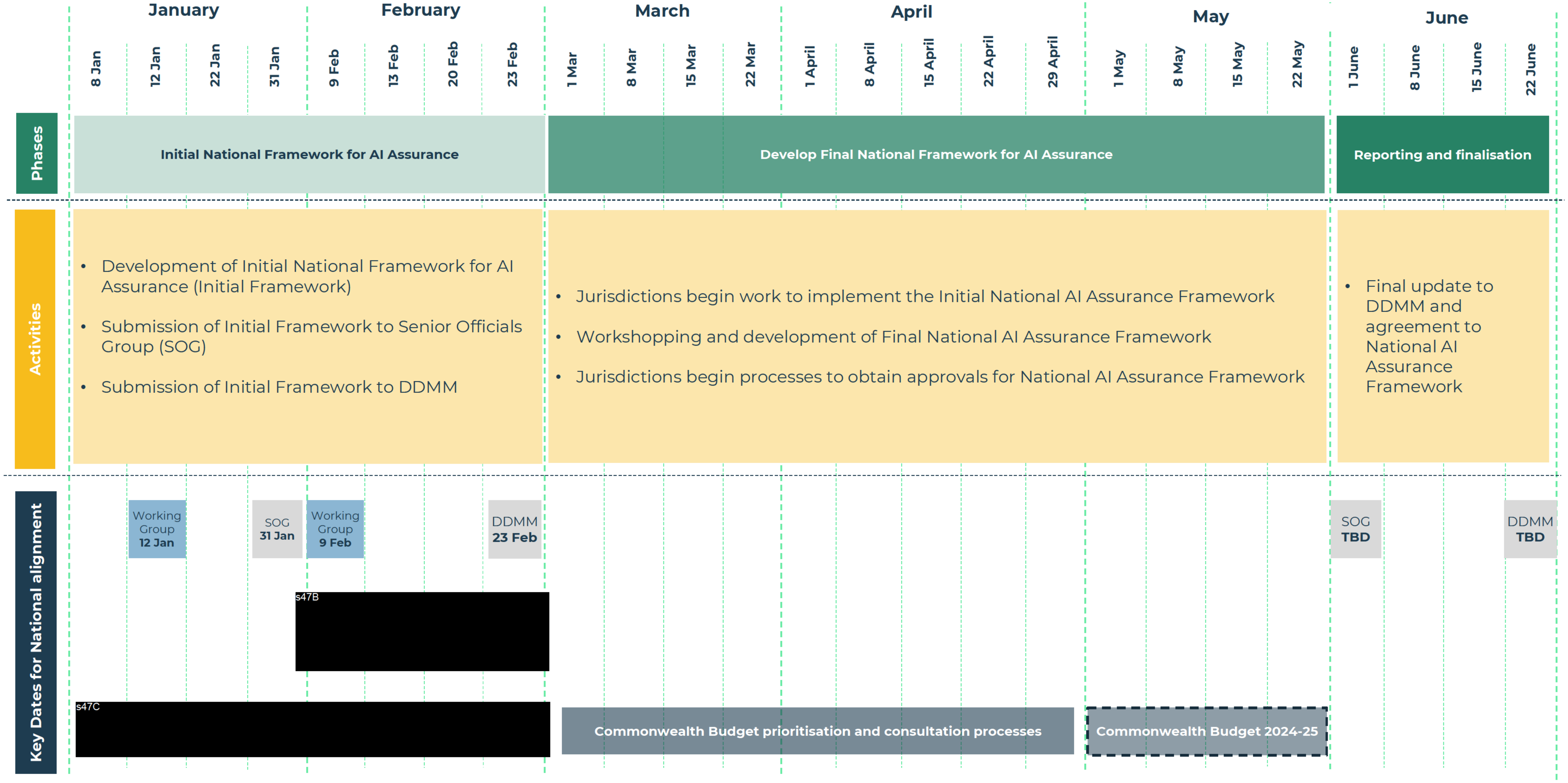
National processes for AI assurance

The below list reflects work by the National AI Working Group, to identify processes considered as best practice for AI Assurance based on the NSW AI Assurance Framework. These processes were agreed by Working Group members to inform the development of AI assurance processes across jurisdictions to ensure national alignment.

Assurance Process	Description
AI Assurance Review Body	Refers to the establishment or designation of an AI Assurance Review Body to review completed AI Assurance Framework project assessments and ensure assurance process requirements are adequately addressed. It is recommended that the AI Assurance Review Body review projects over a specified risk or financial threshold.
Human, societal and environmental impact considerations	Refers to the assessment of a project's potential impact and benefits on human, societal and environmental wellbeing, which could be achieved through implementing the following mechanisms into the assurance process: - Review alignment with human rights obligations - Community engagement plan - Benefits realisation management plan - Environmental impact assessment
Legal advice	Refers to the assessment of a project's requirement for specific legal advice based on the risk profile of the project or other relevant factors.
Transparency mechanisms	Refers to the assessment of the project's transparency mechanisms, so the general public are aware of when they are being significantly impacted by AI and can contest these outcomes.
Privacy Considerations	Refers to the assessment of the project's processes to manage, monitor and protect the privacy of individuals and government data to ensure compliance with relevant privacy legislation. Recommended practices include but are not limited to: - Undertaking a Privacy Impact Assessment

	- Seeking advice from the Privacy Commissioner (or relevant role) - Developing a Privacy Management Plan
Protective and cyber security considerations	Refers to the assessment of the project's implementation of protective security practices for AI projects, that consider risks including but not limited to: foreign ownership, control or influence, mis/dis-information, and democratic integrity.
Data Governance	Refers to the assessment of the project's system of decision rights and accountabilities for data related processes, including for example Indigenous data sovereignty and governance considerations.
Information Governance	Refers to following relevant guidelines where appropriate to ensure effective handling of personal and sensitive information: - Information classification, labelling and handling guidelines for personal information - Reasonably ascertainable identity in the definition, regulation and handling of personal information

2024



Phases

- Initial National Framework for AI Assurance
- Develop Final National Framework for AI Assurance
- Reporting and finalisation

Activities

- Development of Initial National Framework for AI Assurance (Initial Framework)
- Submission of Initial Framework to Senior Officials Group (SOG)
- Submission of Initial Framework to DDMM

- Jurisdictions begin work to implement the Initial National AI Assurance Framework
- Workshopping and development of Final National AI Assurance Framework
- Jurisdictions begin processes to obtain approvals for National AI Assurance Framework

- Final update to DDMM and agreement to National AI Assurance Framework

Key Dates for National alignment

Working Group **12 Jan**

SOG **31 Jan**

Working Group **9 Feb**

DDMM **23 Feb**

SOG **TBD**

DDMM **TBD**

s47B [redacted]

s47C [redacted]

Commonwealth Budget prioritisation and consultation processes

Commonwealth Budget 2024-25

23 February 2024

Agenda item 9: Third National Data Sharing Work Program

RECOMMENDATIONS

That members:

a) **Agree** the third Work Program include a project on Family and Domestic Violence (Attachment A).

b) **Agree** the third Work Program include two cross-cutting system reform initiatives (Attachment A)

   i. Streamlining the development of Enduring Linked Data Assets - a national data integration system that supports multiple policy uses

   ii. Establishing a metadata standard to support the simple and consistent discovery of Commonwealth, State and Territory data.

c) **Note** the progress made to implement recommendations from the Review of the Intergovernmental Agreement on Data Sharing (Attachment B).

KEY ISSUES

National Data Sharing Work Program

Under the Intergovernmental Agreement on Data Sharing (IGA), Data and Digital Ministers are responsible for agreeing and overseeing a National Data Sharing Work Program (Work Program) to focus national effort on specific time-limited data sharing areas.

Projects for the Work Program fall into two streams:

- projects in agreed priority data sharing areas are led by the relevant portfolio Minister with support from Data and Digital Ministers
- over-arching system reform initiatives led by Data and Digital Ministers.

Each Work Program runs for six months, and the third Work program is to commence from 1 March 2024. The proposed projects for the third Work Program are:

Work Program Project	Project type	Lead jurisdiction
Nationally consistent data on Family and Domestic Violence	Portfolio specific	Commonwealth (Department of Social Services and Australian Institute of Health and Welfare)
Establishing a metadata standard to support the simple and consistent discovery of Commonwealth, State and Territory data	System reform	Commonwealth (The Office of the National Data Commissioner)
Streamlining the development of Enduring Linked Data Assets - a national data integration system that supports multiple policy uses	System reform	Commonwealth (Australian Institute of Health and Welfare) and Australian Capital Territory (ACT)

For the Nationally consistent data on Family and Domestic Violence project, Victoria has agreed to work with the Australian Institute of Health and Welfare to explore the feasibility of the proposed test data flow (milestone 2).

For the Establishing a metadata standard to support the simple and consistent discovery of Commonwealth, State and Territory data project, Queensland has agreed to work with the Office of the National Data Commissioner to test ingestion of state and territory data into the Australian Government Data Catalogue test environment (milestone 3) ahead of the rollout of a National Data Catalogue. Further information on the proposed projects is at Attachment A.

Update on the implementation of the IGA Review

At the 29 September 2023 Data and Digital Ministers Meeting (DDMM), Ministers noted the findings of the IGA Review Report and agreed six overarching opportunities for improvement. An update on the implementation of these actions is at Attachment B.

BACKGROUND

Under the IGA, portfolio specific projects require endorsement from one Commonwealth portfolio Minister and at least two responsible state or territory Ministers to progress to Data and Digital Ministers for consideration. All jurisdictions are expected to use best endeavours to participate in and allocate resources to agreed Work Program projects, unless they decide to formally opt-out.

In advance of the third Work Program commencing on 1 March 2024, progress has been made to implement the outcomes from the review of the IGA, agreed by DDMM on 29 September 2023 (Attachment B). A plan to uplift awareness of the IGA and Work Program has been created and implemented, as well as improvements to Work Program design and implementation.

NEXT STEPS

1. Commence Work Program on 1 March 2024
2. Comeback to DDMM with an update on Work Program progress

PREPARED BY: COMMONWEALTH

Attachment A: Summaries of Work Program Proposals

Attachment B: Update on implementation of IGA Review recommendations

Nationally consistent data on Family and Domestic Violence project

Lead Agency: Commonwealth (Australian Institute of Health and Welfare and Department of Social Services)

Summary: DDMM agreed at their 29 September 2023 meeting to work with the Women and Women's Safety Ministerial Council to progress data sharing to support Family, Domestic and Sexual Violence Services nationally. This project seeks to support the National Plan to End Violence against Women and Children 2022-2032, by determining how data can be used to deliver better outcomes for people who access family and domestic violence services nationally.

CURRENT CHALLENGES

- Systems and institutions do not effectively support and protect people impacted by violence.
- Service and prevention programs are not fully effective, culturally responsive, intersectional, and accessible.
- National evidence base requires improvement by working towards consistent terminology and monitoring and evaluation frameworks, and by strengthening collection and sharing of data and evidence.

KEY PROJECT MILESTONES

- **April 2024: Draft recommendations report**
  - Draft report with recommendations for prototype data collection.
- **May 2024: Test data flow**
  - Test data flow arrangements between Commonwealth and at least one state or territory.
- **June 2024: Final report**
  - Final report with recommendations provided to DDMM.
- **June 2024: Data sharing**
  - DDMM considers data sharing stage of the prototype project.
- **August 2024: Summary of agreed approach for prototype data collection**
  - Draft report with agreed approach for the prototype data collection

PROJECT OUTCOMES

- Final recommendations report for prototype national Family and Domestic Violence specialist services data collection.
- Test data flows between Commonwealth and at least one state or territory.
- Specifications, governance, and ethics approvals for the prototype data collection (beyond August 2024).

Establishing a metadata standard to support the simple and consistent discovery of Commonwealth, State and Territory data

Lead Agency: Commonwealth (Office of the National Data Commissioner)

Summary: A National Data Catalogue will support inter-jurisdictional data sharing, access, and use across all jurisdictions. This national standards-based product will bring together multiple data inventories held and managed by Commonwealth, state, and territory governments. It will streamline data discovery and shorten the time taken to identify and access relevant data. The National Data Catalogue project is an extension of the project on the second Work Program. This second tranche of the project looks to take the technical requirements developed in tranche one and use them to inform the build of the Australian Government Data Catalogue (AGDC), and subsequently test those requirements in a pilot.

DDMM agreed at its 23 June 2023 meeting that the second tranche of the National Data Catalogue project should proceed for consideration for the third Work Program.

CURRENT CHALLENGES

- No national standard to capture metadata.
- Currently no framework or system to host a National Data Catalogue.
- Unknown capability of the Australian Government Data Catalogue (AGDC) to ingest metadata records from state or territory catalogues.

KEY PROJECT MILESTONES

- **March 2024: Confirm scope of work**
  - Agree which jurisdictions will participate in the testing of metadata ingestion into the AGDC.
- **April 2024: Agree metadata standards**
  - Agree on national standards for metadata and ensure alignment.
- **May 2024: Test ingestion into AGDC**
  - State or territory metadata ingested into AGDC for testing and evaluation of performance.
- **July 2024: Develop roadmap for National Data Catalogue**
  - Develop and agree a roadmap for transitioning from AGDC and individual state and territory catalogues, towards a national catalogue.
- **August 2024: Evaluation of outcomes and consideration of next steps**

PROJECT OUTCOMES

- Extend the Office of the National Data Commissioner metadata standards to state and territory data custodians to achieve alignment for the National Data Catalogue.
- Demonstrated ability for the AGDC to ingest metadata from state and territory data custodians (in a test environment).
- Preliminary identification of high-value, in-scope state and territory data assets.

Streamlining the development of Enduring Linked Data Assets - a national data integration system that supports multiple policy uses

Lead Agency: Australian Institute of Health and Welfare (AIHW) and Australian Capital Territory (ACT)

Summary: This project seeks to identify how data sharing under the National Disability Data Asset (NDDA) and Australian National Data Integration Infrastructure (ANDII) (such as hospitals and Medicare Consumer Directory data) can support a new national integration system. The national integration system includes a range of existing (e.g. the Person Level Integration Data Asset (PLIDA)) and planned (e.g. Life Course Data Asset) data assets and projects. This project will address barriers to interjurisdictional data sharing by defining how we can reduce the number of disparate data sharing projects, different governance and legal models used, to create streamlined, safe data sharing.

CURRENT CHALLENGES

- Lack of clarity around how the current data integration system works now and how it can transition to a more streamlined national system and continuing to deliver projects using models we know are ineffective and burdensome.
- Duplicative data requests for various data assets.
- Limitations of current legislative landscape.
- Lack of clarity how the whole system can be designed to support a 'share once, use often' model.

KEY PROJECT MILESTONES

- **June 2024 – Draft paper for consultation with Data & Analytics Working Group and ANDII Board**
  - Agree and define how data flows and data integration methods will bring together common datasets for reuse in other national data assets.
- **August 2024 – Final paper and communication materials**
  - Finalised paper and accompanying communications materials developed and agreed.

PROJECT OUTCOMES

- Shared understanding across governments of the relationship between the NDDA and ANDII to other data integration initiatives, including references to what currently works well.
- Improved ability to scope, plan and deliver other interjurisdictional data integration initiatives that build sensibly on the ANDII and NDDA and other infrastructure as appropriate.
- Develop a framework or criteria along with diagram to evaluate and prioritise the best use of the new integration infrastructure.
- Develop best practice guidance for implementing governance arrangements and requirements for future use cases (based on NDDA and ANDII learnings).
- A truly national data integration system with streamlined data sharing and integration that makes best use of national data holdings to inform policy and outcomes for the community.

IGA review outcomes

	Action	Status	Description of activity
1.	Increase awareness and understanding of the IGA and the National Data Sharing Work Program across all jurisdictions	**Ongoing.**	- Communications Plan developed and being implemented. - IGA published on state and territory government websites. - Finance worked with DDMM Data & Analytics Working Group to develop three data sharing factsheets on DDMM the IGA and the Work Program. They have now been published on Finance's website and on Data professions community of practice. - Work to enable references to IGA and Work Program to be added to relevant Australian Public Service Commission training modules. - Regularly scheduled presentations by project leads to DDMM Data & Analytics Working Group introduced.
3.	Uplift data maturity across all jurisdictions	**Ongoing.**	- Time-limited DDMM Senior Officials Group working groups, chaired by South Australia, have been stood up to address Data Quality and Open Data approaches nationally. Their Terms of Reference were agreed by DDMM Senior Officials Group out of session on 13 December 2023. - Two data sharing system-reform projects recommended for endorsement in third Work Program.
4.	Amend Schedule D to update reference from Data Sharing Guide to DAT Act and reference National Agreement on Closing the Gap	**Complete.**	Schedule D to IGA updated.
5.	Amend Schedule A to review IGA and its Schedules following 5 years of operation	**Complete.**	Schedule A to IGA updated.

6.	Support better project outcomes through appropriate Work Program design	**Ongoing.**	- Three projects recommended for endorsement in third Work Program. - National Data Catalogue project carried forward from second to third Work Program, given its significant contribution the data sharing system. - Nomination and Endorsement Process has been refined, including by: o Finance worked with DDMM Data & Analytics Working Group to develop Work Program Welcome Pack which will be shared with project leads for Work Program 3. o Extension of the Nomination and Endorsement timeline, to allow adequate time to accurately scope and refine project plans. o All prospective projects leads have presented their project plans to the Data & Analytics Working Group directly, to improve coordination of nominations across jurisdictions.
7.	Prioritise projects with adequate resourcing	**Ongoing.**	- Nomination form revised to include authority for the project post Work Program, clear objectives for the sprint and senior governance oversight from project leads' organisation. - Work Program Transition Plan developed and agreed by Data & Analytics Working Group in June 2023.

23 February 2024

Agenda item 10: National Disability Data Asset and Australian National Data Integration Infrastructure update

RECOMMENDATIONS

That members:

a) **Note** progress made to deliver the National Disability Data Asset and Australian National Data Integration Infrastructure including:

   i. The majority of jurisdictions have signed the Multilateral Data Sharing Agreement and a National Disability Data Asset Bilateral Schedule

   ii. Two draft Data Sharing Agreements have been shared with jurisdictions

   iii. Establishment of the Australian National Data Integration Infrastructure Board and National Disability Data Asset Council.

b) **Agree** the proposed approach to build momentum for the continued intergovernmental partnership:

   i. Further consult and iteratively co-develop key project artefacts data custodians require to enable signing of data sharing agreements authorising supply of data for a National Disability Data Asset Release 1 in mid-2024

   ii. Consult and co-develop outputs from Release 1 for public release from mid-2024.

c) **Agree** to support State and Territory hospitals data, together with key Commonwealth datasets relating to disability and health, being the priority for inclusion in Release 1 (mid-2024).

KEY ISSUES

The National Disability Data Asset (NDDA) project has made significant progress in building trust with the disability community, establishing the ICT to host the data, and the governance ecosystem for data sharing across all governments. The project remains in the establishment phase and is forecasting a 6 -month delay to the sharing of data agreed in NDDA Bilateral Schedules.

To bring focus and maintain momentum, the project is targeting 3 outputs from mid-2024:

1. Insights into the scope and composition of the disability population based on a new disability indicator methodology
2. Inaugural use of the data asset for the January 2025 release of Australia's Disability Strategy Outcomes Framework publication
3. The ability for accredited users to request access to the data asset from July 2024.

Nearly all jurisdictions have signed overarching agreements to support the NDDA and its supporting infrastructure, the Australian National Data Integration Infrastructure (ANDII). However, negotiating and establishing data sharing agreements for sensitive and personal data not previously routinely shared across all jurisdictions under new legislation (the *Data Availability and Transparency (DAT) Act 2022)* and/or for a new purpose (the NDDA and ANDII) remains the key project challenge.

- Data custodians, from all jurisdictions have highlighted a number of project artefacts they need before they will be able to enter into data sharing agreements. These include a NDDA Data Access, Use and Release Protocol (including Freedom of Information (FOI) and Complaints Policy) and a Data Breach Management Plan.

- The Commonwealth NDDA partners (the Department of Social Services (DSS), Australian Bureau of Statistics (ABS) and Australian Institute of Health and Welfare (AIHW)) and states/territories committed at the inaugural ANDII Board meeting of 8 December 2023 to develop and endorse critical project artefacts (Attachment A) by March 2024 to support signing of data sharing agreements.
- The final Commonwealth NDDA Privacy Impact Assessment, draft NDDA Privacy Statement and ANDII IRAP (Infosec Registered Assessors Program) Certificate were shared in December 2023.

Data custodians have also highlighted a range of internal processes (Attachment B) that must be completed post finalisation of these artefacts, for example, conducting their own privacy impact assessments, legal reviews and security assessments. These processes require time, with 3 months being typical. Early data contributors to the NDDA Release 1 in mid-2024 is encouraged.

Jurisdictions will need to be accredited under the Data Availability and Transparency Act 2022 (DAT Act) to access the NDDA data during later phases of the project. To use the data in the NDDA, each jurisdiction will need to have at least one DAT Act accredited user that will act as an agent until other departments within their jurisdiction are ready to apply for accreditation. The Department of Health WA, and several key Commonwealth agencies are already accredited users including the Department of Health and Aged Care, the Australian Bureau of Statistics, the Australian Institute of Health and Welfare, and the Department of Social Services. Applications from jurisdictions are being prioritised for accreditation by the National Data Commissioner. The National Data Commissioner encourages early applications from those who are yet to apply for accreditation.

Data sharing progress

Data Sharing Agreements (DSAs) outline data custodian controls, acceptable uses by dataset and operationalise the Multilateral Data Sharing Agreement (MDSA) principles.

Templates have been developed to facilitate consistency across individual DSAs and simplify the DSA negotiation process. Of note, the templates have Commonwealth endorsement from the Australian Government Solicitor (AGS) and Office of National Data Commissioner (ONDC) that they provide the basis for legally sound DATA Scheme data sharing arrangements.

Two draft DSAs covering 4 data sets identified for sharing in the NDDA Bilateral Schedules (the Commonwealth Data Over Multiple Individual Occurrences (DOMINO) and State/Territory Admitted Patient Care, Non-Admitted Patient Emergency Department Care and Non-Admitted Patient National Best Endeavours Data Minimum National Data Sets (collectively known as hospitals data) have been developed and were shared in December 2023. This illustrates the DSA templates in practice.

The proposed Release 1 NDDA in mid-2024 will represent the first sharing of data for the NDDA under the Intergovernmental Agreement on Data Sharing. It is therefore important the first release includes both Commonwealth and state and territory data (Attachment A). Hospitals data has been agreed in NDDA Bilateral Schedules and is essential for three new measures in the Australia's Disability Strategy Outcomes Framework. The hospital data is already held by one of the NDDA partners (AIHW) and is ready to be integrated into the data asset once approval has been received by state and territory data custodians.

BACKGROUND

The NDDA project is being led by DSS, ABS and AIHW in partnership with states and territories. DSS are the Senior Responsible Officer for the project. The ABS and AIHW support the delivery and ongoing management of the ANDII, with the ABS responsible for the ANDII ICT solution.

Governments have made substantial progress on the ANDII technical and data governance infrastructure design. This includes progressing the ICT build, design of the national data linkage model, design of data products and the development of data governance, privacy, and ethics frameworks to ensure data sharing for the ANDII to deliver the NDDA is safe, secure, legal and ethical.

On 2 March 2023, Minister Rishworth advised states and territories of the Commonwealth's conditional offer to meet jurisdictions' co-funding contribution to build the NDDA, providing jurisdictions agree to co-governance arrangements and supply of data to the NDDA by signing up to the NDDA MOU, a bilateral schedule to the MOU and the MDSA.

- All jurisdictions have signed the NDDA MOU.
- The MDSA contains broad settings and safeguards for data to be used within the NDDA, ANDII and future domain assets. DDMM Senior Officials are signatories of the MDSA and, as of 19 January 2024, all bar one has signed.
- The NDDA Bilateral Schedules require signing of the MDSA to enable data sharing and payments. As of 19 January 2024, one signature is awaiting finalisation.

NEXT STEPS

1. Finalise signing of NDDA Bilateral Schedules and MDSA
2. Co-develop and deliver key NDDA project artefacts to support DSA development and signing to support NDDA Release 1 by mid-2024.
3. The DDMM Data & Analytics Working Group (D&AWG) has recommended a project be included in the third National Data Sharing Work Program to support progress on this cross-jurisdictional priority area. AIHW is leading this on behalf of Commonwealth Partners and has worked with D&AWG to develop an appropriate project for endorsement by Ministers.
4. The Commonwealth (DSS) will provide a further update on the establishment of the NDDA at the next DDMM.

PREPARED BY: COMMONWEALTH (Department of Social Services, Australian Bureau of Statistics, Australian Institute of Health and Welfare) and state and territory Jurisdictional Implementation Leads

Attachment A: Prioritised data sets, activities and project artefacts for NDDA Release 1

Attachment B: Privacy assessment example of internal processes data custodians must undertake once key project artefacts are available.

Attachment A

Priority data sets for NDDA Release 1

Dataset	Jurisdictional custodian	Needed for
Data Over Multiple Individual Occurrences (DOMINO)	Commonwealth	NDDA (content data and new disability indicator) ANDII (National Linkage Spine)
Medicare Consumer Directory	Commonwealth	ANDII (National Linkage Spine)
National Disability Insurance Scheme (NDIS)	Commonwealth	NDDA (content data and new disability indicator)
Medicare Benefits Schedule	Commonwealth	NDDA (content data)
Pharmaceutical Benefits Scheme	Commonwealth	NDDA (content data)
Hospital Data – Admitted Patient Care National Minimum Dataset (APC NMDS)	States and Territories	NDDA (content data)
Hospital data - Non-admitted Patient Emergency Department Care National Minimum Dataset (NAPEDC NMDS)	States and Territories	NDDA (content data)
Hospital data – Non-admitted Patient National Best Endeavours Dataset	States and Territories	NDDA (content data)
Disability Services National Minimum Dataset	States and Territories	NDDA (content data and new disability indicator)
Death Registrations	States and Territories	NDDA (content data)

Prioritised activities and project artefacts for NDDA Release 1

	Dec-Jan	Feb	March	April	May	June
Activities	Commonwealth, State and Territory Data Custodian negotiations (ongoing)					NDDA insights released using new disability indicator methodology. NDDA opens for Project applications and first Central Analytics Project application is lodged. NDDA Ethical Oversight Panel established
			Commonwealth data ingest commences	Commonwealth data build commences Project Data Sharing Agreement template NDDA Council Terms of Reference NDDA Charter Disability Indicator Panel formed	State and Territory data ingest commences Disability Indicator methodology endorsed by NDDA Council	
	NDDA project artefacts co-development continues DSA template discussions continue					
Project artefacts	1. Privacy Impact Assessment for the NDDA and ANDII 2. Privacy Statement for the NDDA 3. ANDII IRAP (Infosec Registered Assessors Program) Certificate Assessment – Letter of Compliance 4. ANDII Security Risk Management Plan		5. Data Access, Use and Release protocol (including FOI and complaints handling policy) 6. ANDII Security Principles Framework 7. Data Retention, Destruction and Archiving Policy 8. ANDII Data Breach Management Framework		9. NDDA de-identification strategy	10. NDDA Data Quality Framework 11. ANDII ICT Disaster Recovery and business continuity plan

Attachment B

Privacy assessment example of internal processes data custodians must undertake once key project artefacts are available [1]

Stage	Details
1. Initial determination of privacy inclusions	An initial assessment by the data custodian as to whether there is likely to be any personal information/data included within the specified project. If so, proceed to step 2.
2. Undertake a Privacy Threshold Assessment (PTA)	A preliminary assessment to help determine a project's potential privacy impacts and provide the data custodian a sense of the risk level, including whether it could be a 'high privacy risk project'. If a Privacy Impact Assessment (PIA) is assessed as required, proceed to step 3.
3. Progress to Privacy Impact Assessment (PIA) if required	A PIA is a systematic assessment that identifies the impact that a project might have on the privacy of individuals, and sets out recommendations for managing, minimising, or eliminating that impact. PIAs need to include proposed information flows, showing where data is collected, used and disclosed by each participating agency. The information flow should include the technical solution utilised for any data integration/linkage.
4. Record/register PIA results	Once complete, a PIA should be endorsed by an appropriate senior agency representative and registered by the agency. Ideally results should also be provided to relevant stakeholders for full transparency.
5. PIA implementation plan	Consider results of PIA in detail, including privacy mitigations required, the data matching protocol to be used, and proposed data governance arrangements including data sharing agreements and data access, security and audit arrangements. If legislative amendments are required, proceed to step 6.
6. Draft Code (or equivalent) if required	In some cases, legislative amendments may be required for PIA mitigations, e.g. development of a new or amended Code.
7. Seek stakeholder input and approvals	Work with relevant stakeholders (including data providers) to ensure the PIA implementation plan (and any Code) is feasible.
8. Privacy Commissioner approvals (as relevant)	Where necessary (e.g. for a new or amended Code), seek Privacy Commissioner support.
9. Ministerial approvals	Where necessary (e.g. for a new or amended Code), seek Ministerial approval for changes.
10. Parliamentary approval	Where necessary (e.g. for a new or amended Code), progress to Parliamentary approval for passing of relevant legislation.

[1] *Note: this is a 'typical' list based on general steps required. Some custodians will require more (or fewer) steps depending on their specific governance environment, including relevant legislation.*
References: www.oaic.gov.au ; https://www.ipc.nsw.gov.au/; https://ovic.vic.gov.au/privacy/

23 February 2024

Agenda item 11: National Life Events Program

RECOMMENDATIONS

That members:

a) **Agree** the Direction (Attachment A) and Framework (Attachment B) for National Life Events Program in response to the Cross Jurisdictional Life Event Review recommendation 1 and 2.

b) **Agree** that a 5-year plan, including life event initiatives informed by the jurisdictions, be brought forward for DDMM consideration in mid-2024, including any specific patterns and standards required to support them.

c) **Note** a cross-jurisdictional Governance Structure and Benefits Realisation Framework, in response to the Review's recommendations 3 and 4, will be brought forward for DDMM consideration in mid-2024.

KEY ISSUES

- The Cross-Jurisdictional National Life Events Review (the Review) highlighted the need for a revitalised approach to life events to reduce inconsistency across jurisdictions, support smaller jurisdictions to capitalise on the benefits of the life events and encourage interoperability.
- A new approach to Life Events will enable governments of all levels to be more efficient and invest more wisely into the design and delivery of life events by considering smaller, incremental, and reusable changes that will support ongoing change.
- Targeted delivery of common enablers that promote consistency, interoperability, and develop capability, will provide a more seamless and connected experience across Commonwealth, State and Territory services.
- The new direction (Attachment A) and Framework (Attachment B) provides a common way for DDMM to identify initiatives and projects that will support the Life Event Program, while reducing the costs and resource implications of delivery.
    - To support the new approach to Life Events, a 5-year plan of proposed initiatives – including proof of concepts, standards, and patterns – will be developed for DDMM consideration in mid-2024 to practically apply the Framework and promote distribution of effort across jurisdictions. Timing of initiatives will need to consider jurisdictional budget processes.
    - The new direction will achieve consistency, interoperability, and support building capability across agencies through development of common enablers, rather than focussed on large scale, high investment life event delivery.
    - While efficiencies are expected, there is a risk that states and territories require additional funding and resourcing to deliver initiatives and advance the maturity of their life events service provision.
- A library of patterns and standards for all Commonwealth agencies and jurisdictions will enable common approaches to the design and delivery of life events and a more consistent and connected customer experience in line with the new direction.

  - All jurisdictions will have opportunity to contribute to code libraries and standards to support interoperable design and delivery of services, and reduce the work required to connect services.
  - There is a need for increased knowledge sharing across jurisdictions, through communities of practice, which identify maturity frameworks and proposed roadmaps for delivery. This supports cross pollination of knowledge, high value support products and guidance around future planning, enabling more effective Life Events based delivery.

- The benefits of the new approach include increased visibility for DDMM of what is being delivered, active promotion of re-use, leading to interoperability, and the ability for states and territories to be involved in the National Life Events Program while implementing at their own pace.
- The Program will align life event projects and initiatives being put forward by jurisdictions, through a 5-year plan for DDMM consideration in mid-2024. This will ensure that the projects proposed, meet the requirements of the Framework, while also delivering on the 5-year plan. This plan will evolve as new initiatives are considered in future years.
- To support DDMM oversight of the projects being considered as part of the Life Events Program, while also ensuring that benefits are realised, the Program will be underpinned by a cross-jurisdictional Governance Structure and Benefits Realisation Framework (in line with the Review's recommendation 3 and 4), to be brought forward for DDMM consideration in July 2024.

BACKGROUND

- In November 2022, the DDMM requested a review of the Cross Jurisdictional Life Events Program.
- On 23 June 2023, the DDMM endorsed the findings of the Review and agreed to four recommendations to reset the direction and vision for the national life events program:
  - reset direction and vision for the national life events program;
  - establish a scalable framework for life events;
  - new shared governance structure; and
  - better define measurable benefits.
- The Life Events Cross Jurisdictional Working Group was established to co-design the response to the Review.

NEXT STEPS (INCLUDING ANY COMEBACKS)

1. The Commonwealth will continue to engage across states and territories to develop the following for DDMM consideration in mid-2024:
   - A proposed list of cross-jurisdictional life event initiatives, in line with the Framework, including any specific patterns and standards required to support it.
   - Governance Structure (as per recommendation 3 of the Review)
   - Benefits Realisation Framework (as per recommendation 4 of the Review)
   - Cross-jurisdictional 5-year plan (as committed in Government's response to the myGov User Audit, recommendation 8)

PREPARED BY: COMMONWEALTH

Attachment A: Direction for National Life Events Program (Attachment A)

Attachment B: Framework for National Life Events Program (Attachment B)

Australian Government
Digital Transformation Agency

dta

National Life Events Program

Attachment A - Vision & Direction

Response to Cross Jurisdictional Life Event Review - recommendation 1

February 2024

dta.gov.au

A new direction for Life Events

A new direction has been established to achieve the National Life event Program's vision: ***"to drive change across government, providing connected services and improving people's experience during key life events"***.

The new direction will:

- allow recommitment to the National Life Events Program from Jurisdictions and the Commonwealth, to provide validated patterns, standards and tools that enable agencies, States and Territories to advance at their own pace, towards a single vision, with visibility across the system.
- support small scale, high impact, infrastructure and capability-based initiatives to help jurisdictions design and deliver life events, rather than focusing on delivery of individual life events which require large scale funding and resourcing.

Build consistency for delivery of connected services through the provision of a library of patterns and standards.

Build interoperability between systems with code libraries and agreed standards.

Build capability in Life Events based delivery through knowledge sharing and frameworks tools.

13 enablers will drive success of the National Life Events Program

The National Life Event Program will provide oversight of, or connect with, the following enablers to promote consistency, interoperability, and develop capability, to provide a more seamless and connected experience across Commonwealth, State and Territory services.

PRACTICE ENABLERS

- BENEFITS REALISATION
- DESIGN STANDARDS AND PATTERNS
- GOVERNANCE STRUCTURES / DECISION MAKING
- 5 YEAR ROADMAP
- COMMUNITY OF PRACTICE
- DIGITAL LIFE EVENT TOOLKIT

To be managed through the Program.

INTEROPERABILITY ENABLERS

- DIGITAL IDENTITY STANDARDS
- DATA SHARING STANDARDS
- VERIFIED CREDENTIAL STANDARDS
- TECHNOLOGY MATURITY

The Program will leverage and connect with these enablers, as dependencies to the successful delivery of life events, being managed through existing Government programs.

OTHER ENABLERS

- FUNDING
- WORKFORCE
- STANDARDISED POLICY ENVIRONMENT

Success in these areas will be driven by individual Commonwealth agencies and States and Territories.

Australian Government
Digital Transformation Agency

dta

National Life Events Program

Attachment B - Framework

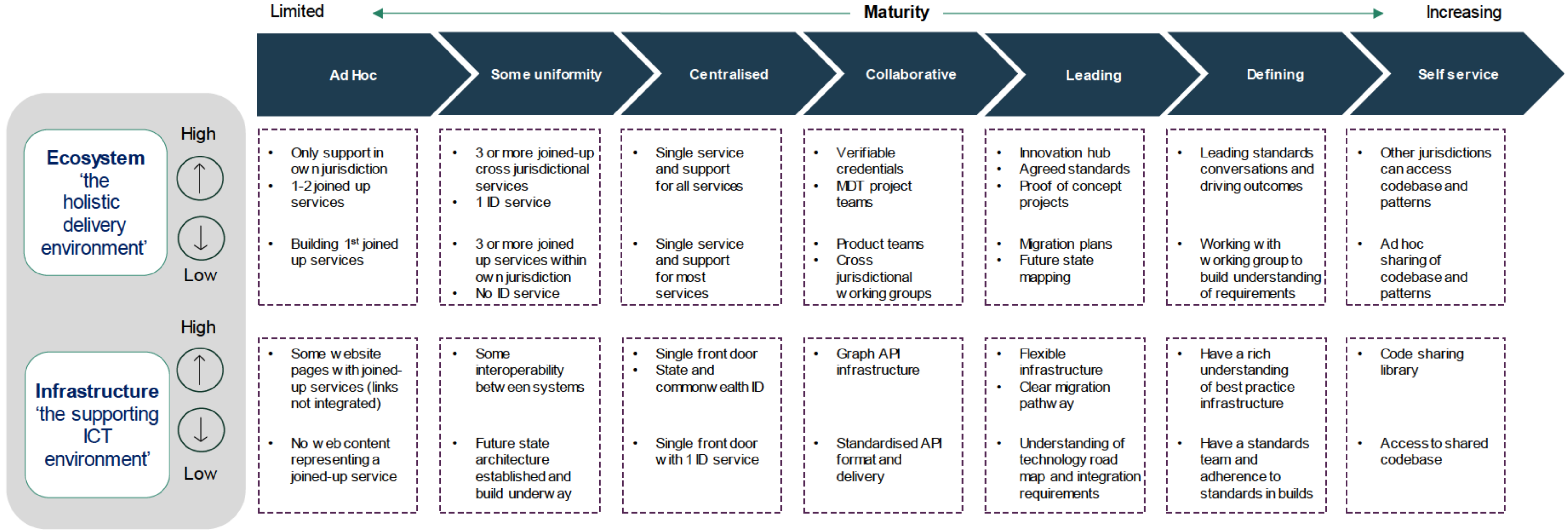
Response to Cross Jurisdictional Life Event Review - recommendation 2

February 2024

dta.gov.au

Life Events Framework

The life event framework is a diagnostic tool that jurisdictions can use, to assess capability to deliver their life event, and identify the four different domains they can improve on to advance their life event service offering.



Limited ← Maturity → Increasing

		Ad Hoc	Some uniformity	Centralised	Collaborative	Leading	Defining	Self service
Ecosystem 'the holistic delivery environment'	High	- Only support in own jurisdiction - 1-2 joined up services	- 3 or more joined-up cross jurisdictional services - 1 ID service	- Single service and support for all services	- Verifiable credentials - MDT project teams	- Innovation hub - Agreed standards - Proof of concept projects	- Leading standards conversations and driving outcomes	- Other jurisdictions can access codebase and patterns
	Low	- Building 1st joined up services	- 3 or more joined up services within own jurisdiction - No ID service	- Single service and support for most services	- Product teams - Cross jurisdictional working groups	- Migration plans - Future state mapping	- Working with working group to build understanding of requirements	- Ad hoc sharing of codebase and patterns
Infrastructure 'the supporting ICT environment'	High	- Some website pages with joined-up services (links not integrated)	- Some interoperability between systems	- Single front door - State and commonwealth ID	- Graph API infrastructure	- Flexible infrastructure - Clear migration pathway	- Have a rich understanding of best practice infrastructure	- Code sharing library
	Low	- No web content representing a joined-up service	- Future state architecture established and build underway	- Single front door with 1 ID service	- Standardised API format and delivery	- Understanding of technology road map and integration requirements	- Have a standards team and adherence to standards in builds	- Access to shared codebase

Life Events Framework (continued)

Limited ← **Maturity** → Increasing

		Ad Hoc	Some uniformity	Centralised	Collaborative	Leading	Defining	Self service
Measurement 'the way benefits are measured'	High ↑ ↓ Low	• Measure transactions. Inconsistencies in measurements • Measuring 1 or 2 elements of a single transaction	• Measure across connected services • Measuring most digital services	• Measure across the omnichannel service delivery • Measuring most digital and in-person services	• Understand service value and measure customer outcomes across jurisdictions • Measuring cross jurisdictionally across services w ith 3 measures	• Deliver consistent measures w ith adaptations for personalisation • End to end measurement and reporting of customer experience	• Driving delivery to set standards that are measured and reported upon transparently • Customer outcomes are understood and measured w ith notifications and tracking	• Performance data is readily available for all jurisdictions to access anytime • Measurements are available via a dashboard w ith alerts
Governance 'models and how they are applied'	High ↑ ↓ Low	• Some project oversight w ith agency level oversight • Governance established for each project	• Oversight and reporting across more than 1 agency • Governance oversees more than 1 project and has some consistent goals	• Oversight across many services with defined measures • All projects have 1 governance model and are aligned to centralised goals	• Oversight and delivery across all jurisdictions is given equal priority • Governance model is cross jurisdictional	• Project has clear measurable deliverables and leverages best practice delivery • Governance is targeting measurement and ongoing improvement	• Project is leveraged to help other projects through shared learning • Governance is setting the standards for future similar projects	• Project is delivered w ith a w hole of government approach and benefit • Governance is completely transparent

This framework will be validated by jurisdictional use and iterated as needed.

23 February 2024

Agenda item 12: Life Event - Birth of a Child

RECOMMENDATIONS

That members:

a) **Note** the revised timing for implementation of the Registration of Birth service; completion of the Birth of a Child pilot; and associated evaluation activities.

b) **Agree** the Birth of a Child project will return to DDMM to discuss national rollout once the full evaluation plan is finalised.

c) **Note** the key achievements, progress and challenges facing the Birth of a Child project.

KEY ISSUES

This paper aims to update members on progress, achievements and key challenges facing the Birth of a Child project.

Registration of Birth service

1. The Registration of Birth service is the final feature to complete the Birth of a Child pilot. Original project timelines anticipated delivery of this feature in the 2021-22 financial year, however delivery was delayed due to a range of factors.

   a) The project has key stakeholders and delivery partners across the health and service delivery sectors, of which the COVID-19 pandemic impacted most heavily. This caused a deliberate and significant slowing of progress while government agencies pivoted to focus on the COVID response and recovery, subsequently shifting project timelines by 12 months including the planned delivery of the Registration of Birth feature to the 2022-23 financial year.

   s47B [redacted]

2. The ACT Government and Services Australia have continued to work closely on implementation timing, noting dependencies between technical implementations and broader change management. In December 2023, the ACT Government and Services Australia developed a revised integrated work plan for end-to-end implementation of Registration of Birth. Once all dependencies were considered, a go-live timeframe of late May or June 2024 was identified and agreed.

3. Considering the revised go-live timing, the full evaluation of the Birth of a Child service is proposed to occur in the second quarter of the 2024-25 financial year. This will allow the service adequate time to operate so an appropriate amount of data is available to consider in the evaluation.

4. Consideration of further Commonwealth investment will align with the revised timeframe for the evaluation. This will also support likely timing for jurisdiction investment decisions in the context of the 2025-26 financial year.

Continued expansion of Birth of a Child service

5. Jurisdictions have expressed in principle support of onboarding additional hospitals with a strong preference to consider the outcomes of the full evaluation prior to investing further. Importantly, the evaluation will articulate the benefits for all participants in the service. It is anticipated the full evaluation will demonstrate cross government return on investment opportunities.

6. The ACT Government and Services Australia are continuing to work with the Northern Territory Government toward onboarding to the Birth of a Child service within 2024. Services Australia has worked closely with the Northern Territory through co-design and continued local engagement with midwives and hospital social workers to design and implement a tailored service for people.

7. This presents opportunities to improve access to government services for expectant mothers in urban and remote areas and to increase the number of First Nations and remote children who have an authoritative identity record created from birth. This enables increased support for the health of newborns within First Nations communities and the potential to reduce persistent disadvantage.

PROGRESS OF BIRTH OF A CHILD PILOT

- On 5 June 2023, a joint letter from Commonwealth Ministers, Minister Shorten and Minister Butler and Australian Capital Territory Ministers, Minister Steel and Minister Stephen-Smith was sent to jurisdictional Health Ministers seeking support to engage in national rollout planning of the service. Responses have been received from all jurisdictions providing support for their respective health agencies to engage in national rollout planning.
- National rollout planning with jurisdictions and co-design with the remaining Registries of Birth Deaths and Marriages will continue through 2024.
- The Project has created nationally scalable foundations that enable future life event re-use. This comprises the Life Events Notification System (LENS) which securely collects, packages, and sends relevant data to relevant government areas.
- The project is in the discovery phase for the creation of a digital consent model, providing an opportunity to deliver a reusable and transparent consent framework that supports customer control over their data and their interactions.
- The Project supports a cross-jurisdictional “tell us once” approach, exploring tailored support for customers experiencing vulnerability or with limited access to digital services and future integration and alignment with the digital identity ecosystem.
- Achievements include:
  - Since December 2020, 15,776 newborns across ACT and QLD have been enrolled in a streamlined Medicare service where data is re-used to support the creation of newborn records.
  - From November 2022 – 23, 1305 birth mothers have been successfully supported through the Centrelink service offer where data is re-used to prepopulate claims for family assistance and Electronic Proof of Birth replaces the need for parents to submit a form.
  - Through the pilot an average of 30 minutes has been saved for an estimated 93.7% of participating parents, equating to approximately 7,392 hours of time saved for parents.
  - The project has integrated the ACT Registry of Births, Deaths and Marriages (RBDM) for Notification of Birth, which has enabled the first stage of a cross government service offer for parents.
  - The integration of a myGov interface enabling parents to provide information in one place and shared across participating agencies. This is currently enabling participating parents to provide the name of their baby to Medicare and Centrelink after they leave hospital.

NEXT STEPS

1. Complete and implement the Registration of Birth service in the ACT by end June 2024

2. Evaluate the end-to-end pilot service by December 2024.

3. Continue to onboard additional hospitals to the Birth of a Child service, including hospitals within the Northern Territory, ongoing through 2024.

4. Jurisdictions to consider further investment and implementation timing, for 2025-26 budget year.

PREPARED BY: ACT and COMMONWEALTH (SERVICES AUSTRALIA)