SENATOR THE HON MURRAY WATT
MINISTER FOR AGRICULTURE, FISHERIES AND FORESTRY
MINISTER FOR EMERGENCY MANAGEMENT

MS23-000516

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

Dear Chair

Thank you for your correspondence of 9 February 2023 concerning the Export Control Amendment (Streamlining Administrative Processes) Bill 2022. Please find below responses to the committee's request for further information to assist the committee's consideration of the amendments:

a) *What kinds of personal information may be disclosed and used pursuant to the proposed authorisations, including examples of such information and the contexts in which the information may be disclosed;*

The proper, effective and efficient performance of functions or duties, or the exercise of powers under the Export Control Act will often involve the use or disclosure of relevant information which may include personal information. For that reason, the authorisations set out in proposed new Division 2 of Part 3 of Chapter 11 of the Act are clearly defined and aimed at the legitimate objective of supporting the effective operation and enforcement of the Act.

These authorisations allow for the use or disclosure of relevant information in certain circumstances, including in the course of, or for the purposes of, the performance of functions or duties, or the exercise of powers under the Act (new section 388), or for research, policy development or data analysis to assist the Department of Agriculture, Fisheries and Forestry (new section 394). They also include the disclosure of statistics (new section 395) and disclosure to a foreign government, an authority or agency of a foreign government or an international body of an intergovernmental character, for the purposes of the export of goods from Australia, managing Australia's international relations in respect of trade or giving effect to Australia's international obligations (new section 389).

The kinds of personal information that may be used and disclosed pursuant to the proposed authorisations is constrained by the operation of the Act, whereby relevant information is limited to information collected for the purposes of performing functions or duties, or exercising powers, under this Act. This may include information used to meet obligations or requirements under the Act, such as personal information contained in applications or other submissions under the Act. The types of personal information collected may include, but is not limited to, an applicant's name; address; business associates and interests; details of intended export operations; previous convictions; or orders to pay a pecuniary penalty under relevant legislation.

Relevant information that is also personal information may be used or disclosed to other Commonwealth entities under proposed sections 391 (disclosures to Commonwealth entities) or 393 (disclosure for the purposes of law enforcement), for example in circumstances where export information is requested in support of investigating suspected criminal activity or undertaking surveillance operations. For example, the Australian Federal Police or Australian Border Force may request personal information from the department relating to an exporter or export operations, in specific cases concerning a port of export, or an export vessel that may be under suspicion. These entities may request information relating to any prior convictions, as well as known business associates or interests.

Several of the authorisations impose specific measures to limit or prevent the sharing of relevant information that may contain personal information. For example, the authorisation to use or disclose relevant information for the purposes of research policy development or data analysis requires reasonable steps to be taken to de-identify personal information, wherever possible, and to otherwise minimise the amount of personal information disclosed. The authorisation to use or disclose statistics can only be used for statistics that are not likely to enable the identification of a person. Authorisations to disclose information to a State or Territory body require an agreement to be in place between the Commonwealth and that State or Territory body before the relevant information may be disclosed, which may include requiring the State or Territory body to confirm that any personal information that is disclosed will be subject to appropriate safeguards.

b) *The person or body to whom relevant information may be disclosed for the purposes of the Act (proposed section 388) or other Acts (proposed section 390) and managing severe and immediate threats (proposed section 397D)—noting that in these circumstances, it is not clear to whom the information may be disclosed;*

While the proposed authorisations for the disclosure of information under proposed section 388, section 390, and section 397D, do not list the persons to whom disclosures may be made, the persons to whom relevant information can be disclosed are necessarily limited by the requirement that the disclosure be for the purpose of a function, duty or power under the Act or export control rules, or the administration of portfolio Acts, or for the specific purpose of managing severe and immediate threats.

Section 388 would authorise the use or disclosure of relevant information for the purposes of performing functions or duties, or exercising powers, under the Act or export control rules, or assisting another person to perform or exercise such functions, duties or powers. The disclosure of information is governed and limited by the functions, duties, and powers under the Act. For example, an approved auditor who has collected information in conducting an audit (which is a function or duty under the Act) may share that information with administrative staff who are assisting the approved auditor to carry out their function of providing an audit report.

Proposed section 390 provides for information to be disclosed for the purposes of the administration of the Act, or other portfolio Acts. This allows for best practice and streamlined information sharing, and by definition limits the persons to whom disclosure of relevant information is allowed, as there must be a clear connection between the disclosure and the specific legislative purpose of the relevant Act. This authorisation would, for example, enable information that is collected in the course of performing a function under the Act that may be relevant to the administration of the *Biosecurity Act 2015* (the Biosecurity Act*),* such as information relating to a pest incursion, to be efficiently shared for the purposes of managing the incursion under that Act.

Proposed section 397D would authorise the disclosure of relevant information where there is a reasonable belief that it is necessary to manage severe and immediate threats that arise in connection with exports or that could cause harm on a nationally significant scale. Proposed section 397D does not limit to whom any such disclosures may be made, as flexibility under the authorisation is necessary and reasonable in responding to circumstances in which a severe and immediate threat exists. It is anticipated that this authorisation will be used rarely, as there is a high threshold that must be met in order to rely on this authorisation – that is, that there is a severe and immediate threat which either relates to exports or has the potential to cause harm on a nationally significant scale. The fact that the power is given to the Secretary and cannot be subdelegated below SES level is a further safeguard on the exercise of this power.

In relation to protected information, there are sanctions for unauthorised use or disclosure. The offence in subsection 397G is triggered if certain persons who obtained or generated protected information in the course of, or for the purposes of, performing functions or duties, or exercising powers, under the Act (or assisting another person to perform such functions or duties, or exercise such powers), use or disclose protected information, and the use or disclosure is not required or authorised by a Commonwealth law or a prescribed State or Territory law (and where the good faith exception in subsection 397G(4) does not apply). The *Privacy Act 1988* regulates disclosures of personal information about an individual.

c) *Why it is necessary to allow all information obtained using powers under the Act to be shared for law enforcement purposes, unrelated to managing risks that arise in connection with export operations or the administration of the Act;*

Section 393 would authorise the disclosure of information for the purposes of law enforcement to certain Commonwealth, State or Territory bodies which have a law enforcement or protection of public revenue function. Relevant law enforcement purposes may include the investigation of offences under the *Crimes Act 1914*.

A robust and effective framework for information sharing for the purposes of law enforcement is a matter of public interest. The amendments address the need to simplify and clarify the current information sharing regime, and allow a key element of best practice, that is, the ability to share information for law enforcement purposes when it is in the public interest to do so.

This would better enable enforcement decisions to be informed by proper investigation of differing, intersecting issues and information, before an effective enforcement decision can be made.

Under these proposed amendments, where information is proposed to be disclosed to a State or Territory body or a police force or police service of a State or Territory, an agreement is required to be in place between the Commonwealth and that body in which the relevant body has undertaken not to use or further disclose the information except in accordance with that agreement. This provides some certainty as to the use and onward disclosure of the information provided.

The amendments outlined in the Bill align with similar changes to the Biosecurity Act agreed to by the Parliament in passing the *Biosecurity Amendment (Strengthening Biosecurity) Act 2022* in November 2022. As noted above, the Biosecurity Act is another key Act regulating the supply chain and administered by the department, and alignment across this authorisation provides consistency and predictability for stakeholders. This amendment is also consistent with the way information sharing regimes are framed in other legislation, for example the *Hazardous Waste (Regulation of Exports and Imports) Act 1989* and the *Industrial Chemicals Act 2019*.

The enforcement of Australian laws is an appropriate framing for the authorised disclosure of relevant information, as it is a matter of public interest. I consider that there are sufficient checks and balances on the use of such information and the authorisation allows the Commonwealth to make a judgement about the necessity of sharing for any proposed purpose.

d) Why the potential safeguards identified in the statement of compatibility in respect of these proposed authorisations are not set out in the bill itself; and

The proposed authorisations for sharing information are aimed at the legitimate objective of supporting the management of the export control framework and for the effective operation and enforcement of the Act. In support of this, the Bill contains safeguards that are reasonable, necessary, and proportionate to meeting this objective.

As identified in the statement of compatibility, it would be consistent with the legislation to also apply additional safeguards when disclosing relevant information, however, it would not be possible and practical to impose all these requirements in the Bill itself because flexibility is required in their application. For example, an agreement between the Commonwealth and a State or Territory body may sometimes prohibit the onward disclosure of information or require that information may only be used for a specific purpose, while in other situations the agreement may impose limitations on onward use or disclosure rather than prohibitions. In some circumstances, it may be clear that the relevant state or territory legislative framework already sufficiently governs the onward use and disclosure of the information, making it unnecessary to impose restrictions as part of the agreement.

Similarly, whether conditions should be placed on the use and onward disclosure of relevant information, and if so, the specific conditions that are required, need to be adapted to the particular circumstances of the initial disclosure, which should not be limited to specific conditions set out in the Bill. For example, where information is being disclosed to another Commonwealth officer for the purposes of the Biosecurity Act, the use or disclosure of that information would be governed by the equivalent information management provisions in that Act and further conditions would be unnecessary. Similarly, disclosures to other Commonwealth entities would be governed by the *Privacy Act 1988* and unauthorised disclosure that could cause harm may breach existing offence provisions in the Criminal Code. Where a disclosure to a person outside the Commonwealth is made, there may already be arrangements in place, for example, by way of conditions imposed through an instrument of authorisation made under section 291 of the Act.

As discretion is required, it is not necessary to reference these safeguards in the Bill itself as there is no need for legislation to specify that something may be done if it would not otherwise be prohibited.

Similarly, the need to create tailored authorisations to govern the use or disclosure of relevant information in the rules, which impose appropriate limitations on the use or disclosure of the information, has been recognised in the formulation of proposed section 397E. It would not be possible to set out these limitations in the Bill because the limitations will need to be tailored to the particular authorisations prescribed in the rules. Rules made under section 397E are disallowable and will be subject to parliamentary oversight.

The following safeguards mentioned in the statement of compatibility have been included in the Bill:

- The ability for disallowable rules made under proposed section 397E to be tailored to particular circumstances by allowing the rules to prescribe the kinds of relevant information that may be used or disclosed, the classes of person who may use or disclose the information, the purposes for use or disclosure and limitations on the use or disclosure of the relevant information
- Section 394 would require reasonable steps to be taken to de-identify personal information, wherever possible, and for personal information to otherwise be minimised
- Section 395 would allow the use or disclosure of statistics only if they are not likely to enable the identification of a person
- Authorisations such as proposed new sections 393 and 397C require an agreement to be in place between the Commonwealth and a State or Territory body before the relevant information may be disclosed
- The legislation makes clear by way of a note that the Commonwealth can make agreements or other arrangements to impose conditions on the use or disclosure of relevant information.

Further, as mentioned in response to point (b) above, where additional safeguards have not been included in an authorisation, this is because the authorisation by definition, limits the persons to whom information can be disclosed, for example, because the use or disclosure must be for the purpose of performing or exercising a function, duty or power under the Act or for the administration of a portfolio Act. Appropriate safeguards have been included in each authorisation that are proportionate and adapted to the purpose of the use or disclosure permitted by that authorisation.

In addition to the offence and penalties set out in proposed new section 397G of the Act for the unauthorised use or disclosure of protected information, the *Privacy Act 1988* applies in relation to personal information about individuals.

Other safeguards such as departmental policies and procedures regarding the proposed authorisations, are appropriately not set out or referenced in the Bill itself. These authorisations can and will provide additional safeguards around what information can be shared and by whom. Further information is provided in the response to e) below.

e) What other safeguards, if any, would operate to protect personal information disclosed or used pursuant to these proposed authorisations.

The department maintains robust policies and procedures to protect any personal information which it holds, as documented in the department's Privacy Policy at agriculture.gov.au/about/commitment/privacy. As part of these processes, personal information is held in accordance with the collection and security requirements of the Australian Privacy Principles, the department's policies and procedures and the Australian Government Protective Security Policy Framework. Should personal information held by the department be subject to unauthorised access or disclosure, the department has procedures in place to assess the incident and mitigate any harm that may have been caused and considers the incident in accordance with its responsibilities under the privacy Act and requirements under the Notifiable Data Breach Scheme to notify the Office of the Australian Information Commissioner of any potential eligible data breaches.

Many of the authorisations impose specific measures to prevent the sharing of relevant information that may also be personal information. For example, new section 394 requires reasonable steps to be taken to de-identify (as defined in section 12 of the Act) personal information, wherever possible, before relevant information is disclosed for the purposes of research, policy development or data analysis. New section 395 also limits the use or disclosure of statistics to where those statistics are not likely to enable the identification of a person.

Authorisations such as new sections 393 (disclosure for law enforcement purposes) and 397C (disclosure to State or Territory body) will require an agreement to be in place between the Commonwealth and a State or Territory body before the relevant information may be disclosed to that body. This may include for example, requiring the State or Territory body to confirm that any personal information that is disclosed will be subject to appropriate safeguards.

In addition, relevant departmental policies and procedures, which can be implemented on a case-by-case basis, include the following:

- application of additional restrictions, including via protective marking, to limit the clearance level for access of personal information
- notifying particular affected parties of a particular disclosure or use, if appropriate
- entering into agreements with other parties, which as noted above is required for certain authorisations, will set out use, handling and storage requirements of personal information; and
- ensuring the storage of personal information meets best practice protocols and is in line with Commonwealth record-keeping obligations.

I would like to thank the committee for bringing these matters to my attention. I trust that the information provided above will support the committee in its consideration of the Bill.

Yours sincerely

MURRAY WATT 21 / 02 / 2023

THE HON ED HUSIC MP
MINISTER FOR INDUSTRY AND SCIENCE

MS23-000276

22 FEB 2023

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

human.rights@aph.gov.au

Dear Chair Josh,

Thank you for your correspondence of 9 February 2023 on behalf of the Parliamentary Joint Committee on Human Rights in relation to the National Reconstruction Fund Corporation Bill 2022.

The National Reconstruction Fund Corporation Bill 2022 (the Bill) gives effect to the Government's election commitment to establish the National Reconstruction Fund Corporation (the Corporation). The Corporation will invest to support, diversify and transform Australia's industry and economy to secure future prosperity and drive sustainable economic growth.

The Committee has noted that the Bill permits the Corporation to disclose official information, which may include personal information. The Committee has therefore requested additional information to assess the compatibility of this measure with the right to privacy. My responses to the Committee's questions are outlined below.

Disclosure of personal information

I confirm that the official information that may be disclosed by the Corporation under clause 85 of the Bill, including national security information, may include personal information, and may therefore engage the right to privacy. The information that would be provided to the Corporation would typically be provided by businesses seeking investment, and could contain some limited personal information, such as the names and contact details of senior officers in the business for the purpose of the Corporation making investments.

The intention of clause 85 is not to be generally permissive but to provide for the Corporation's ability to share information, particularly national security information or sensitive financial intelligence information in a narrow set of circumstances, to facilitate the effective and efficient performance of the Corporation's investment functions.

Compatibility with the right to privacy

The Australian Privacy Principles (APPs) as provided for by the *Privacy Act 1988* authorise the disclosure of personal information where the disclosure is authorised by or under an Australian law (APP 6.2(b)). Clause 85 provides such an authorisation for the provision of information about the affairs of a person (including personal information) to limited classes of recipients to enable appropriate sharing of information in limited circumstances where it will facilitate the exercise of the Corporation's investment functions or enable the receiving entity to perform or exercise any of its functions.

It is the Government's intention that subclause 85(1) could be used, for example, to:

a) enable sharing of information between the Corporation and its subsidiaries; and
b) enable the provision of information by the Corporation to its administering Commonwealth departments;

without requiring the express consent of every individual whose information is contained in the material or the redaction of large amounts of material. The alternative would directly impinge on the effective and efficient performance of the Corporation's investment functions where this performance relies on the Corporation's ability to disclose official information as appropriate.

The Bill also authorises the sharing of information for national security or financial intelligence purposes under subparagraph 85(3)(a)(iii), such as where information is referred to the Australian Transaction Reports and Analysis Centre to investigate potential money-laundering, provided that this information is shared to facilitate the performance of the Corporation's investment functions or to enable the recipient to exercise their functions or powers (clause 85(3)(a) refers). Sharing information for those purposes is broadly consistent with the *Privacy Act 1988*, in particular APP 6.2(e), which permits the disclosure of information where it is reasonably necessary for one or more enforcement related activities conducted by or on behalf of an enforcement body.

Furthermore, the scope of the Corporation's financing remit includes investment in defence capabilities as well as critical technologies in the national interest. It is important that any concerns that may arise in the course of the Corporation exercising its investment functions (including matters that arise during due diligence and negotiation) are able to be shared with relevant national security or intelligence bodies. To the extent that personal information is shared with an intelligence or national security body under subclause 85(3)(a)(iii), that sharing would be proportionate to the essential public interest of enabling this intelligence or national security body to perform its functions.

The proposed measure is therefore directly connected to its objective of facilitating the effective and efficient performance of Government functions. Moreover, it is the Government's view that any risks related to limiting the right to privacy in the manner this provision does are commensurate and proportionate to the necessity of the provision to achieving this objective.

Entities to whom official information may be disclosed

The disclosure powers under clause 85 are also sufficiently circumscribed when considered in the context of the limited classes of recipients that may receive official information under subclauses 85(2) and 85(4) of the Bill. I note that the classes of entities listed under subclauses 85(2)(a), 85(2)(b) and 85(2)(c), including any subsidiaries the Corporation establishes, would themselves subject to the APPs and, as such, would be required to keep any personal information received confidential. Most state and territory governments (subclause 85(d) refers), where they are not subject to the APPs, have equivalent legislation which cover their public sector agencies. Furthermore, any rules made by the Ministers prescribing a further agency, body or person under subclause 85(2)(e) would be subject to disallowance.

It is the Government's view that it would be inappropriate to prescribe specific entities under subclause 85(2), rather than broad classes of entity, since the specific entities the Corporation may be required to interact with in order to exercise its investment functions may reasonably be expected to change over time.

I trust this information will be of assistance to the Committee.

Ed Husic MP

Senator the Hon Don Farrell

Minister for Trade and Tourism
Special Minister of State
Senator for South Australia

REF: MC23-000323

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

7 MAR 2023

Reply via email: human.rights@aph.gov.au

Dear Mr Burns

Thank you for your correspondence dated 9 February 2023 requesting further information about the *Referendum (Machinery Provisions) Amendment Bill 2022* (the Bill). I am pleased to provide the below additional information in response to the Committee's request.

The Government introduced the Bill on 1 December 2022 to amend the *Referendum (Machinery Provisions) Act 1984* (Referendum Act) to ensure a consistent voter experience across elections and referendums. The Bill ensures that referendums reflect contemporary federal election voting processes and aligns the conduct of referendums with equivalent processes in the *Commonwealth Electoral Act 1918* (Electoral Act) to support voter confidence in referendums. The Bill also makes consequential amendments to the Electoral Act where relevant.

Application of the foreign campaigner provisions

The Bill would amend the Referendum Act to prevent foreign campaigners authorising referendum matter, and fundraising or directly incurring referendum expenditure in a financial year equal to or more than $1,000. This is consistent with the Electoral Act and recognises that the threat of foreign influence in democratic referendums, perceived or actual, has the potential to erode democracy by compromising trust in voting results and trust in political participants.

The Committee has asked why the Bill does not allow for an individualised assessment of the threat posed by the foreign person or the form of expression sought to be prohibited. In the lead up to a referendum, including where a referendum is held on the same day as an election, campaigns on the proposed alteration may result in a high volume of communication of referendum matter and referendum expenditure. Requiring the AEC to conduct an individualised assessment of the threat posed by each foreign person or kind of referendum communication would be impracticable due to the complexity, volume of material and cost. The individualised assessments would not be completed prior to the polling day, diminishing the value of that approach and the integrity of the poll.

Instead, by aligning the foreign campaigner provisions across the Electoral Act and Referendum Act, the Bill will ensure a common approach to foreign campaigners across Commonwealth electoral events and provide the AEC with the mechanism to respond to foreign interference, further supporting Australians' trust in democratic processes. For donors and recipients the alignment of requirements to the extent practicable will also minimise compliance burden and risk.

I consider that the foreign campaigner framework proposed in the Bill provides an appropriate framework to safeguard integrity and trust in referendum events. I further note the circumscribed nature of the foreign campaigner provisions, which expressly exclude Australian permanent residents and New Zealand Citizens who hold subclass 444 (Special Category) visas, and also excludes communications for academic, educative and artistic purposes, news content and private communications to ensure the requirements are appropriately confined.

Reversal of the burden of proof

You have requested further advice in relation to the necessity for a rebuttable presumption that matter that expressly promotes or opposes a proposed law for the alteration of the Constitution, to the extent that it relates to a referendum, is a 'referendum matter'.

The Bill inserts new section 3AA into the Referendum Act, with new subsections 3AA(1) and (2) defining "referendum matter" based on the definition of "electoral matter" in the Electoral Act, adapted to a referendum context. Proposed subsection 3AA(6) provides exceptions for matter that is not "referendum matter".

Where contravention of the authorisation of referendum matter is raised, the Bill would require a person or entity to raise specific defences. This because these exemptions are matters that would be peculiarly within the knowledge of the defendant and would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter. This approach is consistent with the guidance provided by the *Guide to Framing Commonwealth Offences.*

The matters in proposed subsection 3AA(6) go the intended communication of the matter, for example if the dominant purpose of the communication was intended to be private communication, or satirical (see proposed subsections 3AA(6)(b) and (c)). As detailed in paragraph 73 of the Explanatory Memorandum to the Bill.

This approach is consistent with the *Guide to Framing Commonwealth Offence* as these are matters that would be peculiarly within the knowledge of the defendant and would be significantly more difficult and costly for the prosecution to prove than for the defendant to establish the matter.

As such the offence-specific defences in the Bill are appropriate, and I do not consider that it necessary to amend the Bill to provide that these matters are specified as elements of the offence.

Information-gathering powers

The Bill would establish an offence for non-compliance with a notice issued by the Electoral Commissioner, seeking information relevant to assessing compliance with the financial disclosure obligations proposed in the Bill, under proposed section 109N. This will support the ability of the AEC to investigate and address non-compliance.

This offence and related penalty provisions replicate the equivalent provisions of the Electoral Act. This replication provides consistency across the Electoral Act and Referendum Acts and supports understanding of those offences by those engaging in both electoral and referendum expenditure.

Exercise of the information-gathering powers is appropriately circumscribed. This includes a requirement that the Electoral Commissioner may only issue a notice where they reasonably believe the person or entity has information or documents relevant to an assessment of their compliance with Part XIIIA of the Bill. Further, before issuing a notice, the Electoral Commissioner is required to have regard to the costs a person would bear in complying with that notice. A person may also request, and must be granted, a review of the Electoral Commissioner's decision to issue a notice.

Proposed section 109Z further protects the privacy of information provide in compliance with a section 109N notice where this does not relate to a contravention of the civil penalty provisions of the Act. I also note the privilege against self-incrimination applies unless explicitly abrogated, which the Bill does not propose.

I am satisfied that the offence provisions are a necessary part of the establishment and enforcement of the financial disclosure obligations provided for in the Bill.

Safeguards

The Bill includes a range of safeguards to ensure the foreign campaigner provisions do not apply broadly, and that the Electoral Commissioner's information-gathering powers proposed in the Bill are exercised subject to reasonable limitations. These are outlined above.

The High Court of Australia has held that an implied freedom of political communication exists as part of the system of representative and responsible government created by the Australian Constitution. Proposed section 109ZA of the Bill provides that proposed Part XIIIA of the Bill (Referendum financial disclosure) does not apply to the extent that any constitutional doctrine of implied freedom of political communication would be infringed. The operation of the implied freedom is a matter for the High Court in each case.

Consideration of alternatives

The restrictions imposed by the Bill on foreign campaigners engaging in Australian referendums are proportionate to achieving the legitimate objective of safeguarding the integrity of referendums by ensuring that only those with a legitimate connection to Australia are able to influence Australian referendums. A less-restrictive approach may result in increased foreign campaigning activity which may undermine trust in the referendum process, and the ability to regulate compliance with the foreign campaigner provisions.

Referendums were the subject of the Standing Committee on Social Policy and Legal Affairs' 2021 *Inquiry in the constitutional reform and referendums*. That inquiry recommended the Referendum Act be updated to prohibit referendum campaign organisations from receiving gifts or donations of $100 or more from foreign donors, consistent with the Electoral Act (recommendation 8). The Committee recommended that the referendum process more generally is modernised (recommendation 10). That Committee accepted public submissions, conducted hearings, and considered previous reports related matters. The Bill responds to those recommendations.

The Bill was also referred to the Joint Standing Committee on Electoral Matters (JSCEM) for inquiry. That Inquiry received submissions on the Bill, and on 13 February 2022 JSCEM released its advisory report on the Bill. That report recommended that, subject to recommendations about strengthening enfranchisement opportunities and the provision of clear, factual, and impartial information, the Bill be passed.

In summary, I consider the Bill provides an appropriate framework for the regulation of foreign campaigners in referendums and the exercise of information gathering powers in relation to compliance with financial disclosure obligations proposed in the Bill. This framework replicates the existing provisions in the Electoral Act and will operate to prevent foreign donations and restrict foreign individuals and entities from exerting political influence in Australian referendums.

I thank you again for writing. I trust that this information will assist you in finalising your consideration of the Bill.

Yours sincerely

The Hon Anika Wells MP
Minister for Aged Care
Minister for Sport
Member for Lilley

Ref No: MC23-003158

Mr Josh Burns MP
Member for Macnamara
Chair of Parliamentary Joint Committee on Human Rights
PO Box 6100
CANBERRA ACT 2600
human.rights@aph.gov.au

Dear ~~Mr Burns~~ Josh,

Thank you for your correspondence of 9 February 2023 regarding the *Aged Care Quality and Safety Commission Amendment (Code of Conduct and Banning Orders) Rules 2022* (Code and Banning Orders Instrument) and *Quality of Care Amendment (Restrictive Practices) Principles 2022*.

Responses to each of the committee's queries are below.

Aged Care Quality and Safety Commission Amendment (Code of Conduct and Banning Orders) Rules 2022

Whether and how these information gathering powers would be circumscribed

The Code of Conduct for Aged Care (Code) began on 1 December 2022. The Code, contained within the Code and Banning Orders Instrument, sets out the minimum standards of behaviour for approved providers, their aged care workers and governing persons in order to help build confidence in the safety and quality of care for older Australians. The

Commission is responsible for monitoring and compliance of the Code.

As the committee notes, protecting the safety of vulnerable aged care recipients is a legitimate objective for the purposes of international human rights law, and taking action to enforce the Code is rationally connected to that objective.

The Aged Care Quality and Safety Commissioner (Commissioner) may become aware of issues relating to compliance with the Code through a range of different mechanisms, including complaints processes, SIRS reportable incident notifications and referrals from other regulators (for example the National Disability Insurance Scheme Quality and Safeguards Commission (NDIS Commission) and the Australian Health Practitioner Regulation Agency).

Once a decision has been made that a particular action, such as the use of information gathering powers, is appropriate in the circumstances to deal with compliance with the Code, the Commission will, as always, ensure that all relevant legislative requirements are adhered to in exercising powers or functions. This includes having due regard to procedural fairness, in accordance with section 23BG of the Code and Banning Orders Instrument and administrative law principles, to ensure that any action can be effectively taken and is legally defensible. For example, decision makers will make their decisions based on relevant considerations, will act in a manner that affords procedural fairness to those affected by a decision, and will explain those decisions in a clear way that people can understand.

The Department has advised that Section 23BG was inserted following consultation on the exposure draft of the Code and Banning Orders Instrument and explicitly states that the Commissioner must have due regard to the rules of procedural fairness in taking action under Division 3 of the Code and Banning Orders Instrument.

These provisions provide acceptable legislative safeguards for approved providers, their aged care workers and governing persons throughout a Code compliance investigation and any other regulatory action that may be taken as a result of the outcome of such an investigation. This is supported by the Commission's internal operational policies and processes, which outline what decision-makers should consider in deciding whether to exercise a power or function, as well as any mandatory requirements or preferred/expected policy positions relating to the exercising of a specific power or function.

Section 76(1B) of the *Aged Care Quality and Safety Commission Act 2018* (Commission Act) provides that the Commissioner must not delegate a function or power to a person under section 76(1) or (1A) unless the Commissioner is satisfied that the person has suitable training or experience to properly perform the function or exercise the power. Having regard to the requirement in section 76(1B) of the Commission Act, the Commissioner has delegated their power under section 23BE of the Aged Care Quality and Safety Commission Rules 2018 (Commission Rules) to Senior Executive Service Band 1, Executive Level 2 and Executive Level 1 Commission staff only. Through appropriate recruitment and performance management processes, there is ongoing oversight to ensure officers at these levels have suitable training and experience to perform their function.

The Commissioner's information gathering powers are also circumscribed by the Commission's statutory obligations under the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs). The Commission's Privacy Policy (Privacy Policy) states that the Commission will only collect the information it needs for the function or activity

being carried out, in accordance with APP 3. Further, in compliance with APP 6, the Privacy Policy provides that the Commission will generally only use and disclose personal information for the particular purpose for which it was collected and will not otherwise use or disclose personal information for another purpose unless the person's consent has been obtained, or the use or disclosure is permitted under the Privacy Act.

What threshold would be required to be met before the Commissioner may exercise these powers

The Commission manages non-compliance and potential non-compliance with the Code in accordance with the Commission's Compliance and Enforcement Policy. Consistent with this policy, the Commission takes a risk-based approach and responds in a way that is proportionate to the risks that the non-compliance or potential non-compliance poses to the safety, health, wellbeing and quality of life of aged care recipients.

The Commission's Compliance and Enforcement Policy notes that when potential non-compliance is identified, there may not initially be enough evidence to determine whether there is compliance or non-compliance, the extent of the non-compliance and/or the appropriate compliance response. In such circumstances, it may be necessary and appropriate for the Commission to use its information gathering powers, including those under section 23BD of the Code and Banning Orders Instrument, to obtain further information to be able to make a determination about non-compliance with the Code. This process supports procedural fairness as the worker will be offered an opportunity to respond to the matter. Decision-makers are responsible for determining all material questions of fact and basing each finding of fact on relevant supporting material.

Disclosure by the Commission of personal information relating to compliance with the Code may be necessary and appropriate, for example, because the personal information:

- promotes the safety and rights of other persons
- relates to the regulatory functions of another entity (for example another regulator such as the NDIS Commission) and is required by the other entity to exercise their powers or perform their functions
- is required by an approved provider to take appropriate action in relation to compliance with the Code by their aged care worker or governing person (as authorised by section 23BD(3)(a) of the Code and Banning Orders Instrument).

What safeguards would apply to protect information that has been collected and shared (including what happens once personal information has been collected and shared, how it is required to be stored, and whether it is required to be destroyed after a certain period)

The Commission has statutory obligations that it must comply with in relation to the collection, use, storage and disclosure of personal information under the Privacy Act, the APPs and the *Archives Act 1983*. The Privacy Policy outlines the personal information handling practices and expectations.

As noted above, the Privacy Policy states that the Commission will generally only use and disclose personal information for the particular purpose for which it was collected. The Commission also states in its Privacy Policy that it will not otherwise use or disclose personal information for another purpose unless it obtains the person's consent, or the use or disclosure is permitted under the Privacy Act. This is all in accordance with APP 6.

In relation to the storage and security of personal information, the Privacy Policy outlines the safeguards implemented by the Commission to protect personal information in its holdings against misuse, interference and loss, and from unauthorised access, modification or disclosure. The Privacy Policy also notes that when no longer required, the Commission destroys or archives personal information in a secure manner and as permitted by relevant legislation, including the Privacy Act and the *Archives Act 1983*. These personal information handling practices of the Commission are in compliance with its obligations under APP 11.

Further, as noted in the explanatory statement, the Commission and its staff are bound by legislative provisions in the Commission Act that regulate handling of 'protected information' collected by the Commission in carrying out its functions. All personal information, including sensitive information, acquired under or for the purposes of the Commission Act or the *Aged Care Act 1997* (Aged Care Act) is protected information for the purposes of those Acts. A breach of the protected information provisions under either Act is an offence, punishable by 2 years imprisonment. The existing penalties for misuse and unauthorised disclosure of protected information under the Commission Act and the Aged Care Act will protect and ensure safe handling of the information collected by the Commission.

Whether other, less rights-restrictive alternatives would be effective to achieve the same objective

The collection, use and disclosure of personal information relating to compliance with the Code is necessary and appropriate because the personal information:

- is directly related to the performance of the Commissioner's Code functions under section 16(da) of the Commission Act (and more broadly, the Commissioner's function under section 16(a) to protect and enhance the safety, health, wellbeing and quality of life of aged care recipients). The Code functions of the Commissioner are outlined in section 18A of the Commission Act and provide a function for the Commissioner to take action in relation to compliance with the Code by approved providers, and their aged care workers and governing persons, and to do anything else relating to that matter as specified in the Commission Rules
- the use of the personal information will relate to an actual, alleged or suspected instance of non-compliance with the Code by an approved provider or their aged care worker or governing person.

It is important for the Commissioner to be able to collect, use and disclose information, including personal information, as part of investigating alleged breaches of the Code in order to be able to effectively investigate and ascertain whether a breach has occurred and where a breach has occurred, to ensure that appropriate action is taken to protect aged care recipients.

The Commissioner's discretion in taking certain actions (including information gathering and sharing) in relation to compliance with the Code is necessary to ensure that the Commissioner can take the most reasonable action allowable to protect the health, safety and wellbeing of aged care recipients, noting that any actions are in accordance with the Commission Rules, the Commission Act, other relevant legislation and the principles of administrative law. If the Commissioner's discretion was limited, the Commissioner's ability to protect the health, safety and wellbeing of aged care recipients could be limited and could potentially cause harm.

The Commission's information gathering and sharing powers under the Code and Banning Orders Instrument are therefore proportionate having regard to the above. There are no effective less rights-restrictive alternatives available for the Commission to achieve the same objective.

Whether any less rights restrictive alternatives to publicly publishing the register (including the register being available only to employers, or on request) would not be effective to achieve the objective of this measure

While the majority of aged care workers exceed expectations in their care of older Australians, like in all industries, there will be occasions when individuals are not suited to this highly trusted work. The Code and Banning Orders Instrument ensures that the Aged Care Quality and Safety Commission is able to consider matters as they arise, investigate if required and respond to ensure ongoing compliance. This approach upholds principles of safety and dignity for both the workforce and care recipients. The introduction of the Code and Banning Orders Instrument is a positive step forward for the sector and will support aged care providers, their governing persons and aged care workers to deliver safe and quality care to older Australians.

Banning orders are considered one of the Commission's most serious enforcement actions and will only be appropriate for the most serious cases of poor conduct. This can be evidenced in only four banning orders having been made since 1 December 2022. Those named are currently subject to criminal justice processes in relation to alleged fraud and acts of physical violence directly involving care recipients. With approximately 380,000 people working in aged care this is a very small proportion of the workforce who may find themselves subject to a banning order. Never-the-less, the Government takes seriously the need for quality and safety in aged care and this regulatory option is an important tool in the suite of safeguards being delivered in line with the Royal Commission's recommendations.

In order to ensure that the register of banning orders (Register) functions properly, it is considered necessary for the personal information of banned individuals to be made public. This is due to the importance of preventing banned individuals from working in the aged care sector and the potential significant consequences for public health and safety if this does not happen.

This aims to ensure the safety of aged care recipients by providing future employers notice of individuals who were found unsuitable to provide aged care or specified types of aged care services.

The Department has advised this provision aligns with the approach taken under the National Disability Insurance Scheme (see section 73ZS of the *National Disability Insurance Scheme Act 2013*).

The Australian Government is seeking to align worker regulation arrangements across the aged care and disability support sector where it is reasonable and practical to do so. Worker screening is an area where the Australian Government is seeking alignment. While worker screening has not yet been expanded to aged care, individuals with an NDIS worker screening clearance can rely on this clearance to work in the aged care sector. This has the effect of preventing banned individuals from working in either the aged care sector or in the National Disability Insurance Scheme.

The publication of the Register is also intended to act as a deterrent to individuals from engaging in conduct that could result in the issuing of a banning order.

Publication of this information is considered reasonable, necessary and proportionate in order to protect the safety of vulnerable older Australians.

Whether it is intended that the date of birth of each person subject to a banning order will be published as a matter of routine, and if so why

It is not intended that the date of birth of each person subject to a banning order will be published as a matter of routine. The Commission will consider whether there is a concern about misidentification for each person subject to a banning order, noting that the inclusion of additional identifying information is to safeguard the identities, reputations, and rights of third parties with similar names. The date of birth will only be added where misidentification is of sufficient concern. The date of birth information previously published has been removed and this will not be standard practice.

Why the instrument does not require the Commissioner to correct inaccurate or misleading information on the register (when brought to their attention) in all instances

Under subsection 74GI(4) of the Commission Act, the Commissioner must ensure that the Register is kept up to date. Sections 23CE and 23CF of the Code of Conduct and Banning Order Instrument are consistent with APP 13 in Schedule 1 to the *Privacy Act 1988*. APP 13 sets out minimum procedural requirements for correcting personal information an entity holds about an individual.

The Commission undertake their functions in accordance with APP 13. It further operates on the basis that there is nothing in APP 13 which excludes information contained in a Commonwealth record (such as APP 11.2(c) which relates to the destruction or de-identification of personal information). The Commission understands information contained in records in its possession or control would also be a Commonwealth record and subject to the requirements of the *Archives Act 1983*.

As noted by the committee, the Commissioner's general discretion under section 23CF of the Instrument to correct information in the Register is a safeguard in terms of ensuring that the content of the register is accurate. The Commissioner's discretion, rather than obligation, to correct personal information in the Register is consistent with APP 13, which does not impose an obligation on APP entities (such as the Commission) to correct personal information in all instances. Rather, APP 13 requires that APP entities must take reasonable steps to correct an individual's personal information, and must only do so if it can be satisfied that the information is incorrect. The level of discretion afforded to the Commissioner under section 23CF of the Instrument is therefore appropriate having regard to the requirements of APP 13. The discretion also takes into account that there may be other legal obligations in certain circumstances (for example, where a family and domestic violence protection order is in place) which may prevent the Commissioner from publishing certain information to the register.

APP 13 operates alongside and does not replace other informal or legal procedures by which an individual can seek correction of their personal information, including under the *Freedom of Information Act 1982*.

If it would assist, the Department can provide a briefing on these matters at the committee's convenience.

Thank you for writing on this matter.

Yours sincerely

[redacted]

Anika Wells

24 February 2023