Independent Panel
myGov user audit
1 Canberra Ave
Forrest ACT 2603

By email: Jordan.Hatch@servicesaustralia.gov.au

30 November 2022

RE: myGov user audit – AIIA Response

The AIIA is pleased to be able to provide comment as part of the myGov user audit. Please note that as well as broad member feedback, the AIIA's response is also informed by the member roundtable that took place with the myGov Audit team on 21 November 2022 in Canberra.

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit organisation to benefit members, and AIIA membership fees are tax deductible. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.
We do this by delivering outstanding member value by:
• providing a strong voice of influence
• building a sense of community through events and education
• enabling a network for collaboration and inspiration; and
• developing compelling content and relevant and interesting information.

We are unique in that we represent the diversity of the tech ecosystem from small and medium businesses, start-ups, universities and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies.

Introduction

In an address to the AIIA on 6 December 2021, then Minister for Employment, Workforce, Skills, Small and Family Business the Hon. Stuart Robert MP described myGov as a "*key piece of national infrastructure*."[1] Investing in the potential of myGov as a platform is a focus for both government and industry to advance a critical national capability.

[1] https://ministers.dese.gov.au/robert/speech-australian-information-industry-association

The AIIA sees this review as an opportunity to elevate the quality, accessibility and efficiency of services provided to businesses and individuals online. The myGov customer experience can be made more dynamic, intelligent and seamless. But ultimately the role of myGov in the national psyche can be taken to the next level, with economy-wide implications.

Timely, relevant and helpful information that both activates data and gives consumers choice around data and services will help to make myGov a platform of choice. Use of the myGov platform should result in customers feeling oriented and informed about their life journeys, be it through a visa application process, childcare enrolment or update an immunisation record. Live customer feedback will be an important driver and diagnostic tool as part of the process; not just in the sense of what customers say about the platform, but in what they do, such as their dwell time on a page and their ability to navigate pages successfully.

The fact that myGov is a digital platform should not diminish the resources and prominence afforded such a 'key piece of national infrastructure,' which is not merely an artefact, but a significant ecosystem in its own right with an opportunity to find sweeping scale. Government should give consideration to the structure and design of the Services Australia and myGov teams to ensure the platform may be managed nimbly and meaningful changes can be implemented quickly and at scale.

It is also critical that careful attention is paid to the curation and acceptance of services made available via myGov to ensure it enhances the brand and quality of customer and user experience (CX; UX). In other words, poor designed UX, apps and digital services should not be approved to be accessible via myGov and likewise, there needs to be oversight of agencies creating their own separate citizen digital front doors.

Technological uplift of government digital services and industry partnerships

Orchestration

The concept of orchestration, whereby multiple computer systems, applications and services are coordinated and managed, synthesising multiple repeatable tasks in order to execute a larger workflow or process, is an important consideration for MyGov,[2] as is the related concept of cloud orchestration, whereby infrastructure and workflows are managed and automated across cloud-based systems.[3]

Customer journey orchestration, or journey orchestration, has particular applications for the development of MyGov. This kind of orchestration uses real-time customer insights and galvanises automation to personalise customer experience (CX) and respond to such customer insights at scale.[4]

Collaborative innovation spaces

Creating the space for innovation in a collective environment where government and industry have safe places in which to innovate.

[2] https://www.databricks.com/glossary/orchestration
[3] https://www.servicenow.com/products/it-operations-management/what-is-it-orchestration.html
[4] https://www.qualtrics.com/blog/journey-orchestration/

Defence industry innovation is an exemplar of public-private collaboration.[5]The divided structure of above-the-line (**ATL**) and below-the-line (**BTL**) organisations, taken from defence industry, whereby above-the-line contractors define capability requirements and execute strategy for Defence and below-the-line organisations bid for work, design systems and deliver on capability requirements set by ATL, is a worthwhile model of delivery against capability.

Case study: Digital Identity Ministerial Advisory Council (NSW)

The **Digital Identity Ministerial Advisory Council** in New South Wales, whereby key Ministers, Department of Customer Service leaders, academics, privacy experts, banking executives, consultants, and entrepreneurs come together to execute on trust and privacy requirements and advise on a strategic direction and roadmap for digital identity in New South Wales, is a strong example of commercial and government interests coming together collaboratively in one space, galvanised by strong ministerial direction.[6]

Data considerations

Government needs to determine the specific data it requires in order to ensure a relevant customer service provision, limiting data collection so that information, whether personal or otherwise, is used in the most effective way to make services relevant. Good design and data standards are essential in this regard. MyGov could require data practices that are open-by-default, which encourage the consolidation of services by such practices as publishing open APIs.

The standards and Outcome and Technical principles that have been developed for CDR under the Consumer Data Standards project, which focus on open, robust standards that are widely used by industry, are instructive, particularly CX Principle 3:

> *CX Principle 3: The CDR is Comprehensible*
> *When interacting with the CDR, consumers are able to understand the following:*
> - *who their data is shared with;*
> - *what information is shared;*
> - *when sharing begins and ceases;*
> - *where data is shared to and from;*
> - *why their data is being requested; and*
> - *how they can manage and control the sharing and use of their data.*[7]

Government must seek to understand the whole-of-government legislative context within which technology is leveraged and data is collected and shared, including potential barriers, by considering the application of legislation such as the *Data Availability and Transparency Act*.

[5] https://www.innovationhub.defence.gov.au/about/
[6] https://www.nsw.gov.au/media-releases/new-digital-identity-advisory-council-established
[7] https://consumerdatastandardsaustralia.github.io/standards/#principles

Leading practice for platforms

API-driven capabilities such as seen is taxation, where single-touch payroll has reduced reporting burdens for employers,[8] could result in compelling use cases with service providers. MyGov has a compelling opportunity to link data in real-time based on transactions to produce customer insights, but legislative considerations may constrain progress.

'Plug-and-play' interoperability and minimum onboarding standards

The community needs to lift from the view of myGov beyond an aggregator of services to a seamless ecosystem will start with trust and transparency. With authentication and credentialing of external organisations with life journey relevance for customers, services could be incorporated as provider choices for the consumer as a 'plug-and-play' proposition sitting within a broader government policy and delivery framework. This would have a broad benefit of reducing the amount of data individual service providers need to collect. To enable incorporation into myGov, a trust mark or technical stamp that represents endorsement by government of that organisation, and the meeting of minimum onboarding standards, may need to be developed with clear guidelines for data standards and technological practices necessary to obtain the mark.

Case study: Service NSW's single view of customer

ServiceNSW is driven by the desired outcome of a single view of customer, with predictive servicing and known patterns of behaviour. The approach underpinning the development of ServiceNSW was shifting to view government as an enterprise. The 'enterprise' is focused on building repeatable architecture and assets based on functionality and capability. One of the customer considerations ServiceNSW encountered was the level of control and visibility over government data holding citizens expected. Government and industry partnering around visible control will be essential as myGov develops.

Transaction-driven customer journeys

It is important for government to remember that the number of non-government transactions across the economy vastly outstrips government transactions. Government should not seek to do what private enterprise does as its bread and butter.

Government must centre customer-facing journey design principles around pay-off and future time-saving once citizens have undergone processes. Customers encounter frustration when similar processes have to be repeated with two or more circumstances of use being linked together in the mind of the customer. Taking a methodical approach to impact and process within the customer-facing journey will yield important dividends for customer experience.

Cross-jurisdictional service delivery

Portability and interoperability between states and territories is a desirable end-state, with the agency of delivery or authority administering a certain citizen-facing process unimportant to the citizen compared to the task they are seeking to complete. The inclusion of HousingVic and the State Revenue Office Victoria are encouraging

[8] https://www.ato.gov.au/business/single-touch-payroll/

examples that should buoy the future consideration of myGov's role in expanding to state-based service provision.

Disaster-state as an exemplar?
Joint service delivery and co-location of differing government authorities in times of pandemic or natural disaster whereby state and federal agencies, together with the community services sector, work together, provide a model in which traditional delineations give way to the task at hand.

Case study: Forbes flood relief
While the high-cost and labour-intensive nature of these times of crisis are unsustainable for a daily solution, initiatives such as the 'Tell My Story Once' Form that was initiated in Forbes, with government processes supervening on the relevant information provided in the form of a customer story, could have resonance for myGov's operation.

Uncommon structural environments, combined with important common goals, can result in exemplary service delivery; but artefacts of service delivery that do not always turn into well-integrated processes once society reverts to business-as-usual. Government needs to review test-cases of disaster and pandemic-induced joint service delivery in order to discover efficient, cost-effective processes and insights for ordinary times.

Case study: Tell-us-Once (UK)
Similarly, the 'Tell Us Once' program in the United Kingdom enables citizens to inform government of a death one time, with government then informing up to seven different government organisations and some pension schemes on behalf of the citizen.[9] In Australia's federated system similar schemes flowing down to state and territory authorities could be facilitated through an expanded myGov platform.

Security

MyGov collects sensitive and personally identifiable information that must be appropriately secured to ensure citizen trust in the platform and help Australia realise its potential to be a world leader in digital citizenship. To this end, the AIIA would encourage the Government to appropriately fund and prioritise the security of MyGov.

Best-practice, robust encryption of data (at rest and in transit) that follows international standards for the design and validation of hardware and software cryptography, ISO/IEC 19790:2012 and ISO/IEC 24759:2017, is an important consideration for the security of myGov users' information. The ongoing referential integrity of data with other dispersed information systems when personal details change or conflict, must also be ensured.

Five Important Security Principles for myGov

The Government should give consideration of the following five security principles:

[9] https://www.gov.uk/after-a-death/organisations-you-need-to-contact-and-tell-us-once

1. **Consider moving from two-factor authentication to multifactor authentication.** Two-factor authentication (2FA) requires users to present two types of authentication, while multifactor authentication (MFA) requires users to present at least two (if not more) types of authentication. Today, MyGov leverages 2FA, whereby the user logs into the application (with their username and password) and is asked to provide an additional factor – a one-time code sent via text message/SMS – to verify their identity before gaining access to the application. However, as threat actors improve their ability to circumvent SMS-based 2FA, many organisations are moving to multifactor authentication (MFA), requiring users to provide additional authentication, such as biometrics or a code generated by an authenticator app.

2. **Implement Zero-Trust Principles –** Zero-Trust is a strategic approach to cybersecurity that underpins the security of an organisation by eliminating implicit trust and continuously validating every stage of a digital interaction. Zero-Trust assumes the network is compromised and brokers resource-specific access through a least-privileged approach supported by continuous authentication, authorisation, and risk evaluation for every request. Zero-Trust principles are increasingly important in the context of credential theft.

3. **Leverage automation to detect, prevent and respond to cyber security attacks.** Today, both cyberattacks and cybersecurity defences are leveraging machine learning and automation. An automated attack is one performed by a computer program rather than the attacker manually performing the steps in the attack sequence. If organisations try to defend against these attacks manually, the fight becomes man-versus-machine, with highly unfavourable odds for the organisation. To successfully protect against automated attacks, it is essential to incorporate automation into cybersecurity efforts. Automation levels the playing field, reduces the volume of threats, and allows for faster prevention of new and previously unknown threats. Automation also supports real-time incident response.

4. **Map myGov infrastructure to understand its attack surface through the eyes of the adversary.** Today, attackers regularly scan the internet to find vulnerabilities in public facing infrastructure and exploit them. Attack surface management is the process of continuously identifying, monitoring and managing all internet-connected assets, both internal and external, for potential attack vectors, exposures and risks. Attack Surface Management principles are founded in the understanding that one cannot secure what one does not know about.

5. **Simplify and consolidate across the myGov security environment.** Network complexity is the enemy of cyber defenders. It is critical that organisations simplify their ICT environments to ensure security teams have complete, continuous and consistent visibility across the network, cloud and endpoint (including Internet of Things).

Cyber security risk management program

Services should prioritise the implementation of a cyber security risk management program such as required in the *Security of Critical Infrastructure Act* as a

foundational requirement. This system is likely our most significant from a national perspective and should be delivered by organisations with the highest level of maturity.

Digital identity

Leveraging and delivering digital identity will be essential in safeguarding the delivery of connected digital services. Digital identity is a nation-building proposition with a whole-of-economy potential to uplift security across banks, telecommunications providers, health funds, and retail sectors. Attribute-sharing under a centralised common consent model against which the private sector may execute will be pivotal to Digital ID's success.

Using cutting-edge enhancements to security such as biometrics and blockchain, accommodating data and decisions from non-digital customers on digital platforms, and tiering interactions and transactions against graduated security requirements are all important considerations for myGov.

Rather than moving vast swathes of data between agencies, myGov could ensure that accreditation and authentication are provided at face-value to services, limiting the amount of data exposed in a breach affecting any one service.

Especially in the current context of high-profile data breaches, government is understandably risk-averse in its footing to data security. A mosaic of agencies, each with different security maturities and definitions, complicates the task at hand. However, the decision not to adopt or become embedded within digital, customer-facing solutions must be considered as a risk in itself. Being fit-for-purpose in a durable, fully-leveraged, nation-building manner to serve citizens for decades ahead is at stake.

Conclusion

Citizens seek out government services because they need to fulfil a need or discharge an obligation. In both cases, the information, quality and efficiency of service delivery are central indicators that a system is fit-for-purpose and serving a customer well.

Technology, including cyber security, data analytics, automation and customer journey orchestration, will be essential to government's task: equipping myGov to become the service delivery ecosystem of choice for both citizens and providers, engineered for the 21st century.

The AIIA thanks the Panel for the opportunity to respond to the user audit. If you have any questions about the content of this submission, please contact the AIIA via rachel@aiia.com.au.

Yours sincerely

Simon Bush

CEO
AIIA