

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

8 Oct 2023

2023 Digital ID Bills and Rules submission  
Australian Government

**Feedback on the draft 2023 Digital ID Bill, including notes on the introduction of myGovID in the Commonwealth workplace**

Dear Sir/Madam

As reflected in the title of my submission, and my experience working for a Commonwealth agency where myGovID has been made a compulsory requirement of employment contrary to extant Government law; I hold some concerns about the proposed *Digital ID Bill 2023*.

Towards the end of 2022, staff in my department were informed the Australian Government Security Vetting Agency (AGSVA) security clearance database; would be changing to the MyClearance database. This would require current staff (with security responsibilities), security clearance holders, applicants and those needing to update their clearance; to establish a myGovID so as to be able to access MyClearance.

At no stage prior to this change were staff:

- Informed the Commonwealth's policy on digital identity was voluntary opt-in
- Provided an alternative process for logging into MyClearance – such as maintaining their previous unique AGSVA identifier
- Provided evidence the department had conducted a Privacy Impact Assessment of the change
- Provided clarity on the authority or exemption the department was acting under to compel personnel to establish a digital identity
- Asked to provide their consent to establish a digital identity
- Made clear this change represented a significant amendment to employment conditions
- Provided evidence that a technical and security risk assessment had been undertaken of MyClearance and myGovID
- Explained what actual risks and problems were driving this change, and why this change would provide a solution
- Explained what extant legal and legislative protections there are to protect Australian citizens who establish a myGOVid, and what to do in the case of a spill/breach
- Provided assurance in relation to using private emails, and mobile phones to establish, and then to access myGovID on an ongoing basis

An enquiry to my department's senior leadership elicited a polite response, but absent substance. The then Digital Transformation Agency took a similar line – friendly, but substance free. Staff in the divisional area of my department responsible for the change would not engage on concerns raised. The department's (overall) ICT Security Manager refused to discuss whether technical and security risk assessments had been undertaken of the many elements of the system. Overall, the sole justification for digital identity has seemed to and continues to be, *'because.'*

I appreciate the current (and former) Government's clarity on the voluntary nature of Digital ID. And *Chapter 4, Part 2, Division 4, Section 71, (6), (a)* of the draft bill; appears to make it absolutely clear that the Digital ID Regulator 'must not' grant an exemption to Commonwealth entities from the underlying

principal of voluntary opt-in. Which would seem to apply to my agency. Security, condition of employment, and consent issues aside; my department is therefore almost certainly in breach of extant Government policy, and the right of an Australian citizen not to establish a digital identity.

Noting the electorate's antipathy towards any initiative which resembles a digital Australia Card (and the Digital ID is a fit on that front), consideration might be given to amending this draft to align with community values and actual wants. Australian citizens are less likely to reject establishing an individual security key (the 'key') if they understand clearly the Australian Government's only involvement is in regulating the key. The key could not be used to share information about an Australian citizen, and a citizen's use of the key to access services from or interact with government agencies would be a protected activity. Digital linking of information between departments would be explicitly banned, and most importantly this would be made clear to the public. And it would remain a voluntary option.

Unfortunately, the language of government around digital identity places its efforts under suspicion, rather than held up by the electorate as an example of the government working to protect them. The system is developed and spruiked by our well-off political, bureaucratic and corporate classes – none of whom are likely to be subject to digital intrusion in their future lives – a not unreasonable concern by everyone else. While the impenetrable legalise of the draft bill appears to lay a framework of protection for Australian citizens, once established the footprint of digital identity will only expand.

There is a reasonable and widely held concern digital identity will become a single point of aggregation without the need for a warrant. While the SIM in my workplace security swipe card holds every actual piece of personal identification an Australian citizen can hold (including my entire personal history as part of my clearance); I can establish a myGovID with only my Medicare card and territory drivers licence. This in turns provides me unfettered access to MyClearance.....using an iPhone6 and a fifteen-year-old Gmail account as part of the setting up and access process. The security benefit of introducing a Digital ID to the system is unclear.

I am unconvinced digital identity provides a solution to a problem, and cannot see how it would solve the broader and entrenched issues of poor administration, process, governance and assurance. Particularly within government. Alternatively, as a private citizen concerned about the protection of my identity online, I *might* consider setting up a security key if it was clear Government's only role was regulation, and all private information would be permanently compartmentalised and quarantined.

Yours sincerely

JF Barlow

██████████ ██████████