Ministerial responses — Report 12 of 2023[1]

1 This can be cited as: Parliamentary Joint Committee on Human Rights, Ministerial responses, *Report 12 of 2023*; [2023] AUPJCHR 119.

The Hon Michelle Rowland MP

Minister for Communications
Acting Attorney-General and Cabinet Secretary
Federal Member for Greenway

MC23-038508

Mr Josh Burns MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

By email: Human.rights@aph.gov.au

Dear Chair Josh

Thank you for your correspondence of 19 October 2023 regarding the Parliamentary Joint Committee on Human Rights' request for further information (as set out in Report 11 of 2023) on the Identity Verification Services Bill 2023 (IVS Bill) and Identity Verification Services (Consequential Amendments) Bill 2023 (Consequential Amendments Bill).

I appreciate the time the Committee has taken to review the Bills. I have enclosed the Government's response to the Committee's questions for your consideration.

I trust this information is of assistance.

Yours sincerely

[redacted]

Michelle Rowland MP
6 / 11 / 2023

Encl. Attachment A – Response to *Report 11 of 2023*: Identity Verification Services Bill 2023 and Identity Verification Services (Consequential Amendments) Bill 2023

The Hon Michelle Rowland MP
PO Box 6022, Parliament House Canberra
Suite 101C, 130 Main Street, Blacktown NSW 2148 | (02) 9671 4780

Attachment A

Identity Verification Services Bill 2023 and Identity Verification Services (Consequential Amendments) Bill 2023

Response to the Parliamentary Joint Committee on Human Rights – Report 11 of 2023

The Government provides the following responses to the Committee's questions.

(a) how the measures are effective to achieve the stated objectives of preventing identity theft and fraud, and preventing fraud and misuse of government funds in the context of the social security system

The identity verification services are a critical tool in protecting governments and industry from the harms of identity crime, and preventing nefarious actor from benefiting from identity theft and fraud.

The importance of the service, in particular the Document Verification Service (DVS), to preventing identity crime is discussed further in a Privacy Impact Assessment undertaken to support the expansion of the DVS for private sector use:

> A significant proportion of identity crime is facilitated by use of stolen, counterfeit or fraudulently obtained identity documents (e.g. documents obtained by using false or stolen information). Available information on the nature and extent of data breaches, together with the cost of fraudulent identity documents, indicates that these documents and/or the information needed to fraudulent manufacture or acquire them are readily available to criminals.
>
> The DVS plays an important role in preventing identity crime by ensuring that the veracity of information on identity documents can be confirmed directly and securely with the document issuing agency. Documents that have been reported stolen, have been cancelled or have expired cannot be successfully verified (returning an 'No' response)

For this reason, the DVS is used to satisfy the identity proofing standard when making a claim for social security payment through Services Australia. The standard involves identity confirmation and verification as provided by section 8 of the *Social Security (Administration) Act 1999* (Cth). In May 2023, almost 90,000 documents were successfully verified by Services Australia through the Document Verification Service for social security payment purposes.

(b) whether individuals need to consent to government authorities supplying identification information in the first instance to one of the identification verification services, and if so, can individuals withdraw consent at a later stage and request the information be removed from a service

The provision of consent to the collection, use and disclosure of identification information at the initial point of collection by government authorities or creation of an identity document (for example, when an individual applies for a passport) is subject to relevant Commonwealth, and state and territory legislation. This is outside the scope of the IVS Bill.

The IVS Bill requires entities to obtain an individual's consent to the collection, use and disclosure of identification information that relates to the individual, for the purposes of requesting identity verification services, (subclause 9(2)(b)).

When obtaining consent, entities must notify individuals of certain matters (subclause 9(3)). This supports a person to provide informed consent, after considering key matters, including:

- how the entity seeking consent uses identity verification services and how any facial images collected by that entity for the purpose of making a request for services will be used and disposed of (subclause 9(3)(a) and (b)
- whether facial images will be retained for any other purposes (subclause 9(3)(c))
- what legal obligations the entity seeking to collect identification information has in relation to that collection, what rights an individual has and what the consequences of declining to give consent are (subclause 9(3)(d), (e) and (f)), and
- where the individual can get information about making complaints (subclause 9(3)(d)), and where the individual can get information about the operation and management of the approved identification verification facilities (subclause 9(3)(h)).

To clarify, it is not technically possibly or authorised under the IVS Bill for identification information to be stored on the identity verification services. The services do not act as databases. Instead, the services facilitate the comparison of information on a person's identification document against government records held by the issuing agency rather than within the services.

Identity verification through the DVS and Face Verification Service (FVS) is almost instant, with an average response time of under 1 second. The services only provide a response indicating that there is or is not a match, and will not return any identification information as part of the result.

Therefore, the concerns about withdrawal of consent do not arise and the services do not hold any identification information that would need to be removed if consent is withdrawn.

(c) why consent from the relevant individual is not required for their driver's licence to be included on the Driver Licence database (noting that individual consent is required for use of the Document and Face Verification Services)

Consent requirements for the NDLFRS have been agreed with states and territories and are reflected in the Intergovernmental Agreement on Identity Matching Services (IGA):

> When individuals apply for new or renewed driver licences (or any other documents containing facial images to be used in the National Driver Licence Facial Recognition Solution) Road Agencies (or other relevant licensing agency) will take all reasonable steps to notify these applicants that the personal and sensitive information being collected by the Road Agency may be disclosed for the purposes of biometric matching through the National Driver Licence Facial Recognition Solution for law enforcement, national security and other purposes.

Furthermore, subclause 13(3)(a) requires state and territory authorities that are party to a National Driver Licence Facial Recognition Solution (NDLFRS) hosting agreement to take reasonable steps to

inform each individual that their personal information on a driver's licence has been uploaded onto the NDLFRS.

(d) what constitutes 'reasonable steps' in the context of informing individuals whose identification information is, or is to be, included in the Driver Licence database

'Reasonable steps' in the context of subparagraph 13(3)(a) and for the purposes of the IGA will vary depending on the nature of operations in each state and territory. States and territories that have uploaded their jurisdictions' data to the NDLFRS have undertaken a privacy impact assessment which, amongst other things, considered existing arrangements for notifying individuals.[1] The Government understands that some jurisdictions have amended privacy statements and provide further advice and guidance on government websites to inform individuals that information on their licence will be uploaded onto the NDLFRS.

(e) what are the consequences of declining to consent to biometric verification in the context of accessing government services, particularly Centrelink

This is not covered by the IVS Bill, which only seeks to regulate the operation of the identity verification services. It does not seek to regulate the use of biometric verification in order to access government services.

To assist the Committee, the following information can be provided.

- Biometric verification is not required to receive a government service from Services Australia, including services provided through Centrelink, obtaining a Medicare Card, and Child Support.
- To receive most Centrelink payments, Services Australia requires individuals to prove who they are by providing documents including an acceptable photo identity document to make a visual comparison of facial features. This facial check is undertaken in person at a service centre or using video chat and is not equivalent to facial biometric verification.
- A strong myGovID includes a biometric verification, currently using an Australian Passport photo, is an option available to individuals wishing to prove who they are to Services Australia, and meets the identity standard for Centrelink payments.

(f): whether there are alternative methods for individuals to authenticate or verify their identity, including for the purposes of creating a strong myGov account, to access social security services

This is not covered by the IVS Bill, which only seeks to regulate the operation of the identity verification services. It does not seek to regulate the use of biometric verification in order to access government services.

[1] For example, see Privacy Impact Assessment – VicRoads participation in the National Driver Licence Facial Recognition Solution and Response to the Privacy Impact Assessment of VicRoads' participation in the National Driver Licence Facial Recognition Solution.

To assist the Committee, the following information can be provided.

- Services Australia has alternative methods of identity confirmation for customers who do not want to use a digital identity or consent to a biometric check. This includes avenues to support people who have genuine difficulty proving their identity.
- The alternative identity assessment consists of a series of knowledge based questions, to be answered by the customer, to prove their identity and gain access to a payment or service.
- A person accessing services or payments on the basis of an alternative identity assessment may be asked to verify their identity information periodically. Alternatively, a customer may present to a service centre, with their identity documents, to confirm their identity without use of a biometric check.
- A myGov account linked to a strong digital identity is considered more secure for authentication purposes and will help keep the account holder's personal information secure, however a myGov account does not require any digital identity (strong or otherwise).

(g) whether consent in the context of accessing the social security system and other government services can be said to be genuinely free, given that such consent is required to access certain services and declining to consent would appear to restrict access to such services

Customers who have not provided consent and successfully undertake the alternative identity assessment have the same level of access to payments and services as customers who have provided consent and met the required identity standard. Declining consent does not restrict access to Centrelink, Medicare or Child Support payments and services.

(h) with respect to informing individuals about data breaches, how will the threshold 'reasonably likely to result in serious harm' be assessed and why is this threshold necessary (namely, why are individuals not informed when there is a data breach without there needing to be 'serious harm')

The requirement at subclause 13(3)(c) is intended to align with, and be read in a manner consist with, requirements under the Notifiable Data Breach Scheme under Part IIIC of the *Privacy Act 1988* (Cth).

The Notifiable Data Breach Scheme requires an organisation or agency to notify affected individuals and the Office of the Australian Information Commissioner about an eligible data breach. An eligible data breach occurs when there is unauthorised access or disclosure of personal information, or a loss of that information, and this is likely to result in serious harm to one or more individuals. The reason that an organisation or agency would be required to report a data breach is that they have not been able to prevent the likely risk of serious harm with remedial action. This threshold was established in 2018 in an attempt to balance the need to know against unnecessary notifications to individuals that might raise the risk of notification fatigue.

Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position. Similar to the Privacy Act, 'reasonable' and 'reasonably' are not defined in the IVS Bill and the term bears the ordinary meaning. What is reasonable can be influenced by current standards and

practices. 'Serious harm' is not defined in the Privacy Act or IVS Bill, but in the context of a data breach, may include serious physical, psychological, emotional, financial, or reputational harm.

Similar to the NDB scheme, entities should assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm.

(i) to which persons or organisations are the department and entrusted persons authorised to disclose identification information to, noting the bill authorises disclosure of such information but does not clearly specify to whom it may be disclosed

The IVS Bill provides legislative authority for the department to collect, use and disclose identification information that has been communicated to an approved identity verification service, or generated using the NDLFRS. Authority for the department to disclose identification information (subclause 28(1)) is limited to the purposes listed in subclause 27(2). The disclosure of information in these circumstances is appropriate and necessary as it reflects the department's role in facilitating the operation of, and supporting the making of requests for, the identity verification services.

Subclause 30(3) allows departmental officers and other entrusted persons to disclose protected information where:

- the conduct is authorised by a law of the Commonwealth or of a state or territory, or
- the conduct is in compliance with a requirement under a law of the Commonwealth or of a state or territory.

For example, these exceptions may enable the disclosure of protected information in response to a court where information is requested by subpoena, or in response to a search warrant obtained by a law enforcement agency.

Clauses 31, 32, 33, 34, and 35 of the IVS Bill also permit departmental officers and other entrusted persons to disclose protected information (including identification information) in the following circumstances:

- they were performing their functions or duties or exercising a power related to an approved identity verification facility (for example, this could include a departmental officer disclosing information under a request for a person's own information under the *Freedom of Information Act 1982* or Australian Privacy Principle 12)
- they reasonably believed that it is necessary to prevent a serious or imminent threat to the health or life of a person and the disclosure was made for the purpose of preventing or lessening that threat (for example, this may include circumstances where it is unreasonable or impracticable to obtain the consent of the individual whose health or safety is threatened to the disclosure given the imminence of the threat)
- they were disclosing protected information to an IGIS official for the purpose of the IGIS official exercising a power, or performing a duty, as an IGIS official
- they were disclosing protected information to an Ombudsman official for the purpose of the Ombudsman official exercising a power, or performing a function or duty, as an Ombudsman official

- they had obtained the consent of the person to whom the protection information relates, or
- the protected information that was held in, or generated using the NDLFRS, was supplied by an authority of a state or territory, and that authority has consented to the recording, disclosure, or access.

The IVS Bill also limits the information that is provided in response to a request for identity verification through the identity verification services. In particular, subclause 15(1)(g) and subclause 19(d) ensure that the outcome of a DVS and FVS comparison is communicated to the requesting entity as either a match or not. This ensures that personal information is not communicated back to the entity in response to an identity verification request.

(j) what circumstances can law enforcement agencies access and use information communicated to an identity verification service or held in, or generated by, the Driver Licence database, and what safeguards are in place to ensure that any access and use of identification information is a proportionate limitation on the right to privacy

In order for the department to disclose protected information to a law enforcement agency, an exception to the offences in clause 30 must apply. Subclause 30(3) establishes exceptions to these criminal offences where

- the conduct is authorised by a law of the Commonwealth or of a state or territory, or
- the conduct is in compliance with a requirement under a law of the Commonwealth or of a state or territory.

Entrusted persons may rely upon these exceptions to disclose protected information (including identification information) to law enforcement agencies. For example, subclause 30(3)(b) would allow entrusted persons to disclose information to law enforcement officers in response to a search warrant obtained under section 3E of the *Crimes Act 1914* (Cth).

In such circumstances, safeguards and protections will be provided by the relevant law that triggers the exception at subclause 30(3). For example, the approval and execution of a section 3E search warrant is subject to safeguards and limitations in the Crimes Act, ensuring proportionate limitations on the right to privacy.

Subclause 35(2) of the IVS Bill provides that an entrusted person may make a record of, disclose, or access protected information that was held in, or generated using the NDLFRS . This provision may be relied upon to support disclosures to law enforcement agencies. However, such disclosure must be with the consent of the relevant jurisdiction that has responsibility for the data supplied to the NDLFRS. The requirement for consent ensures that any limitation on the right to privacy is proportionate and appropriate.

(k) what safeguards are in place to mitigate the risk of data verification errors, including inaccurate face matching that may disproportionately affect one group over another, and the adverse impacts this may have on individuals, particularly in the context of the right to equality and non-discrimination

In relation to the NDLFRS, a range of measures and capabilities have been built into the system that are aimed at minimising the risk and impact of false negative and false positive matches, including: access policies, system design and testing (including biometric matching threshold testing). Relevant states and territories have also been engaged to ensure that the

face recognition engine in the NDLFRS is workable and appropriate against their jurisdiction's data sets.

When fulfilling a request for the identity verification services, the matching or comparison of information on an identification document occurs at the data source. For this reason, the Attorney-General's Department continues to work with states and territories to ensure the comparison or matching process aligns with best practices, including those provided by the National Institute of Standards and Technology and advice from other government agencies.

Furthermore, the annual report for the IVS Bill will include information about the accuracy of the systems for biometric comparison of facial images that are operated by the Department, which will be the NDLFRS, or the Department administering the *Australian Passports Act 2005* (Cth), for the purposes of providing identity verification services.

(l) what safeguards are in place to mitigate the risk of data breaches and hacking, or what assurances have been given by technical experts regarding the risks in the system, noting that the consequential interference on the right to privacy arising from such an event would be significant given the extensive scope of information communicated to identity verification services and held in the Driver Licence database

The identification verification facilities operate subject to safeguards, limitations and oversight arrangements to mitigate the risk of data breaches and protect the privacy of Australians. This includes the use of encryption and other arrangements to maintain the security of electronic communications to and from the facilities (clause 25), information held in the NDLFRS (subclause 13(4)), and limitations on the collection of information for the purposes of operating the facilities in the IVS Bill.

The Department has a number of existing measures in place to protect the security of the identity verification services. These include:

- entry into the system (built to PROTECTED standards) is controlled through a Secure Internet Gateway that authorises traffic from approved IP sources and inspects all data traffic to block threats based on real-time intelligence.
- the internal system elements are segregated and communication between environments is prohibited
- all communications and databases are encrypted using ASD Approved Cryptographic Algorithms.
- access to the system is strictly controlled, with all users and administrators required to have individual accounts that undergo strong authentication protocols
- automated real-time security scanning for vulnerabilities to continuously mitigate any emerging threats.

(m) how long will an individual's data be held in the Driver Licence database, and if it is indefinite, how is this a proportionate limit on the right to privacy

The length of time an individual's data is held in the NDLFRS will be a matter for road agencies in each state and territory.

Information in the NDLFRS is deleted on instruction from the jurisdiction's road agency. Where identification information (a drivers licence) is deleted from a jurisdiction's road agency data, it is also removed from the NDLFRS. Similarly, where an individual is provided

with a new licence or photo, the relevant jurisdiction's road agency will update its records with the new identification information, and this information will then be replaced on the NDLFRS.

(n) whether the measures are accompanied by any safeguards to ensure that any limitation on the rights to social security and equality and non-discrimination are proportionate in practice; and

(o) whether less rights restrictive alternatives were considered and if so, why these were not considered appropriate

As stated in the Statement of Compatibility with Human Rights, it is the Government's view that the IVS Bill will have a positive impact on the right to social security by ensuring individuals can more easily and securely verify their identity when seeking access to welfare payments and other benefits. Similarly, the IVS Bill promotes the right to equality and non-discrimination by facilitating the biometric verification of identity using information on licences uploaded on the NDLFRS and, in doing so, support more Australians to securely access critical services.

However, the Government notes the concerns raised by the Committee at paragraph 1.72. There are a number of safeguards in the IVS Bill and non-legislative policies in-place to promote the rights to social security and equality and non-discrimination, and ensure any perceived limitation is proportionate:

For non-legislative safeguards, see responses to (f) for alternative options for establishing a myGov account and access government services and (k) for safeguards in place to mitigate the risk of data verification errors.

Relevant safeguards in the IVS Bill include:

- the requirement to obtain consent (subclause 9(2)(b) and 3)) which is discussed further in response to (b)
- the requirement for requesting entities to conduct privacy impact assessments[2] in relation to requesting identity verification services (subclause 9(2)(a))
- requesting entities must establish and maintain a mechanism to deal with complaints from individuals whose identification information is held by the entity (subclause 9(2)(d))
- state and territory government authorities must have a means for dealing with complaints by individuals relating to their information on the NDLFRS (subclause 13(3)(d)), and
- other relevant Commonwealth, state and territory complaints handling mechanisms will continue to be available, including those provided by the Commonwealth Ombudsman and the OAIC under section 36 of the Privacy Act.

[2] The IVS Bill defines privacy impact assessment to have the same meaning as in subsection 33D(3) of the Privacy Act. A number of privacy impact assessments have been undertaken for the identity verification services and the NDLFRS, which can be found at www.idmatch.gov.au/privacy-security/privacy-impact-assessments

The Hon Tony Burke MP
Minister for Employment and Workplace Relations
Minister for the Arts
Leader of the House

Reference: MC23-003795

Mr Josh Burns MP
Chair
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

By email: human.rights@aph.gov.au

Dear Chair Josh

Social Security (Administration) (Public Interest Certificate Guidelines) (DEWR) Determination 2023

Thank you for your correspondence of 19 October 2023 regarding the Parliamentary Joint Committee on Human Rights (the Committee) request for further information as set out in Report 11 of 2023 on the *Social Security (Administration) (Public Interest Certificate Guidelines) (DEWR) Determination 2023* (Determination).

The Determination balances the protection of personal information with the public interest in ensuring transparency and accountability of government operations through the use of secrecy provisions in legislation, such as the provisions set out in the *Social Security Administration Act 1999* (Cth).

I appreciate the time the Committee has taken to review the Determination, and my response to the Committee's questions are enclosed.

I thank the Committee for bringing these matters to the Government's attention and I trust this response is of assistance.

Yours sincerely

[redacted]

TONY BURKE

2 / 11 / **2023**

Encl.

Response to the Committee's questions on the Determination

(a) what personal information the department holds and may therefore be disclosed under these grounds

The Public Interest Certificate Guidelines contained in the Determination (Public Interest Guidelines) defines "information" as follows:

> ***information*** means information acquired by an officer in the performance of his or her functions or duties, or in the exercise of his or her powers, under the social security law.

This definition is consistent with sub-paragraph (a) of the definition of 'protected information' in the *Social Security Act 1991* (Cth).

The Department of Employment and Workplace Relations is the agency responsible for oversight and administration of employment service programs, including Workforce Australia. The administration of these employment service programs is supported by a network of contracted employment service providers (providers).

In accordance with the *Privacy Act 1988* (Cth), personal information is only collected by the department or providers where it is reasonably necessary for or directly related to the administration of employment service programs, including to provide assistance to individuals participating in those programs, or where otherwise authorised by another legislation, for example, the *Social Security (Administration) Act 1999* (Cth).

Personal information collected by the department or providers may include:

- identifying details, such as name, date or birth and racial/ethnic information;
- contact details;
- education history, employment history and activity details;
- health information; and
- information relevant to an individual participating in an employment service programs (for example, appointment dates or barriers associated with obtaining employment).

Not all personal information that is requested to be disclosed, is in fact disclosed. The Public Interest Certificate Guidelines specifically provide that only the necessary amount of personal information required to be disclosed, should be disclosed. This has meant that in the majority of cases, only **limited** information such as individuals' names, dates of birth, residential addresses, telephone numbers, rather than the entire files, have been certified for disclosure.

(b) whether each of the grounds for disclosure would constitute a proportionate limit on the right to privacy (including whether each measure is sufficiently circumscribed, accompanied by sufficient safeguards, whether any less rights restrictive alternatives could achieve the same stated objective, and whether there is the possibility of oversight and the availability of review)

The Public Interest Certificate Guidelines include various safeguards to ensure that protected information is only disclosed where the public interest outweighs any limitation on the right to privacy.

All of the purposes for which a Public Interest Certificate can be issued are sufficiently circumscribed in the following ways:

- Section 9 requires it to be established that there is a threat to the life, health or welfare of a person.
- Section 10 only applies to serious criminal offences and civil penalty matters. It does not allow for disclosure in relation to minor criminal offence and civil penalty matters.
- Section 11 is designed to support proceeds of crime regimes so that criminals are not able to retain the proceeds of their criminal activities.
- Sections 12 and 13 require that the decision maker be satisfied that there are no reasonable grounds to believe that the relevant person would object to the disclosure.
- Section 14 is designed to provide a benefit to individuals by supporting those who have applied for, or are tenants in, public housing or other State-or Territory-managed housing.
- Section 15 is designed to provide a benefit to individuals by supporting the work of the Queensland Family Responsibilities Commission in assisting welfare reform communities.
- Section 16 is designed to provide a benefit to individuals by supporting them in receiving reparations to which they may be entitled.
- Section 17 is designed to promote the rights of the child by assisting in contact being made with a parent or relative.
- Section 18 is designed to provide a benefit to individuals by assisting them to obtain concessions for public utilities.
- Section 19 is designed to facilitate the delivery of services by the department and other agencies to income support payment recipients.
- Section 20 is designed to support research and evaluation so that the department can improve the employment services it provides.
- Section 21 is designed to support the investigation of alleged breaches of the Australian Public Service Code of Conduct.
- Section 24 is designed to support the rights of the child by ensuring that they receive appropriate support where they are subject to abuse or violence.
- Section 25 is designed to ensure homeless young persons are able to support themselves if they are not able to live at home.
- Section 26 is designed to assist in the reconciliation between a homeless young person and their parents.
- Section 27 is designed to provide reassurance to parents of a homeless young person whilst not forcing the homeless young person to communicate with their parents if it is against their wishes.

All of the provisions include a requirement that the decision maker be satisfied that the disclosure is necessary for the particular purpose. This serves to limit the disclosure to only that required to meet the particular objective.

Section 23 provides that information about a homeless young person can only be disclosed if that disclosure will not cause them any harm. This ensures that the right to privacy is only limited where there is a benefit to the homeless young person.

The Public Interest Certificate Guidelines include a requirement that the information cannot reasonably be obtained from a source other than the department (sections 8(1)(a) and 23(1)(a)) this ensures that the power can only be used as a last resort and that disclosure can only be authorised where no other less rights restrictive alternative is available.

There are a number of safeguards in place in relation to the disclosure of information under the Public Interest Certificate Guidelines. These include the following:

- While the Privacy Act continues to apply in relation to the handling of protected information that is also personal information as defined in the Privacy Act, the social security law imposes a higher level of protection to such information than is imposed under the Privacy Act. For example, criminal sanctions apply for the unauthorised use or disclosure of information under section 204(1) of the *Social Security (Administration) Act 1999*;

- Public interest certificates made on the basis of the Public Interest Certificate Guidelines are made by the Secretary and her delegates at appropriate levels, and are subject to administrative arrangements which recognise the significance of such decisions;

- In appropriate circumstances, the disclosure of information under the Public Interest Certificate Guidelines may be accompanied by additional measures to further protect the information (e.g. Deeds of confidentiality may be required for recipients of the information); and

- The social security law provides that information provided to a person on the basis of a Public Interest Certificate must be used for the purpose for which it was provided. That recipient is not permitted to further disclose the information to other parties unless the disclosure is for the same purpose or the disclosure is otherwise authorised by law.

(c) whether officers administering this measure would have training or specialised experience in assessing relevant factors, such as whether a young person has experienced violence or abuse, or whether there is a threat to the life of a person

The Secretary's authority to issue a public interest certificate is currently exercised by the National Contract Manager for employment services (Senior Executive Service Band 2). This is a senior position and is held by a highly experienced officer. The National Contract Manager is supported by a specialist team of officers and dedicated Provider Leads, who process requests for disclosure. Legal advice is sought in relation to each disclosure request to support them in deciding whether they can be satisfied that all the requirements are met.

Training provided to the specialist team includes:

- mandatory departmental privacy training;
- training on the Privacy Act and information disclosure schemes (delivered by in-house and external lawyers including the Australian Government Solicitor);
- specific Public Interest Certificate training (delivered by an in-house legal team);
- the employment services-specific Information Exchange and Privacy training module (produced by an external legal firm); and
- vicarious trauma training (delivered by an external specialist training provider).

Upon receipt of a request for disclosure, the Secretary or their delegate will consider relevant information available to the department. This includes:

- information held in the department's IT systems regarding the participant, including information provided by Services Australia, such as vulnerability indicators;
- the context in which a request for information is made, or the circumstances leading to the information being requested;
- evidence that obtaining the individual's consent had been attempted (and if not, the reason for not doing so); and
- evidence from the provider regarding their interactions with the individual(s).

(d) how the Secretary would determine that a person is unable to provide updates on their own circumstances, and what training they would have in relation to assessing such factors

The Committee is referred to the response set out in relation to question (c) above.

(e) whether the measure is compatible with the rights of people with disability to equality before the law, including how the Secretary would determine that a person with disability is unable to give notice of their own change in circumstances

The Public Interest Certificate Guidelines are compatible with the rights of persons with disabilities under the Convention on the Rights of Persons with Disabilities. There are no particular impacts of the Public Interest Certificate Guidelines on people with disabilities over and above the limitation on the right to privacy that applies to everyone.

Section 6(b) of the Public Interest Certificate Guidelines requires consideration to be given to whether various vulnerabilities, including disability, might limit the information available to the department in relation to an individual's circumstances to inform the decision on issuing a Public Interest Certificate. The decision maker would use the information already available to the department about the individual in determining whether they are unable to give notice of their own circumstances. If it is determined that they may be unable to give notice, this would prompt a more cautious approach to be taken in deciding whether to issue a Public Interest Certificate taking into account the individual's vulnerabilities. This supports the rights of people with disabilities by ensuring that their disability is taken into account in the decision-making process.

(f) whether the disclosure of personal information may, in circumstances provided for in this measure, engage and limit further human rights (for example, the rights of the child)

The Statement of Compatibility with Human Rights provided alongside the Public Interest Certificate Guidelines sets out the other rights which are engaged. These include rights under the Convention on the Rights of the Child and the International Convention on Economic, Social and Cultural Rights.

The Hon Linda Burney MP

Minister for Indigenous Australians

Reference: MB23-000358

Mr Josh Burns MP
Chair, Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

Dear Mr Burns

I refer to the Parliamentary Joint Committee on Human Rights' (the Committee) request in *Human Rights Scrutiny Report 10 of 2023* (the report), dated 13 September 2023, for further information on the *Social Security (Remote Engagement Program) Determination 2023* (the Instrument).

I note this instrument was informed by the outcomes of co-design with the Ngaanyatjarra people. The engagement of stakeholders from the Ngaanyatjarra Lands in the design of the Remote Engagement Program (REP) Trial originally arose from a Commonwealth commitment made as part of settling a class-action lawsuit brought by the Community Development Program (CDP) Participants in 2019 and settled by the previous Government in 2021.

When we formed Government in 2022, we committed to replace the CDP with a new program with real jobs, proper wages and decent conditions developed in partnership with First Nations people. The trial in the Ngaanyatjarra lands continues in line with the commitment to the community and will inform the design of the new program. I note that accessing the REP payment is voluntary and time limited. It will cease on 30 June 2024.

I provide the following responses to the Committee's request for further information to assist the Committee's consideration of the Instrument:

(a) what are the types of circumstances in which a placement may be cancelled (and thus the payment removed)?

The REP Placement may be cancelled or ended:

- at the request of the REP Host or REP Participant
- if the REP Participant is no longer eligible (e.g. is no longer receiving a qualifying income support payment)
- if the REP Participant is not compliant with the terms of the REP Placement Agreement
- if the REP Host is not compliant with the terms of the REP Placement Agreement, or if the Provider believes the REP Participant would be endangered or placed in an unlawful situation as a result of the REP Placement
- for other reasons, such as the REP Participant gaining employment with the REP Host or if directed by the Department.

In the event of a REP Placement ending due to non-compliance by the REP Host, Providers should aim to arrange another REP Placement for a REP Participant. Providers can also choose to arrange another REP Placement where the REP Participant or REP Host has requested to end an existing placement. A request from the Department to end a REP Placement would only occur in extraordinary and unforeseen circumstances, such as a risk to the REP Participant, the REP Host, or the Provider.

(b) noting that the work performed by a participant may constitute a form of employment for the purposes of international human rights law, is the rate of remote engagement program payment (that is, $190 per fortnight for at least 15 hours work) compatible with the right to fair remuneration (noting participants could work up to 8 hours per day);

The REP Trial has been designed to offer participants the opportunity to participate in a placement to gain experience and develop skills. Participation in the REP Trial is not employment. The REP Payment is an incentive to encourage participation in the REP Trial, not remuneration. As outlined in the CDP Head Agreement Annexure 1, Part G - REP Trial Services (niaa.gov.au/sites/default/files/part-g-annexure-1-head-agreement-cdp-2019-2024.pdf), the REP Payment provides an incentive for Eligible Participants to participate in placements designed to build their skills that will support them to find and maintain employment. Under the terms of the REP Placement Agreement, REP Participants cannot be employees of REP Host organisations.

The REP Payment is paid in addition to a REP Participant's primary income support payment and other supplements.

Clause 7.1 of Annexure 1, Part G provides that REP Placements:

- are voluntary;
- do not include paid employment and do not, in themselves, create an employment relationship between the REP Participant and the REP Host or Provider;
- must not be approved if a REP Host has downsized its workforce in the previous 12 months before the commencement of REP Trial Services (i.e. through redundancies or termination) and the proposed REP Placement/s involve the same tasks as those performed by former employees;
- must not be used as a stop-gap measure while a REP Host is undertaking recruitment exercises, or as a way of meeting ad-hoc needs in lieu of creating paid employment positions;
- must not, in whole or in part, involve work which would otherwise have been undertaken by a paid worker if the REP Placement had not taken place; and
- must be ended where the REP Participant commences paid employment with the REP Host.

A REP Placement must not replace jobs or a paid worker. REP Placements must also be tailored to the needs of the REP Participant.

(c) how is the measure effective to achieve the stated objectives and in particular, noting the mixed findings of the CDP regarding its effectiveness in achieving employment outcomes for participants, how is the remote engagement program different from the CDP such that it is more likely to achieve the stated objectives;

The Remote Engagement Program Trial uses a co-design approach to trial ideas that could be considered in the design of a new remote employment program to replace the CDP. The REP Trial aims to test ideas and understand barriers to employment in remote areas. Under the *Social Security Act* payments cannot be made after 30 June 2024. It complements other trials currently under way, including the new community projects approach in CDP and the New Jobs Program Trial which commenced on 18 September 2023.

The outcomes of these trials will help to provide an evidence base for what works and what does not work in remote employment services. The REP Trial is trialling a new supplementary payment in the social security system as an incentive for eligible jobseekers to attend a placement designed to build their skills that will support them to find and maintain employment and contribute to their community. The REP Trial is unique in its integration with the income support system. No other CDP trials or projects currently underway offer the delivery of incentives via the income support system to gain experience and develop skills.

(d) whether communities were consulted about the proposed measure in this instrument, as opposed to the broader policy underpinning the remote engagement program, and if so, what were the outcomes of those consultations;

The REP Trial was a concept that emerged from ongoing engagement with stakeholders from the Ngaanyatjarra Lands in Western Australia as part of settling a class-action lawsuit brought by CDP Participants in 2019 and settled by the previous Government in 2021.

A Ngaanyatjarra Lands Co-Design Group, comprising community and Ngaanyatjarra Council (Aboriginal Corporation) (NCAC) representatives, was established in March 2022 and met in March and May 2022 to determine the details of the REP Trial, including the rate of the REP Payment.

At the May 2022 Co-Design Group meeting, the Board of Ngaanyatjarra Council asked NCAC to bring forward design options for a trial program. The Board of Ngaanyatjarra Council endorsed the REP Placements in November 2022.

The Paupiyala-Tjarutja Aboriginal Corporation, the governing body for the Spinifex people and the CDP provider in Tjuntjuntjara within CDP Region 3, expressed an interest in being involved in the REP Trial on 28 September 2022 and were subsequently invited to participate.

Additionally, Providers must engage broadly with communities to identify their priorities for the REP Trial, including their preferred REP Host organisations and preferred activities to be undertaken as part of REP Placements.

(e) whether review is available for certain decisions made in relation to this measure, such as where a person's placement is cancelled, and their payment is removed; and

REP Participants have several options to request a review of decisions relating to their REP Placement, including: internal review by the Provider; formal review by Services Australia; and review by the Administrative Appeals Tribunal. Before agreeing to be a REP Participant, REP Participants will be provided with information about making a complaint or appealing a decision.

In the event of non-compliance by a REP Participant, Providers must consider alternatives to ending the REP Placement Agreement and outline factors that must be taken into consideration before making a decision to end the placement, including:

- reasons for the non-compliance, including whether the REP Participant was fully able to comply with the requirements of the REP Placement Agreement;
- the severity and impact of the non-compliance (for example, a REP Participant engaging in unsafe practices despite appropriate guidance and training compared with failure to notify in advance of a single absence);
- whether the REP Participant was adequately warned of the consequences of non-compliance;
- the frequency or repeated nature of the non-compliance; and
- how other REP Participants have been treated by the Provider in similar situations.

Providers must support REP Participants over the course of their REP Placement and act as an advocate for the REP Participant. When making a decision to end a REP Placement, REP Providers must make lawful decisions; observe natural justice; evidence, facts and findings; explanation of reasons and documenting decisions.

(f) what other safeguards accompany the measure.

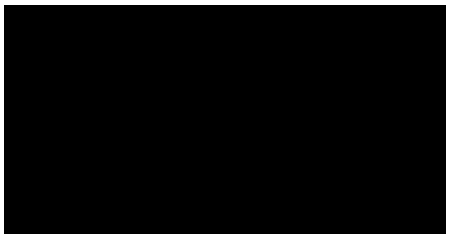
Safeguards for REP Participants under this measure include:

- Participation in a REP Placement is voluntary.
- The REP Participant can end the REP Placement at any time and for any reason.
- Providers must use a case management approach, whereby adjustments are made for the differing needs and strengths of each Eligible Participant.
- Providers must conduct an assessment of individuals before they commence in a REP Placement.
- Before commencing a REP Placement, Providers must discuss the Eligible Job Seeker's skills, aspirations, and the nature of REP Placement the Eligible Job Seeker would like to participate in.
- Participation in REP Placements cannot be used to replace real jobs at a REP Host.

- Before signing the REP Placement Agreement, REP Participants must be informed of the REP Trial arrangements that will impact on them, and providers must:
    - provide the REP Participant with a copy of the Fact Sheets for REP Participants and the REP Placement Agreement, including the Privacy Collection Notice;
    - explain the content of the Fact Sheets for REP Participants and the REP Placement Agreement, including the Privacy Collection Notice;
    - explain the impact of the REP Payment on the REP Participant's income and potential impact on benefits, including:
        - the REP Payment is taxable;
        - the REP Payment does not need to be reported to Centrelink;
    - the REP Payment forms part of the person's taxable income, and may affect the REP Participant's entitlements from State Government authorities or other organisations to whom changes in income must be reported;
    - explain that in order to receive the REP Payment, the REP Participant must attend a REP Placement for at least 15 hours every week in their payment fortnight;
    - tell the REP Participant that participation is voluntary and they can end their REP Placement at any time and for any reason;
    - ensure the REP Participant understands the duration, conditions and participation requirements of the REP Placement and the REP Payment.
- Providers must assess job seeker eligibility and suitability for a REP Placement, and support the REP Participant in their REP Placement to ensure the REP Participant has the best chance to successfully participate in the REP Placement and gain the desired skills and experience.
- A three way REP Placement Agreement is signed by the Provider, REP Participant and REP Host that ensures the REP Participant's safety and the provision of appropriate tasks and supervision.
- Contractual requirements to engage with communities in the implementation of the REP Trial.

I thank the committee for raising these issues for my attention.

Yours sincerely



The Hon LINDA BURNEY MP
Minister for Indigenous Australians

13 / 10 / 2023