The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Multicultural Affairs
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MC23-033717

Senator Dean Smith
Chair
Senate Standing Committee for the Scrutiny of Bills
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Chair Dean

Thank you for your correspondence of 30 November 2023 to the former Minister for Home Affairs and Minister for Cyber Security, the Hon Clare O'Neil MP concerning the Senate Standing Committee for the Scrutiny of Bills' consideration of the Migration Amendment (Bridging Visa Conditions) Bill 2023 and the Migration Amendment (Bridging Visa Conditions and Other Measures) Bill 2023.

Thank you also for your further letter of 14 August 2024 in relation to this matter, addressed to me in my capacity as the Minister for Home Affairs and Minister for Immigration and Multicultural Affairs. I acknowledge the delay in responding to the Committee's request for information in relation to these Bills. I also acknowledge the Committee's longstanding position that it is important to provide a response to scrutiny concerns raised by the Committee, including in circumstances where a Bill has already passed.

My response to the matters raised by the Committee in relation to the two Bills is provided at Attachment A. I appreciate the time the Committee has taken to consider both Bills, and I trust this information is of assistance to the Committee to complete its consideration of them.

Yours sincerely

TONY BURKE
23/12/2024

Attachment A

SENATE STANDING COMMITTEE FOR THE SCRUTINY OF BILLS
Scrutiny Digest 15 of 2023

Migration Amendment (Bridging Visa Conditions) Bill 2023
Migration Amendment (Bridging Visa Conditions and Other Measures) Bill 2023

General comments

The BVC Bill and BVCOM Bill include amendments of the *Migration Act 1958* (the Migration Act) and the *Migration Regulations 1994* (the Migration Regulations) to ensure non-citizens released from immigration detention following the High Court judgment in *NZYQ v Minister for Immigration, Citizenship and Multicultural Affairs (S28/2023)* [2023] HCA 37 (NZYQ) on 8 November 2023 and those in similar circumstances in the future (the NZYQ-affected cohort) are subject to appropriate visa conditions on the Bridging (Removal Pending) visa (BVR) granted to them following release.

The BVC Bill was introduced and passed on 16 November 2023. On 27 November 2023, the BVCOM Bill was introduced. On 5 December 2023, Senate amendments were made to the BVCOM Bill, including renaming the BVCOM Bill the Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Bill 2023 (BVSOOM Bill). On 7 December 2023, the *Migration Amendment (Bridging Visa Conditions) Regulations 2023* (BVC Regulations) were registered on the Federal Register of Legislation; these Regulations commenced on 8 December 2023, at the same time as the amendments in the BVCOM Bill. The below responses to the Committee's request for further information on the BVC Bill and the BVCOM Bill includes references to measures in both Bills as passed, and the BVC Regulations, where relevant.

The NZYQ-affected cohort is made up of non-citizens who have been refused grant of a visa, or had their visa cancelled, and who are on a removal pathway but who have no real prospect of removal becoming practicable in the reasonably foreseeable future. Of the current known cohort, the majority were refused a visa, or had their visa cancelled, on character grounds. Others in the cohort had their visa cancelled on other grounds, but had not previously been granted a bridging visa due to risks they present to the Australian community.

The objective of the amendments in the Bills and the Regulations is to ensure that members of the NZYQ-affected cohort are managed in the community in a way that supports community safety objectives and enables the management of the cohort to a removal outcome once removal becomes reasonably practicable.

As noted above, following the introduction of the BVCOM Bill, Senate amendments were made to the Bill, including a name change, and the BVCOM Bill was passed and enacted as the *Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Act 2023.* Supporting amendments were also made to the *Migration Regulations 1994* by the BVC Regulations.

These amendments support and strengthen the BVR framework for the NZYQ-affected cohort including by:

- Creating a framework in the *Criminal Code* for court-issued Community Safety Orders. The Community Safety Orders scheme is a new judicially supervised regime that will enable the Minister administering the Migration Act (the Minister) to apply for court orders to detain certain high risk violence and sexual offenders for the purpose of community protection, or to impose other supervisory conditions, complementary to those already imposed on a BVR, in order to protect the Australian community.
- Creating new criminal offences for breaches of BVR conditions 8622 (no work with minors or vulnerable people), 8623 (must not go within 200 metres of a school) and 8624 (must not make contact with victim or victim's family) that appropriately apply where a person has a relevant criminal history.
- Changing the BVR grant provisions in regulation 2.25AA and 2.25AB to allow the Minister to grant a BVR to a non-citizen, without application, without requiring the Minister to be satisfied that the non-citizen will comply by the conditions of the visa. This amendment was necessary to ensure that a non-citizen cannot avoid the imposition of those conditions – and the consequences for breaching them – merely by informing the Minister they will not comply with the conditions. Prescribing that these conditions must be decided by the Minister in a sequential order, to ensure that the extent to which other BVR conditions contribute to the protection of the Australian community is appropriately considered prior to imposing further conditions.
- Creating a 12 month time limit after which BVR conditions 8617, 8618, 8620 and 8621 cease to have effect. These are conditions that must be applied unless the Minister is satisfied that they are not reasonably necessary for the protection of the community. At any time before or after the 12 month period, the Minister can re-grant the person a BVR with these conditions imposed (subject to consideration of the Community Safety Test). This amendment ensures regular review that conditions remain appropriate for the particular circumstances of the individual and allows for a BVR to be re-granted without these conditions imposed if the Minister is satisfied that they are no longer reasonably necessary for the protection of the community.
- Creating a grant power in the Migration Act to enable new BVR to be granted, by operation of law, where a person is issued a Community Safety Order. This new BVR will be subject to a range of Status Resolution and National Security Conditions. These conditions are intended as far as possible to complement, but not duplicate, conditions that a Court might impose on a Community Safety Order.

Responses to the Committee's specific questions

Undue trespass on rights and liberties; broad scope of offence provisions; significant penalties in primary legislation

Why it is proposed to have conditions that result in a serious deprivation of personal rights and liberties, such as a requirement to remain in a specified address for a specified period of time and a requirement to wear a monitoring device at all times mandatorily apply to all holders of the Bridging (Removal Pending) Visa?

The conditions 8620 (curfew) and 8621 (electronic monitoring) must be applied unless the Minister thinks it is not reasonably necessary for the protection of the community.

This means the risk that each BVR holder poses can be assessed and those conditions are applied in consideration of that risk. Additionally the amendments create a 12 month time limit after which these BVR conditions cease to have effect. These are conditions that must be applied unless the Minister is satisfied that they are not reasonably necessary for the protection of the community. At any time before or after the 12 month period, the Minister can grant the person a new BVR with these conditions imposed or not imposed (subject to consideration of the Community Safety Test). This amendment ensures regular review that conditions remain appropriate for the particular circumstances of the individual and allows for a BVR to be granted without these conditions imposed if the Minister is satisfied that they are no longer reasonably necessary for the protection of the community.

These BVR conditions are appropriate because the NZYQ-affected cohort includes individuals with serious criminal histories who are no longer able to be managed in immigration detention where there remains no prospect of removal in the reasonably foreseeable future.

The curfew has the community protection purpose of BVR holders who have, for example, been assessed to fail the character test and to be of particular concern to the Minister in terms of future criminal offending. Therefore any deprivation of liberty that the curfew may constitute, is intended to protect public order and the rights and freedoms of others, and would not be arbitrary and be necessary, reasonable and proportionate to achieving that objective.

One purpose of electronic monitoring is to deter the BVR holders from committing further offences, knowing they are being monitored, and thereby keep the community safe. The electronic monitoring will also assist with prevention of absconding behaviour which is contrary to the obligation of the BVR holder to engage in the Department's efforts to facilitate their removal.

The use of electronic monitoring ensures the BVR holder meets the obligation where there is a higher likelihood of non-compliance by the BVR holder, and provides an alternative avenue for compliance that will be more suitable to some circumstances such as where additional support alone will not prevent reoffending.

The provisions put beyond doubt the types of behaviours that are unacceptable for NZYQ-affected persons to engage in whilst they resolve their migration status residing in the Australian community, and the sanctions that will apply to any person who breaches the conditions of the BVR they are granted. This is appropriate and reasonable to ensure the Australia community can continue to have confidence that the migration system is being well-managed in respect of this cohort.

Why it is proposed to have significant penalties of a mandatory minimum sentence of 1 year imprisonment and a maximum penalty of 5 years imprisonment applicable to the offences under subsections 76B(1), 76C(1), 76D(1), 76D(2), 76D(3) and 76D(4), and proposed subsections 76DAA(1), 76DAB(1) and 76DAC(1), when these offences relate to breach of visa conditions and do not require consideration as to whether the conditions are reasonably necessary for the protection of the Australian community? The committee's consideration of this matter would be assisted by reference to the Attorney-General's Department's Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers?

The mandatory minimum sentence of one year's imprisonment was proposed by the Opposition and agreed in the Senate as an amendment of the Bill on 16 November 2023. The use of a minimum sentence of one year's imprisonment and maximum penalty of five years imprisonment or 300 penalty units reflects the seriousness of the regard that the NZYQ-affected cohort are expected to have towards the conditions imposed on their BVR and the seriousness of the offence if these conditions are contravened, reflecting the level of protection necessary for community safety and the management of the cohort.

As BVR holders who continue to be NZYQ-affected cannot be detained in immigration detention, the usual potential consequences for breaching visa conditions, cancellation of that visa and immigration detention, is not available. This removes these measures as an effective deterrent against non-compliance with reporting requirements and other key visa conditions.

Breaches of conditions that fall within the scope of the new offences are subject to the usual judicial processes. This includes the assessment by the Commonwealth Director of Public Prosecutions of whether to pursue a prosecution, taking into account whether it is in the public interest to do so. The defence of a reasonable excuse is available, and the court retains discretion to consider individual circumstances during the judicial processes.

Members of the NZYQ-affected cohort have no substantive visa to remain in Australia, having had their visa applications refused, or a visa cancelled, in most cases on character grounds under section 501 of the Migration Act. Consequently, the Government considers that mandatory minimum sentencing is proportionate to the particular circumstances of the NZYQ-affected cohort and aimed at the legitimate objective of protecting community safety.

The mandatory minimum sentence if convicted following a fair hearing before a court reflects the seriousness of the offending and the need to protect community safety and the most vulnerable members of Australian society.

Whether a list confirming the visa conditions under Schedule 8 of the Migration Regulations that attach to the offence provisions under subsections 76B(1), 76C(1), 76D(1), 76D(2), 76D(3) and 76D(4), and proposed subsections 76DAA(1), 76DAB(1) and 76DAC(1) can be provided.

The following table outlines the visa conditions that are within scope of the relevant offence provisions:

Offence provision	**Related visa condition(s)**
Section 76B	8401,8513, 8542, 8543, 8552, 8561, 8615
Section 76C	8620
Section 76D	8621
Section 76DAA	8622
Section 76DAB	8623
Section 76DAC	8624

Regulation 2.25AC provides that the following reporting conditions that may be imposed on a BVR are not conditions that engage the offence in section 76B – visa conditions 8612, 8616, 8617, 8618 and 8621.

What are the consequences of breaching a visa condition that does not attach to the offences under subsections 76B(1), 76C(1), 76D(1), 76D(2), 76D(3) and 76D(4), or proposed subsections 76DAA(1), 76DAB(1) and 76DAC(1)?

The conditions that do not attract criminal penalties are imposed to ensure that it is clear for BVR holders in the NZYQ-affected cohort what behaviour is expected of them while they remain in the Australian community. Individuals who breach these BVR conditions will be warned and counselled about expected conduct. These conditions also appropriately support continuing engagement between the individual BVR holder and the Department in relation to their migration status and any changes in their circumstances, including where the visa holder's removal from Australia may become reasonably practicable.

The Government has introduced the Community Safety Order scheme in the Criminal Code, through the BVCOM Bill as amended in the Senate – establishing legislation to provide for Community Safety Detention Orders and Community Safety Supervision Orders that can be issued by a court, on application to the court by the Immigration Minister. Relevantly, previous compliance with visa conditions is one of the factors to be taken into account when assessing whether a person should be referred to the Court for consideration under these new provisions.

What conduct may fall within the scope of 'reasonable excuse', whether examples can be provided of such conduct, and what measures will be implemented to minimise the risk that visa holders are likely to be overly cautious in considering whether the reasonable excuse defence is applicable to their circumstances?

Whether conduct falls within the scope of the defence of 'reasonable excuse' for the purposes of the new offences is a matter for the court to determine on a case by case basis based on submissions made and evidence adduced by the prosecution and the accused in the course of proceedings.

The inclusion of the defence ensures that there is a mechanism where an accused can put forward what they consider to be a justification for the alleged behaviour, as a defence for the prosecution of the offence. Including the 'reasonable excuse' defence ensures that the offences strike the appropriate balance between deterring and punishing offending while affording for reasonably excusable behaviour on a case by case basis, and as part of a fair hearing by the courts.

Procedural fairness

What information must be provided to the visa-holder by the minister when inviting the visa-holder to make representations?

The Minister may invite the person to make representations, in a manner specified by the Minister, as to why one or more of the conditions attached to a BVR should not apply. The information to be provided would be determined on a case-by-case basis, but at a minimum will include any information that is prescribed in the *Migration Regulations 1994*. No regulations have been made for the purposes of this provision at the time of providing this response to the Committee.

What information must be disclosed by visa-holders when making representations to the minister regarding the application of conditions?

The information to be disclosed by BVR holders in making a representation to the Minister would ultimately be a matter for the visa holder. The BVR holder will be able to provide the Minister with any additional information the visa holder considers relevant to making representations to the Minister regarding the application of BVR conditions and why the BVR should not be subject to one or more of the prescribed conditions. If the BVR holder makes representations to the Minister under new section 76E and the Minister is satisfied that those conditions are not reasonably necessary for the protection of any part of the Australian community, the Minister must grant a further BVR that is not subject to any one or more of the prescribed conditions. In making representations to the Minister, it would be appropriate for the BVR holder to have regard to these requirements.

Why 'the conditions are not reasonably necessary for the protection of any part of the Australian community" is an appropriate test for removing mandatory visa conditions, noting it is a subjective standard and that broad and restrictive conditions are applied on all individual visa holders within the class?

Why 'are not reasonably necessary for the protection of any part of the Australian community' is the only criterion considered relevant to the relaxation of conditions?

Why more guidance has not been included in the legislation to guide the minister's determination of whether conditions of 'are not reasonably necessary for the protection of any part of the Australian community?

Many NZYQ-affected individuals would not otherwise meet character or security requirements for a visa to remain in Australia; however, they can no longer be managed in immigration detention. Many have committed serious criminal offences, including murder and serious sexual assault. The Government is committed to monitoring the behaviour of these individuals and, where necessary, imposing additional measures to protect the Australian community.

The individual circumstances of each BVR holder will be considered to assess whether conditions are necessary for the protection of the Australian community. Conditions such as curfew (8620) and electronic monitoring (8621) must be imposed unless the Minister considers it is not reasonably necessary for the protection of the community. This provides scope for the Minister to consider whether it is not reasonably necessary in an individual's circumstances to impose those conditions.

Importantly, where these conditions are imposed, they will be subject to a 12 month time limit after which they cease to be in effect on the individual's BVR. This ensures the circumstances of the individual are regularly reviewed and that assessments about whether the condition is reasonably necessary for the protection of the community remains relevant and appropriate.

To improve proportionality, the BVC Regulations (registered on 7 December 2023) prescribe that condition 8401 (requirement to report) cannot be imposed where electronic monitoring (8621) is imposed. This ensures that a reporting requirement is not unnecessarily imposed where the holder is already subject to the electronic monitoring condition.

The BVC Bill also created new conditions that will only apply where a person has a relevant criminal history. For example, conditions 8622 (the visa holder must not work or participate in any regular activity involving more than incidental contact with minors or vulnerable people), 8623 (the visa holder must not go within 200 metres of a school) apply only where the individual has been convicted of an offence involving a minor or vulnerable person. Condition 8624 (must not make contact with victim or victim's family) applies only where a person has been convicted of an offence involving violence or sexual assault. Further, the BVC Regulations prescribe condition 8262, which provides that if a BVR holder has been convicted of an offence involving a minor or a vulnerable person, the holder must notify the Minister of a change in an online profile or user name. The applicability of these conditions only to BVR holders who have previously been convicted of offences involving a minor or a vulnerable person ensures those conditions are appropriately targeted to protecting the Australian community and that the conditions are proportionate and reasonable to the circumstances of the individual.

The conditions applied to the BVR holders in this cohort ensures the Australian community is appropriately protected. If the BVR holder makes representations to the Minister regarding the imposition of the visa conditions, the Minister may then determine whether the conditions are not reasonably necessary for the protection of the community. Importantly, without limiting the Minister's discretion, the test allows for consideration of the seriousness of harm to the community caused by the BVR holder, including the impact on victims, compliance with visa conditions, relevant behaviour known to the Minister (including emerging or diminishing risks to the Australian community), and any other relevant factors.

This legislation allows the Minister to consider the particular circumstances of each NZYQ-affected person before determining whether certain BVR conditions are reasonably necessary for the protection of the Australian community. This ensures the legislation will achieve the intended policy outcomes and can be adapted to a variety of different situations and scenarios in a dynamic operating environment. It also ensures the risk that each individual BVR holder poses can be assessed and those conditions are applied where appropriate in consideration of that risk.

Whether decisions made by the minister under subsection 76E(4) are eligible for independent merits review by the Administrative Appeals Tribunal and, if not, why not?

Decisions made under subsection 76E(4) are merits reviewable under Part 5 of the *Migration Act 1958.*

The committee requests the minister's detailed justification as to why items 9, 10, 11 and 12 of Schedule 2 have been amended to allow for the Minister to orally specify matters for a visa holder to comply with, noting that oral notice is not as clear as written notice.

Non-citizens granted any visa, including a BVR, are notified in writing of the decision to grant the visa. This notification includes information about all conditions that apply to the holder of the visa.

In the case of BVRs granted under this legislation, the amendments allow – in addition to the written notice – for officers of the Department to provide oral notification to each individual and explain the conditions that apply. Interpreters are available for BVR holders during these conversations if required.

Where a BVR holder's primary language is not English, oral notification of a requirement to report, or any change in reporting conditions, affords the BVR holder the opportunity to ask questions to clarify and confirm their understanding in their preferred language. Interpreters are available during these conversations for BVR holders if required.

During subsequent interactions with the Department, BVR holders are reminded of their obligations to comply with visa conditions include to report any changes in circumstances, in addition to discussing the person's well-being.

Significant matters in delegated legislation

The committee requests the minister's detailed advice as to why it is considered necessary and appropriate to allow delegated legislation to change the visa conditions that form elements of the offences under sections 76B, 76C and 76D.

Section 76B – the offence relating to monitoring conditions of certain bridging visas – includes provision to carve out certain conditions imposed on a BVR from the scope of the offence. Regulation 2.25AC provides that the following conditions are not conditions that engage the offence in section 76B – visa conditions 8612, 8616, 8617, 8618 and 8621. This provides that a breach of one or more of these prescribed conditions by the BVR holder cannot constitute an offence under subsection 76B(1) of the Migration Act. This ensures that the BVR visa conditions that remain within scope of the offence focus appropriately on establishing criminal liability on the most serious threats to community safety, with the legislative framework providing for a graduated approach to sanctions and penalties. Any regulations made for this purpose are a disallowable legislative instrument, and would be appropriately subject to parliamentary scrutiny. While noting that the Digest also includes reference to sections 76C and 76D (relating to requirements of conditions dealing with curfew and monitoring), only section 76B includes a provision to make regulations to carve out conditions from the scope of that offence. Sections 76C and 76D are specific offences dealing with curfew and monitoring device requirements respectively.

Broad delegation of administrative powers and functions; significant matters in delegated legislation; privacy; retrospective application

Why it is necessary and appropriate to allow powers relating to monitoring devices and equipment to effectively be delegated to any person?

Whether the bill can be amended to provide legislative guidance as to the categories of people to whom those powers might be delegated.

The Government does not propose to pursue further amendments of the kind proposed by the Committee at this time, noting that the Bills have both been passed and enacted. The Department has established polices and processes in place in relation to considering the appropriate delegation of any powers or functions of the Minister or another officer holder provided for in the Migration Act and Regulations. Any delegation of a legislative power or function – or authorisation of a person as an authorised officer – must be in writing. Appropriate consideration is given, at the time of making a delegation or authorisation instrument, in relation to requisite qualifications, training or experience, consistent with established departmental practice. Additional support and guidance is provided to delegates and authorised officers through the Department's Policy and Procedure Control Framework, together with related training and assurance mechanisms.

Whether any safeguards or limitations exist on the operation of an authorised officer's powers under proposed subsection 76F(1), noting that there appears to be no limits on what may be 'convenient' for an authorised officer to require a person subject to monitoring to do.

Section 76(4) of the *Migration Act 1958* provides that an authorised officer's exercise of power under subsection 76F(1) is subject to any conditions, restrictions or other limitations that are prescribed by the regulations. This framework provides a mechanism to implement appropriate safeguards as needed. Further, any regulations made for these purposes would be subject to Parliamentary scrutiny and disallowance pursuant to section 42 of the *Legislation Act 2003*.

Why it is necessary and appropriate to provide that an authorised officer can disclose information, including personal information, to any other person for such a wide range of purposes under proposed subsection 76F(2)?

The scope of the authorisation to collect, use and disclose information raised a number of policy issues which were carefully worked through by my Department, including:

- who should be authorised to collect, use and disclose information
- the purpose for which the information may be collected, used and disclosed
- the scope of the information covered, for example:
  - the initial disclosure of information by the Commonwealth to State or Territory authorities, contractors and subcontractors for the purpose of configuring a monitoring device
  - information obtained through the use of monitoring devices
  - information obtained through other surveillance and enforcement activities, such as curfew checks
- safeguards or restrictions to prevent the misuse of this information.

Further, I am advised that any use of personal information by ABF officers and the department's staff would likely be consistent with the *Privacy Act 1988*.

This approach is necessary and appropriate where a disclosure is made to a law enforcement body, such as the Australian Federal Police, or a State or Territory police service in relation to a person who is alleged to have committed an offence.

This disclosure might occur where a person who is subject to monitoring is released into the community in a different State, with the relevant receiving State or Territory police service able to be notified of the person's personal information including the offence the person served one or more custodial sentences for, and the reason the person is subject to monitoring. This is particularly the case if the removal of the person from Australia becomes practicable in the reasonably foreseeable future or a visa held by the person ceases to be in effect (for example, because they are in breach of a visa condition).

A further example is the need to disclosure information for use where a law enforcement body is investigating or prosecuting a criminal offence.

What safeguards are in place to protect the personal information of both individuals subject to monitoring and any other person whose information has been collected, used or disclosed?

Why it is considered necessary and appropriate to leave conditions, restrictions or limitations on an authorised officer's exercise of powers under subsection 76F(1) to delegated legislation?

Personal information collected in the monitoring process would be held in accordance with the collection and security requirements of the Australian Privacy Principles (APPs), my Department's policies and procedures and the Australian Government Protective Security Policy Framework (AGPSPF). The Department holds personal information in a range of audio-visual, paper and electronic based records (including in cloud-based applications and services). The Department complies with the AGPSPF for protecting departmental resources (including information) from harm or unauthorised access. If personal information held by the department is lost, or subject to unauthorised access or disclosure, the Department will respond in accordance with the Office of the Australian Information Commissioner's guidelines. Only the Minister, the Secretary of the Department or the Australian Border Force Commissioner may provide for a person to be an authorised officer for the purposes of section 76F.

The committee also requests the minister's advice as to whether actions provided for under proposed section 76F undertaken prior to the commencement of the bill had lawful basis, noting that the bill appears to retrospectively validate such actions.

The purpose of section 76F is to make clear, on the face of the Migration Act, the powers that an authorised officer may exercise in relation to a person who is subject to monitoring, and in relation to the collection, use and disclosure of personal information in these circumstances. In doing this, section 76F also clarifies the interaction of these powers with other laws of the Commonwealth, States and Territories. Section 76F operates prospectively from the date of commencement, and the Bill did not include a validation provision to validate past actions. The inclusion of new section 76F is intended to clarify and provide greater detail on the face of the legislation in relation to available powers relating to monitoring devices and related monitoring equipment. It also provides scope to establish additional legislative constraints on an authorised officer's exercise of powers under subsections 76F(1) or (2), by way of regulations made for the purposes of subsection 76F(4).

The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Multicultural Affairs
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MC24-005512

Senator Dean Smith
Chair
Senate Scrutiny of Bills Committee
Suite 1.111, Parliament House
CANBERRA ACT 2600

Dear Senator Dean

Thank you for your correspondence of 28 February 2024 to the former Minister for Immigration, Citizenship and Multicultural Affairs, the Hon Andrew Giles MP, concerning the Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Bill 2023. Your correspondence has been referred to me as the matter falls within my portfolio responsibilities. I apologise to you and members of the Senate Scrutiny of Bills Committee (the Committee) for the delay in responding.

I appreciate the Committee's concerns with respect to the circumstances around the introduction of the abovementioned Bill.

As you are aware, in line with the High Court ruling in *NZYQ v Minister for Immigration, Citizenship and Multicultural Affairs & Anor* (NZYQ) on 8 November 2023, all non-citizens for whom there were no real prospect of removal from Australia becoming practicable in the reasonably foreseeable future were required to be released from immigration detention.

This included a number of individuals who had previously committed serious violent or sexual offences, some of whom constitute a reasonable concern in relation to possible reoffending, which consequently necessitated new measures to ensure community safety.

In addition to the development of new monitoring conditions, the establishment of the Community Safety Order scheme was a measure this Government felt was required to best mitigate the risk of harm to the community.

Importantly, for a Community Safety Detention Order or Community Safety Supervision Order to be made by the court, the Minister for Immigration must first be convinced of the risk of harm posed to the community, based on a body of evidence and recommendations provided by the Community Protection Board. If convinced, the Minister would then apply to the courts for the making of an order, thereby ensuring the preservation of the rights of the individual through the conduct of independent judicial processes.

As set out in the *Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Act 2023*, the maximum duration of any order is limited to three years, to be reviewed annually. As the committee has noted, the court could make successive orders, however they would not constitute extensions of a previous order. Each order would be considered, made and reviewed on its own merits by the court, ensuring that any detention or deprivation of liberty could not by definition be arbitrary or indefinite.

Thank you for bringing your concerns to the Government's attention.

Yours sincerely

TONY BURKE

23 / 12 / 2024

The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Multicultural Affairs
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MC24-034939

Senator Dean Smith
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

by email: scrutiny.sen@aph.gov.au

Dear Chair Dean

Thank you for the correspondence of 28 November 2024 from the Secretary of the Senate Standing Committee for the Scrutiny of Bills, Ms Anita Coles, concerning the Committee's consideration of the Migration Amendment (Prohibiting Items in Immigration Detention Facilities) Bill 2024.

I appreciate the time the Committee has taken to consider the Bill. My response to the matters raised by the Committee in its *Scrutiny Digest 15 of 2024* is provided at Attachment A. I trust this information is of assistance to the Committee in its further consideration of the Bill.

Yours sincerely

TONY BURKE

13 / 12 / 2024

Attachment A

SENATE STANDING COMMITTEE FOR THE SCRUTINY OF BILLS

Scrutiny Digest 15 of 2024

Migration Amendment (Prohibiting Items in Immigration Detention Facilities) Bill 2024

The Senate Standing Committee for the Scrutiny of Bills (the Committee) has requested advice from the Minister for Home Affairs in relation to the Migration Amendment (Prohibiting Items in Immigration Detention Facilities) Bill 2024 (the Bill). The Committee's initial scrutiny of the Bill is set out in the Committee's *Scrutiny Digest 15 of 2024* (at pp. 11-19). The information below is provided to assist the Committee in its further consideration of the Bill.

Responses to the Committee's specific questions

1.43 The committee notes it has previously considered the effect of very similar proposed measures on personal rights and liberties. The committee retains concerns as to the breadth of the proposed powers and as such seeks the minister's advice as to:

- **why the power to search or seize 'prohibited things' applies to all detainees, regardless of whether possession of such a thing by that individual detainee poses a specific risk;**
- **would the legislation enable authorised officers to seize prohibited things (such as mobile phones) from all detainees, even where only certain detainees pose a risk of possessing them, on the basis that the authorised officer considers seizing the thing to be necessary to lessen a risk to the good order of the facility;**
- **when would the search or seizure of a prohibited thing be likely to be considered necessary to prevent or lessen a risk to 'the order of the immigration detention facility', and why is it appropriate to include 'order of the detention facility' in addition to risks to health, safety or security or persons;**
- **why the bill does not provide that strip searches to seize 'prohibited items' are only conducted when absolutely necessary;**
- **why there is no requirement that the authorised officer have formed a reasonable suspicion that the person to be searched possesses them prior to the search occurring; and**
- **whether there exists any monitoring and oversight of the use of force by authorised officers and their assistants, including access to review for detainees to challenge the use of force and the strip search powers.**

The *Migration Act 1958* provides powers of examination, search, detention and identification that are exercisable in particular places or in relation to particular people. The powers that may currently be exercised in relation to detainees are:

- searching detainees, their clothing and any property under their immediate control;
- conducting screening procedures in relation to detainees;
- conducting strip searches of detainees;
- retaining certain items found in the possession of detainees in the exercise of the above powers.

Currently, officers may exercise those powers for the purposes of finding out if the detainee has hidden on their person, in their clothing, or in their possession, a weapon or other thing capable of being used:

- to inflict bodily injury; or
- to help the detainee or another person escape from immigration detention.

The Bill includes amendments of the Migration Act to expand the purposes for which the search and screening powers outlined above may be used. Under the proposed amendments of the Act, the powers may also be exercised in order to find prohibited things in the possession of detainees or people entering immigration detention facilities.

The Bill proposes to expand the search and seizure provisions to allow authorised officers to screen and search for prohibited things (determined in a legislative instrument), which may include mobile phones, SIM cards, internet-capable devices, illegal drugs and prescription drugs held by a person other than the person to whom they are prescribed.

Where the prohibited thing is otherwise lawful to possess but poses a risk to the security, safety or health of detainees or staff, or the order of the facility, authorised officers must additionally believe on reasonable grounds that the seizure of the thing is necessary to prevent or lessen that risk. For example, it may be necessary to seize mobile phones, SIM cards, and internet-capable devices (if determined to be a prohibited thing) from detainees in certain circumstances to ensure the health, safety and security of detainees, staff and visitors in immigration detention facilities and the stability of the facility. These devices may be seized from where they are being used by a certain detainee to coordinate and facilitate escape efforts and other criminal activity such as facilitating the movement of other prohibited things; conveying threats to persons within the facility; enabling access to child exploitation or terrorism-related material.

In the event that a communication device is seized from a detainee and the Department is not in a position to return that thing as it continues to pose some risk to the health or safety of others, or the good order of the facility, the Bill expressly requires the Department to ensure the detainee is provided access to alternative means of communication.

The amendments in the Bill will also support the effective management of prescription medications within immigration detention facilities by ensuring that safe and appropriate health care continues to be provided to detainees prescribed these medicines for their individual use, and the ability to respond appropriately to the misuse of prescription medications for unlawful purposes.

The Commonwealth has a duty of care that encompasses taking reasonable steps to avoid reasonably foreseeable risks of harm to people in the facilities. The amendments in the Bill are appropriate and necessary to support the Commonwealth in discharging this duty effectively, providing powers necessary to take reasonable steps to prevent or mitigate risks to the orderly function of the facility itself.

The Minister may determine items as 'prohibited things' by disallowable legislative instrument if:

- possession of the thing is prohibited by law in a place or places in Australia; or
- possession or use of the thing in an immigration detention facility might pose a risk to the health, safety or security of persons in the facility, or to the order of the facility.

The amendments of the Migration Act will make clear that a search power may be exercised or a screening procedure conducted for a thing, whether or not the thing is visible to the authorised officer beforehand, and whether or not the thing has been intentionally concealed. In amending the Act, the Bill also removes references to a thing being 'hidden' on a detainee, or in their clothing or property.

The amendments in this Bill will reduce the Australian Border Force's reliance on State or Federal Police to attend immigration detention facilities and support any searches of a detainee's person and to take custody of any illegal items or substances located within immigration detention facilities. The Bill also provides for the use of trained detector dogs by authorised officers (not assistants) who are conducting searches of immigration detention facilities that are operated by or on behalf of the Commonwealth. Detector dogs cannot be used to search detainees personally or people about to enter an immigration detention facility.

The Migration Act currently includes a number of safeguards regulating the proposed search and seizure and use of force powers. The amendments in the Bill do not change the authorisations currently in place for strip searches, and there are no amendments of the safeguards in sections 252A and 252B of the Migration Act. For example, a strip search of a detainee aged at least 18 will still need to be authorised by the Secretary, the ABF Commissioner, or an SES Band 3 employee in the Department; and if a detainee is under 18 years old (but at least 10) a strip search may only be authorised by a magistrate; and strip searches must not be conducted on detainees under 10 years old.

Strip searches must only be conducted as a matter of last resort and when absolutely necessary. Other existing protections that ensure the dignity of the detainees include that the authorised officer conducting the search must:

- not use greater force, or subject the detainee to greater indignity, than is reasonably necessary to conduct the search or screening procedure; and

- be of the same sex as the detainee being strip searched.

Implementation of the measures will be subject to scrutiny from various bodies with inspection powers, including the Office of the Commonwealth Ombudsman and the Australian Human Rights Commission.

All persons in immigration detention have the right to lodge complaints. Detainees are made aware of their right to complain without hindrance or fear of reprisal and their avenues of complaint and redress, including:

- written complaints addressed to the Department;
- directly with the Department through the Global Feedback Unit or through the Department's website;
- direct communication with external scrutiny agencies such as the Australian Human Rights Commission and the Commonwealth Ombudsman.

1.49 Noting the above, the committee requests the minister's more detailed advice as to why it is considered necessary and appropriate to allow the minister to determine, by legislative instrument, what things are to be prohibited in immigration detention facilities and why is it not appropriate to set these out in primary legislation.

The modern immigration detention population predominantly comprises a high-risk criminal cohort who have had their visas cancelled or refused on character grounds due to their serious criminal histories. An increase in the number of substance-related incidents, regular threats and acts of violence against detainees, staff and contractors, sets the precedent for why such legislation change is required.

The Migration Act currently provides for authorised officers to search for and seize:

- weapons;
- escape aids;
- things capable of being used to inflict injury; and
- evidence which may be relevant to grounds for cancelling a visa.

The Migration Act does not currently allow for the search and seizure of anything else that might pose a risk to the health, safety or security of people in Immigration Detention Facilities, or to the order of those facilities. As such, the amendments in the Bill are necessary to meet both community expectations and the Commonwealth's duty of care obligations, to counter the risks posed by increasingly frequent dangerous, violent and illegal behaviour.

The amendments in the Bill address these risks by empowering the Minister to determine (in a disallowable legislative instrument) that an item is a 'prohibited thing', and provides authorised officers with powers to search for and seize prohibited things.

The amendments will empower the Minister to designate any item that is already prohibited to possess under Australian law (that is, an unlawful thing) as a 'prohibited thing' in relation to persons in detention and in relation to Immigration Detention Facilities. These things would include illicit substances and child exploitation material.

The Minister may also designate other items that are not otherwise prohibited to possess under Australian law (that is, not an unlawful thing), as 'prohibited things' if possession or use of such thing poses an immigration detention facility risk. These types of things may include communication devices, prescription medication in possession of a person to whom it was not prescribed or supplied, and equipment or other items used in the making of alcohol. An immigration detention facility risk means a risk to the health, safety or security of people in an Immigration Detention Facility, or to the order of the facility.

It is appropriate for prohibited things to be determined by legislative instrument rather than set out in primary legislation, as it affords the necessary flexibility to designate new or different things from time to time, informed by intelligence and incident reporting. It would also provide capacity for the Minister from time to time to revise the instrument to, in effect, de-list items determined as prohibited things where they are no longer considered to pose a risk to the health, safety or security of people in an Immigration Detention Facility, or to the order of the facility, to ensure facilities do not operate with and impose unreasonable restrictions on detainees and visitors entering the facilities. Specifying certain things in the primary legislation would not afford the necessary level of responsiveness to address new and emerging risks to the health, safety or security of people in an Immigration Detention Facilities, including detainees and staff.

Providing that the legislative instrument is disallowable (despite the operation of subsection 44(2) of the *Legislation Act 2003* and table item 20 of section 10 of the *Legislation (Exemptions and Other Matters) Regulation 2015*) also ensures that it is appropriately subject to parliamentary scrutiny and oversight.

1.57 Noting the above, the committee requests the minister's more detailed advice as to:

- **why it is considered necessary and appropriate to provide the minister with broad discretionary powers to require an authorised officer to exercise seizure powers; and**
- **why is it appropriate that the minister's determination should not be subject to disallowance.**

The Minister will be empowered to issue binding written directions to authorised officers – in the form of a non-disallowable legislative instrument – requiring officers to seize a thing by exercising one or more of the relevant seizure powers. This new ministerial direction power will allow for the implementation of a targeted, intelligence-led, risk-based approach in relation to the seizure of certain things from detainees in facilities specified in a written direction. The Minister's direction can cover seizure of a prohibited thing, or a thing that is expressly covered by the relevant seizure power – such as weapons, escape aids and visa cancellation

evidence. Such a direction could be based on risk assessment of security or safety concerns prevalent at a specific facility.

The Minister is also able to specify a thing - or a class of things - in the written direction, requiring that thing to be seized. The Minister is not able to give directions that would be inconsistent with the Migration Act or Regulations. Therefore items to be seized in accordance with a direction must be specified in either the Act, Regulations, or in a legislative instrument made under subsection 251A(2).

The direction may require the seizure of a thing in relation to:

- a person in a specified class of persons, or all persons, to whom the relevant seizure power relates
- a specified thing, a thing in a specified class of things, or all things, to which the relevant seizure power relates
- a specified immigration detention facility, an immigration detention facility in a specified class of facilities, or all immigration detention facilities
- any circumstances specified in the direction (for example, a particular period during which the direction is to take effect).

If a direction is provided for a prohibited thing that is not otherwise unlawful to possess (that is, prohibited things determined under paragraphs 251A(2)(b)), that direction is subject to subsection 251AA, that is, its seizure must be for the purpose of preventing or lessening a risk to the health, safety or security of people in an Immigration Detention Facility, or to the order of the facility. Despite any direction given, a thing cannot be seized if the seizure is not authorised under subsection 251AA(3) relating to preventing or lessening immigration detention facility risks.

The direction will not be disallowable, in order to provide appropriate and immediate operational effect and certainty for officers in relation to the status of the Minister's direction. It is expected that this power will only be exercised in relation to the most serious circumstances. As the direction will be a legislative instrument, it must be registered on the Federal Register of Legislation (FRL), which is publicly available. An explanatory statement will accompany the instrument on the FRL, and it will also be tabled in the Parliament.

1.63 The committee therefore requests the minister's advice as to:

- **who it is intended will be authorised as an 'authorised officer' and an 'authorised officer's assistant' to exercise coercive powers and whether these will include non-government employees;**
- **why it is necessary to confer coercive powers on 'other persons' to assist an authorised person and how such persons are to be appointed; and**
- **what specific training and qualifications will be required of persons conferred with these powers, and why the bill does not provide any legislative guidance about the appropriate training and qualifications required of authorised officers and assistants.**

These powers can only be used by authorised officers who may be employees of the

Department or the detention services provider. To be an authorised officer, a person must be authorised in writing by the Minister, the Secretary or the ABF Commissioner. Authorised officers will receive training and guidance on the exercise of relevant seizure powers, as well as how to comply with any direction by the Minister.

Officers authorised to carry out searches of detainees will be required to satisfy training and qualification requirements in the following areas:

- civil rights and liberties;
- cultural awareness;
- the grounds for conducting a strip search;
- the pre-conditions for a strip search;
- the role of officers involved in conducting a strip search;
- the procedures for conducting a strip search;
- the procedures relating to items retained during a strip search.

Officers authorised to use detector dogs for searches will also be required to undergo specific training in relation to handling detector dogs to ensure the dog is prevented (taking all reasonable precautions) from touching any person and is kept under control for the duration of the search. An authorised officer's assistant will not be able to use detector dogs to search an immigration detention facility.

An authorised officer's assistant must follow the directions of the authorised officer, but may exercise any of the powers or functions of the authorised officer. Subsection 252BB provides that an authorised officer may be assisted by other persons in exercising powers or performing functions or duties for the purposes of a search under section 252BA (other than subsection 252BA(4) which provides for authorised officer's power to use a dog to conduct searches) or in relation to seizing and retention of things found in the course of a screening process or search under sections 252C, 252CA and 252CB if that assistance is necessary and reasonable. The assistant must exercise these powers in accordance with any directions given by the authorised officer. By including the wording 'necessary and reasonable' this restricts the use of officers' assistants to situations where such assistance is necessary to ensure the authorised officer can carry out their powers, functions or duties.

Examples of where the use of an assistant may be necessary and reasonable include the search of the whole facility, where numerous officers are necessary in order for the search to be conducted, or where a locksmith is required on a one-off basis to unlock a door within an Immigration Detention Facility in order to facilitate a search of that premises. The Bill does not require that an "authorised officer's assistant" be appointed – they will be deployed as and when assistance is necessary.

THE HON STEPHEN JONES MP

ASSISTANT TREASURER AND MINISTER FOR FINANCIAL SERVICES

Ref: MC24-019845

Senator Dean Smith
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

scrutiny.sen@aph.gov.au

Dear Senator Smith

I am writing in response to the Senate Standing Committee for the Scrutiny of Bill's comments in Scrutiny Digest 14 of 2024 regarding the Scams Prevention Framework Bill 2024.

I have attached detailed responses to the matters raised by the Senate Committee about the Scams Prevention Framework Bill 2024.

I trust that the information attached provides further context about the drafting of the Bill and assists with the Committee's deliberations.

Scams Prevention Framework Bill 2024

Privacy

In the Committee's Scrutiny Digest 14 of 2024, you sought my advice as to whether:

- the power to use or disclose personal information under sections 58BT and 58BV contains sufficient safeguards to appropriately protect the right to privacy;
- the appropriateness and necessity of providing that the Scams Prevention Framework (SPF) regulator need not notify any person (including potential victims of scams) that they have collected, used or disclosed their personal information; and
- the appropriateness of amending the Bill
  - to require that disclosures of SPF information containing personal information pursuant to proposed section 58BV can only be made by the SPF general regulator for specific purposes linked to the achieving the objectives of the SPF framework;
  - to require that all SPF information be de-identified when shared under proposed section 58BV, unless doing so would not achieve the object of the SPF framework;
  - to require regulated entities to de-identify personal information when reporting on actionable intelligence regarding scams, unless to do so would not achieve the object of the SPF framework, and/or requiring the authorised person under proposed section 58BT to specifically consider the need for de-identification; and
  - to provide that notice need not be given under proposed 58EI of the collection, use or disclosure of the personal information of alleged scammers only (enabling scam victims to be notified), and provide all persons to be notified once any investigation is complete.

Powers to use or disclose personal information

The Scams Prevention Framework Bill 2024 (the SPF Bill) establishes a mechanism for information sharing to support regulated entities, SPF regulators and law enforcement to prevent and respond to scams impacting SPF consumers. This mechanism is therefore a key component of the SPF as it is directly aimed at protecting consumers from scams.

As set out below, I consider that the SPF Bill, together with the obligations of the *Privacy Act 1988* (the Privacy Act), contain sufficient safeguards to appropriately protect the right to privacy, taking into account the object of the SPF is to prevent and respond to scams impacting consumers.

Authorised data gateway, website or portal

Subsection 58BT(1) establishes a power for the SPF rules to prescribe a scheme for authorising third parties to operate data gateways, portals or websites that give access to reports that regulated entities are required to give under the Division. This includes reports:

- of actionable scam intelligence (section 58BR);
- about scams upon written request by the regulator (section 58BS); and
- about the outcomes of investigations (section 58BY).

Subsection 58BT(3) provides that an authorised third party may use or disclose any personal information to the extent that it is reasonably necessary to achieve the object of the SPF. This requires the authorised third party to come to a view that the use or disclosure of personal information is needed to prevent and respond to scams impacting SPF consumers. I consider that this is an important safeguard that will ensure personal information is only used and disclosed in this context where necessary.

In addition, the SPF rules may be used to prescribe conditions on any authorisations (paragraph 58BT(2)(c)). This rule-making power may be used to prescribe additional safeguards relating to personal information, including the collection, handling and storage of that information. This has not been provided for in the SPF Bill given the appropriate safeguards will vary depending on the third party that is being authorised. For example, if an authorised third-party would not be subject to the Privacy Act, it would be appropriate to impose similar requirements to that Act as a condition on the relevant third party's authorisation. I note however, this is unlikely and it is expected that all authorised third parties would be subject to the Privacy Act, in which case there are clear requirements and safeguards concerning the handling of personal information.

For example, the Australian Financial Crimes Exchange (AFCX), may be an authorised third party under the SPF rules. The AFCX currently supports information sharing for the purpose of preventing financial and cyber crime and receives reports from participants whose customers have consented to the sharing of the information for the purpose of using the information to fight fraud and scams. As the AFCX is subject to existing privacy regulation, including the Privacy Act, additional safeguards relating to the handling of personal information may not be necessary if the AFCX is authorised under the SPF rules. I will ask my Department to consider this further during the development of the SPF rules.

The SPF rules will also be used to prescribe the kinds of information (including personal information) to be provided in an actionable scam intelligence report and in reports about the outcomes of investigations. Accordingly, the personal information that could be obtained by a third party authorised by the SPF rules will be constrained to any personal information required by the SPF rules to be included in those reports.

The information required for these reports needs to be consulted on and carefully considered in the context of evolving scam activity. Accordingly, it is not appropriate for this detail to be set out in the SPF Bill. However, any personal information would only be prescribed and therefore required to be provided to the extent it is necessary to meet the object of the SPF – that is, any personal information provided would be for the purpose of preventing and responding to scams impacting SPF consumers.

Where an SPF regulator requests personal information to be included in a report about a scam under section 58BS, the personal information must first be de-identified, unless doing so would not achieve the object of the SPF. This requirement further safeguards the right to privacy against the disclosure of this personal information.

SPF general regulator sharing information

Section 58BV enables the SPF general regulator to share information about scams with certain entities. This may include the disclosure of personal information.

Disclosure of personal information under this provision is limited to the entities listed in the provision, rather than to any entity that the SPF general regulator considers appropriate. In my view, this provides an important safeguard to ensure personal information is not shared beyond what is necessary to achieve the object of the SPF.

Under this provision, the SPF general regulator may disclose information about scams to regulated entities, Commonwealth agencies involved in developing Government policy relating to the SPF, Australian law enforcement agencies, foreign law enforcement agencies and foreign regulatory agencies responsible for scam prevention.

Disclosure to these entities is intended to prevent and disrupt scams (noting the transnational nature of scams requires a coordinated international approach to minimise scam harms), or to assist with the development of scam prevention law, with the ultimate view of protecting consumers from scams.

While the disclosure of any personal information by the SPF general regulator is authorised for the purposes of Australian Privacy Principle 6, the Australian entities receiving this information will generally be subject to the Privacy Act obligations and/or equivalent obligations in relation to handling personal information. For example, this will ensure these entities can only use or disclose personal information for the purpose for

which it was collected. This safeguards against the personal information being handled, used or disclosed in a way that is beyond the scope of the disclosure or otherwise contrary to the right to privacy.

Further, any personal information disclosed to a Commonwealth agency or authority involved in developing Government policy relating to the SPF must first be de-identified, in order to protect the right to privacy, unless doing so would not achieve the object of the SPF.

Additional safeguards are included in the SPF Bill with respect to disclosure to an agency of a foreign country, which may not be subject to an equivalent of the Privacy Act. Specifically, the agency is required to give the SPF general regulator an undertaking about controlling the storage, handling and the use of the information to be shared, and the SPF general regulator must consider that it is appropriate in all circumstances to disclose the information. These safeguards are designed to ensure that any information, including personal information, is appropriately handled by an agency of a foreign country.

No obligation to notify any person that an SPF regulator has collected, used or disclosed their personal information

A key aim of the SPF is to prevent and disrupt scam activity before a consumer is impacted. This aim is supported in the SPF framework by enabling prompt and dynamic sharing of information relating to scams. This information may include personal information, and may need to be collected, used and disclosed by an SPF regulator promptly to enable effective disruption activities to protect consumers from scam harms.

In most cases, personal information shared under the reporting requirements in the SPF Bill will relate to the persons perpetrating the scam or otherwise involved in the scam. This information may include a phone number a scammer is using to contact consumers, information about a social media account being used to create fraudulent advertisements or otherwise deceive consumers, or information about a bank account used to receive scam funds.

It would not be appropriate in these cases to require an SPF regulator to notify individuals that they have collected, used, or disclosed their personal information, as this will tip-off the person perpetrating the scam, help them evade anti-scam measures and may prejudice a criminal investigation.

In the limited circumstances where an SPF regulator collects, uses, or discloses the personal information of a scam victim (or potential scam victim), it would be impractical for the SPF regulator to contact each of these individuals to notify them of such. To the extent the SPF regulator obtains this type of personal information, this is likely to be unsolicited information given by the regulated entity in purported compliance with the reporting requirements. As such, the SPF regulator is unlikely to have sufficient information about the person to contact them about the collection of their information.

This provision does not prevent regulated entities or SPF regulators from providing notifications to consumers of the use of their personal information where it is appropriate to do so.

Regulated entities under the SPF are also expected to be subject to the Privacy Act. This means that regulated entities must notify customers of their policies regarding collection, use and disclosure of personal information, which will need to be updated to incorporate the SPF obligations. This may involve the secondary purposes for which the regulated entity may use a customer's personal information, which may relate to reporting requirements under the SPF.

There are other mechanisms in the SPF Bill where it may be reasonable in the circumstances for a regulated entity to notify or warn a consumer that they may have been impacted by suspected scam activity. For example, section 58BO requires regulated entities to identify impacted SPF consumers and section 58BX requires a regulated entity to take reasonable steps to disrupt scam activity. These provisions provide a mechanism for regulated entities to consider notifying SPF consumers that they may be exposed to scam activity, and that their information, where relevant, has been disclosed to an SPF regulator and the purpose of that disclosure.

Advice on whether it would be appropriate to amend the Bill

Disclosures of SPF information containing personal information pursuant to proposed section 58BV

I consider the existing settings under section 58BV are appropriate to enable information about scam activity to be shared in real-time and to effectively support disruptive action to combat scams, while balancing the need to protect privacy. Information sharing by the SPF general regulator to the entities listed in section 58BV is critical to minimise scam activity across the economy.

The proposed amendment suggested by the Committee would require the SPF general regulator to assess whether the information is sufficiently connected to the purpose before sharing in every circumstance.

I am concerned that this would frustrate the objects of the SPF, as it would preclude the SPF general regulator from setting up intelligence sharing systems to ensure that information about suspected scam activity flows to relevant entities in real-time to support their response to the scam. If the SPF general regulator is required to assess each piece of information before sharing it with a specified entity, by the time the information is received by the relevant entity it may be too late to effectively disrupt the action and protect consumers.

In my view, the existing settings in section 58BV provide appropriate privacy protections in this context, which are broadly consistent with the objects of the SPF.

- Subsection 58BV(1) limits the information that can be shared to information about a scam. This broadly ensures the information is necessary to support the objects of the SPF and enables entities to take disruptive action to combat scam activity.
- Subsection 58BV(2) only allows for the sharing of information to a limited and defined set of entities. This is constrained to regulated entities and relevant Government bodies that are in a position to take action against scams.
- Subsection 58BV(3) limits sharing with international counterparts, requiring that they give an undertaking about the storage, handling and use of that information and ensuring that the information will only be used for the purpose for which it was disclosed. The SPF general regulator is further constrained by only being able to share information if it considers that it is appropriate to do so.
- Subsection 58BV(4) requires that any disclosure to a Commonwealth agency or authority involved in developing Government policy relating to the SPF must only contain de-identified personal information, unless doing so would not achieve the object of this Part.

These safeguards seek to balance the need to protect personal information, while recognising that it is in the public interest to support a coordinated whole-of-economy response to address scams.

De-identification of SPF information

I consider the existing settings are appropriate, noting the importance of timely sharing of information to disrupt scam activity to support the object of the SPF.

As above, the requirement to de-identify information unless doing so would not achieve the object of the SPF will require the SPF general regulator to make an assessment before disclosing information in every circumstance. This requirement would preclude the SPF general regulator from setting up automated intelligence sharing systems and more broadly delay the disclosure of time-sensitive information with relevant entities.

Where entities are unlikely to need personal information or information in real-time, the SPF protects against arbitrary interference with privacy by including requirements to de-identify personal information prior to the disclosure, unless doing so would not achieve the object of the SPF.

This includes subsection 58BV(4), which requires the SPF general regulator to de-identify personal information where it would not frustrate the object of the SPF before it is shared with Commonwealth agencies or authorities involved in development Government policy relating to scams. This recognises that this type of entity is not likely to need personal information, or information in real-time to support the object of the SPF.

In other cases, such as when sharing with law enforcement agencies or regulated entities, it is expected that any necessary personal information will need to be shared quickly to enable the receiving entity to use the information to take effective disruptive action to prevent consumer loss. The intent and purpose for this power is to facilitate the efficient sharing of any available information about the person responsible for perpetrating or involved in the scam. This information may include the bank, social media, or telephone account used by the scammer to perpetrate scam activity so that the entity receiving the information can take steps to block access to those mechanisms. It will also enable law enforcement agencies to take appropriate action against the scammer.

Where relevant, entities receiving this personal information will need to comply with their obligations under the Privacy Act in relation to that personal information.

Accordingly, I consider that an obligation on the SPF general regulator to de-identify all personal information before disclosing it under 58BV would significantly limit the effectiveness of the provision in supporting the prevention and disruption of scams.

<u>De-identification of personal information when reporting actionable intelligence scams</u>

I consider the existing settings are appropriate noting how fundamental the timely sharing of scams-related information is to support the object of the SPF.

As with the suggested amendments above, the requirement for regulated entities to de-identify information unless doing so would not achieve the object of the SPF, or requiring an authorised person under section 58BT to consider the need for de-identification, would require the entity to make an assessment before disclosing actionable scam intelligence in every circumstance. This requirement could preclude regulated entities from promptly disclosing time-sensitive intelligence which could subsequently be used by an SPF regulator or another regulated entity to prevent and disrupt scams.

To the extent that a regulated entity is required to share personal information when reporting on actionable scam intelligence, this will be limited by what is prescribed by the SPF rules. As set out above, this is expected to be information that is necessary to prevent and disrupt scam activity.

Section 58BT enables authorised third parties to facilitate information-sharing on behalf of regulated entities to assist them to comply with their reporting obligations. This recognises the benefit of leveraging established intelligence sharing networks that exist to combat scam activity, such as the AFCX. This will support the information sharing scheme established by the SPF and facilitates the flow of information for the same purpose – to support effective and timely disruptive action.

On this basis, it is not necessary or appropriate to require the authorised third party to further consider whether personal information should be de-identified. This requirement would slow the movement of information, frustrate the object of the SPF and risk further consumer loss.

<u>Notification once investigation is complete</u>

I consider the existing settings appropriate, noting the nature of information that will be collected and shared and the practicality of contacting and notifying impacted persons.

As outlined above, introducing a requirement to notify persons on each occasion that their personal information is collected, used or disclosed by an SPF regulator is likely to delay the disclosure of time-sensitive information, may divert resources from the objectives of the SPF, and may result in tipping off a suspected scammer.

As the Committee understands, in most cases personal information being shared under the reporting obligations in the SPF Bill will be information about the person perpetrating the scam activity. As such, section 58EI provides a necessary carve out from the general procedural fairness obligation to notify a person about the collection, use or disclosure of personal information.

There are practical challenges associated with requiring SPF regulators to notify scam victims in the limited circumstances in which it is expected that their personal information will be collected, used or disclosed.

The Committee notes that the SPF Bill could be drafted to prevent notice of collection, use or disclosure only to the alleged scammer. I consider that this would risk tipping off scammers as notifications to scam victims may inadvertently or otherwise tip-off scammers with which they are engaged in communication. This is heightened by the reality that scammers are generally highly skilled at manipulating scam victims to provide them with sensitive information. Furthermore, it may not always be clear to SPF regulators whether account information relates to a scam victim or alleged scammer, noting scammers often have several bank, telecommunication and social media accounts to support their scam activities.

In addition, the SPF Bill seeks to limit the personal information collected and shared to the information that is actionable, being that information which is necessary to be shared to support disruptive action. This means that the SPF general regulator is unlikely to have sufficient information to be able to identify and contact individual consumers to notify them that their information has been shared. In addition, introducing this requirement would impose significant burden on regulators, is likely to be challenging to implement, and may divert resources and focus from the objectives of this legislation. It is also likely that additional personal information would need to be shared with the regulator to enable this notification to effectively take place.

As an additional safeguard, SPF regulators may decide that it is appropriate to notify consumers of the collection and use of their personal information.

I also consider that a regulated entity who has directly received this information from a consumer or may have a direct customer relationship with the consumer may be more appropriately placed to provide this notification to a consumer. Under the SPF Bill, a regulated entity is required to take various steps on receipt of actionable scam intelligence. Section 58BO requires regulated entities to identify impacted SPF consumers, and section 58BX requires a regulated entity to take reasonable steps to disrupt activities that is the subject of actionable scam intelligence. These provisions provide a mechanism for regulated entities to consider notifying SPF consumers that their information, where relevant, has been disclosed to an SPF regulator and the purpose of that disclosure

Incorporation of external materials as existing from time to time

You also sought my advice as to:

- the type of documents that it is envisaged may be applied, adopted or incorporated by reference under proposed subsection 58CC(4);

- whether documents applied, adopted or incorporated by reference under proposed subsection 58CC(4) will be made freely available to all persons interested in the law; and

- why it is necessary to apply the documents as in force or existing from time to time, rather than when the instrument is first made.

The Bill allows for an SPF code to make provision in relation to a matter by applying, adopting or incorporating any matter contained in any other instrument or writing as in force or existing at a particular time, or from time to time.

An SPF code may apply, adopt or incorporate by reference, material contained in State or Territory legislation, instruments made by an SPF regulator, or materials published on the SPF regulators websites.

For example, an SPF code may reference existing standards of practice, such as those found on the Australian Communications and Media Authority's (ACMA's) register of telco industry codes and standards.[1] These standards are technical in nature and sit appropriately on the ACMA register given they may be made by, or in conjunction with, industry stakeholders in the telecommunications sector.

Where an SPF code applies, adopts or incorporates by reference, material from another instrument or in writing, the location of where a person may access it will be clear in the SPF code or explanatory materials.

Where the relevant material is in State or Territory legislation or instruments made an SPF regulator, there will be no charge for access, in accordance with existing practice and publication policies of these entities. This will also be the case for any publicly available standards, codes or guidance material that may be incorporated by reference.

There may be exceptional circumstances where it is necessary for an SPF code to refer to material such as an industry standard that may require a fee for access. If this is necessary, I consider that the costs to affected entities in accessing the material would substantially outweigh the costs they may incur by needing to comply with a new bespoke standard. In addition, it is likely the affected entities may also already have access to that document from the normal course of their business.

Given the wide range of industries and sectors of the economy to which the SPF can apply and the fluid nature of scam activity, the ability to incorporate extrinsic material from time to time is necessary and appropriate to achieve the object of the SPF.

As scam activity evolves, material that has been incorporated by reference may be updated to reflect the necessary change in regulatory settings.

If those materials are updated from time to time but have been incorporated when the material is first made only, any delays in amending the relevant SPF code to reflect the updated material would risk the regulatory obligations not being fit for purpose.

Privacy and procedural fairness – public warning notices

You also sought my advice as to:

- the appropriateness of proposed section 58FZL enabling the SPF general regulator to issue public warning notices, with consideration provided to the impacts of such a notice on both procedural fairness and individual privacy, and how procedural fairness will be provided in practice to a person likely to be affected by a public warning notice;

- whether SPF regulators will be required to take down, within a reasonable time, any public warning notices that were issued but which, upon review, are incorrect; and

- what type of matters may lead the regulator to reasonably suspect conduct may constitute a contravention of the SPF framework; and whether consideration was given to applying a higher threshold to the issuing of a public warning notice, or, if not, why not.

The SPF Bill allows the SPF regulators to issue a public notice about the conduct of a person if the regulator:

- reasonably suspects that the person's conduct may constitute a contravention of the SPF principles or code;

- is satisfied that one or more persons has suffered, or is likely to suffer, detriment as a result of the conduct; and

- is satisfied that it is in the public interest to issue the notice.

[1] Register of telco industry codes and standards | ACMA

Given the obligations under the SPF apply to regulated entities only (which is expected to include banks, telecommunications providers and certain digital platforms), any public notice that is issued under the SPF is likely to relate to an entity rather than a natural person.

These notices will be an important and necessary enforcement tool for the SPF regulators to efficiently notify affected consumers directly affected by the relevant conduct, and alert consumers and/or small businesses to the alleged conduct more broadly.

This enforcement tool does not seek to limit the fundamental common law right of procedural fairness, nor does it seek to negatively impact individual privacy. Instead, the tool is intended to support individual privacy as it will be used to prevent and disrupt scam activity, which may otherwise involve the loss of personal information to a scammer.

In determining whether it is in public interest to issue the notice, an SPF regulator is likely to key consider whether there is an imminent need to inform consumers so they can avoid suffering detriment, as well as the likely impact on the business involved in the suspected contravention.

Consistent with existing approaches by SPF regulators such as the Australian Competition and Consumer Commission (with respect to its existing public warning notices), it is likely that the SPF regulator will alert a regulated entity to an investigation that has commenced with respect to the entity and the proposal to issue a public warning notice. Where appropriate, the SPF regulator is expected to invite a response from the entity on the allegations, including the steps it has taken or proposed to be taken to address the alleged conduct.

There may be circumstances when there have been substantial scam losses in a short period of time and it is therefore critical for an SPF regulator issue a public warning notice quickly to warn consumers. In these cases, timely or limited engagement with the regulated entity may be appropriate.

It is therefore not appropriate that a process for consultation or engagement, including timeframes, with the relevant entity be required in the SPF Bill. Instead, this should be dealt with as matter of policy for the SPF regulator, taking into account the sector it is regulating.

I consider that the conditions that must be met prior to an SPF regulator issuing a public warning notice and the benefit to consumers that a warning notice may provide, are appropriately balanced with the need to afford procedural fairness to an entity suspect of contravening a requirement under the SPF Bill.

For completeness, I note this provision is based on various existing regulatory powers, for example section 51ADA of the *Competition and Consumer Act 2010* (the CCA), section 223 of Schedule 2 to the CCA (the Australian Consumer Law) and section 12GLC of the *ASIC Act*.

<u>Take down of notices</u>

There is no requirement in the SPF Bill that an SPF regulator must take down a public warning notice from their website that is later found to be incorrect.

A public warning notice can only be issued when an SPF regulator has reasonable grounds to suspect that certain conduct has constituted or may constitute a contravention of the SPF, and where that regulator is satisfied of the other matters set out in section 58FZL. The requirements are designed to ensure a public warning is issued based on reasonable information available to the SPF regulator at that time.

This is intended to minimise the risk of any incorrect information being provided to the public in the public warning notice.

There is also an informal mechanism for a regulated entity that has identified any incorrect information in a public warning notice to notify the relevant SPF regulator. This may result in the correction of that notice or revocation of the notice where appropriate. The SPF Bill does not preclude this from occurring.

In addition, issuing a public warning notice is an administrative decision that is subject to judicial review under the *Administrative Decisions (Judicial Review) Act 1977*. This provides a mechanism for a person

aggrieved by the decision to seek judicial review of the decision, and includes an obligation on the decision-maker to provide reasons for the decision.

Accordingly, I consider that the existing settings in the SPF Bill are appropriate.

Conduct that may constitute a contravention of the SPF

The power in section 58FZL to issue a public warning notice can only be exercised if the SPF regulator is satisfied of each of the conditions, which I have described above.

I consider that the provision is framed appropriately as it does not unnecessarily constrain, via an exhaustive list, the type of matters that may lead an SPF regulator to reasonably suspect that conduct may constitute a contravention of the SPF framework.

This reflects the principles-based nature of the SPF obligations and the fluid nature of the scam activity that leads to the consumer harm that this framework seeks to mitigate. For example, it allows an SPF regulator to consider the evolving nature of scam activity in a particular sector as that impacts on what may be a 'reasonable step' for the purpose of an SPF principle.

I also consider that the threshold for an SPF regulator to issue a public warning notice is set at an appropriate level. A higher threshold, such as the requirement to reasonably believe conduct may constitute a contravention of the SPF framework, would likely require an SPF regulator to undertake a longer investigation and make additional inquiries – even if the conduct has led to consumer detriment and there is a clear public interest in issuing the public notice.

In my view, a higher threshold would significantly limit the effectiveness of this enforcement tool in notifying consumers at large about certain conduct by a person that is potentially harmful conduct. In the scams context, the earlier this notification can occur, the more likely it is that the risk of scams harm to the community is minimised.

Significant matters in delegated legislation

The Committee drew to the attention of the senators whether it is appropriate to leave matters integral to the operation of the scheme to delegated legislation, and requested an addendum to the explanatory memorandum, containing a justification for the inclusion of codes of conduct in delegated legislation, be tabled in the Parliament as soon as practicable.

Thank you for drawing this to my attention. I am proposing to make an amendment to the explanatory memorandum, which will contain further justification for the inclusion of SPF codes in delegated legislation. This will be tabled in Parliament as soon as practicable.

No-invalidity clause

You also drew to the attention of the senators whether it is appropriate for the SPF Bill to provide, in subsections 58AE(2) and 58DB(2), that instruments will remain valid regardless of whether the minister met specified requirements in making the instrument. You requested an addendum to the explanatory memorandum, containing a justification for the no-invalidity clause in proposed subsection 58DB, be tabled in the Parliament as soon as practicable.

Thank you for drawing this to my attention. I am proposing to make an amendment to the explanatory memorandum, which will contain further justification for the inclusion of the no-invalidity clause in proposed 58DB. This will be tabled in Parliament as soon as practicable.

THE HON DR ANDREW LEIGH MP
ASSISTANT MINISTER FOR COMPETITION, CHARITIES AND TREASURY
ASSISTANT MINISTER FOR EMPLOYMENT

Ref: MC24-019850

Senator Dean Smith
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

scrutiny.sen@aph.gov.au

Dear Senator Smith

Thank you for your correspondence of 21 November 2024 originally directed to the Treasurer, concerning the Treasury Laws Amendment (Mergers and Acquisitions Reform) Bill 2024. Your correspondence has been referred to me as the matter falls within my portfolio responsibilities.

I have attached a detailed response to the matters raised by the Senate Committee for the Scrutiny of Bills in the Committee's *Scrutiny Digest 14 of 2024*.

I trust that the information attached provides further context about the drafting of the Bill and assists with the Committee's deliberations.

Thank you again for your letter.

Andrew Leigh

W: andrewleigh.com | E: andrew.leigh@treasury.gov.au | P: +61 2 6277 4140
Parliament House Canberra ACT 2600 Australia

Treasury Laws Amendment (Mergers and Acquisitions Reform) Bill 2024

Exemption from disallowance

In the Committee's Scrutiny Digest 14 of 2024, you requested an addendum to the explanatory memorandum, containing a justification for exemptions from parliamentary disallowance, be tabled in the Parliament as soon as practicable.

As I consider that the explanatory memorandum adequately explains the justification for these exemptions from disallowance, I do not propose to table an addendum to it.

As stated in the Explanatory Memorandum at paragraph 3.17 (in relation to notifications) and paragraph 5.12 (in relation to public benefit applications), and explained further below, the exemption from disallowance in relation to the Minister's determination of the forms and the information or documents that must accompany the notification or public benefit application is appropriate, as it is important to provide commercial certainty to merger parties.

The new system in relation to notifications will operate in all States and Territories of Australia through the Competition Code. If the notifications were subject to disallowance, this may also create uncertainty for the States and Territories about the application of the Competition Code under State and Territory law.

A key objective of the reform is to provide certainty to merger parties about their obligations in relation to merger control, including the obligation provide the Commission with sufficient information about a merger so that it can properly undertake its review, and efficiently and expeditiously differentiate benign mergers from those that are potentially anti-competitive. Proportionate upfront information requirements will ensure merger parties provide relevant information to the Commission and mitigate the need for subsequent requests and possible delay. The forms and requirements for any accompanying information or documents for notifications and public benefit applications are therefore critical to ensuring the Commission is able to acquit its functions and duties under the new system, namely to scrutinise, and where necessary, prevent, potentially anti-competitive mergers.

The exemption from disallowance for these instruments is appropriate on the basis that disallowance would undermine commercial certainty. As noted above, it is important, particularly for time-critical transactions, to provide commercial certainty to merger parties in relation to compliance with the forms and requirements for accompanying documents, by ensuring that there is no risk that the instruments containing those requirements will be disallowed. Setting notification and application requirements in subordinate legislation facilitates their update from time to time, and the exemption from disallowance will minimise potential disruption to the ACCC's function of considering notifications and applications, and the time, cost and effort for businesses to prepare.

Further, the instruments are part of an intergovernmental scheme, namely the Competition Code and the 1995 Intergovernmental Conduct Code Agreement. As the new system will operate in all states and territories of Australia via the Competition Code, the details of the system are the product of negotiations with the states and territories as part of the 1995 Intergovernmental Conduct Code Agreement. As a result, disallowance may also create uncertainty for the states and territories about the application of the Competition Code under state and territory law.

Abrogation of privilege against self-incrimination

You also sought my advice as to the appropriateness of:

- abrogating the privilege against self-incrimination when requiring a person to give or produce information, documents or evidence relating to the making of an acquisition determination; and
- not providing for a derivative use immunity in this context.

Schedule 1 to the Bill extends the Commission's power to obtain information, documents and evidence in section 155 of the *Competition and Consumer Act 2010* (the CCA) to cover matters relevant to the making of an acquisition determination by the Commission. In essence, this extension of the Commission's existing information gathering powers is an amendment consequential to merger reform. It does not alter existing settings under section 155, including in relation to the privilege against self-incrimination and constraint on the use of incriminating evidence, which are consistent with the general approach to the Commission's information gathering powers, as explained below with reference to the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide).

Section 155 notices have been a longstanding element of Australia's competition law. The power to compel the production of evidence, information and documents is crucial to the Commission's administration and enforcement of the Act.

The extension of the section 155 power to matters relevant to the making of an acquisition determination by the Commission reflects the fact that the Commission is the first-instance administrative decision-maker under the new system. The amendments in Schedule 1 do not alter the existing removal of the privilege against self-incrimination and constraint on the use of incriminating evidence, except to the extent that section 155 notices may now be issued in relation to certain additional matters (i.e. to support acquisitions determinations under the new merger control system).

Existing subsection 155(7) provides that a person is not excused from producing information, documents or evidence on the basis that such material would tend to incriminate that person or expose that person to a penalty. The removal of the privilege against self-incrimination when required to provide information to the Commission has been a feature of Australia's competition and consumer law since 1974.

The information, documents or evidence obtained using the powers cannot be used as evidence against the individual in criminal proceedings or in proceedings where the person may be liable to a criminal penalty unless those proceedings are for an offence under section 155 or for an offence against certain sections of the *Criminal Code* relating to section 155. Subsection 155(7) ensures that self-incriminating material cannot be used against that person in any criminal proceedings other than proceedings for an offence relating to section 155. This is known as a use immunity. The use of any self-incriminatory material produced in response to a section 155 notice is therefore restricted to investigation of conduct by that person and third parties.

The Guide provides that 'the privilege against self-incrimination may be overridden by legislation where there is clear justification for doing so' and 'if the privilege against self-incrimination is overridden, the use of incriminating evidence should be constrained' (Section 9.5.3-4 of the Guide refers).

The Guide indicates that legislation that removes the privilege against self-incrimination and provides a use immunity provision, as in this case, has been accepted by the Scrutiny of Bills Committee for legislation governing the Commission. Section 9.5.5 (pages 89-90) of the Guide indicates that limited use immunities have been accepted for legislation governing the Commission (who regulates the activities of bodies corporate) due to the particular difficulties of corporate regulation and that a derivative use immunity would unacceptably fetter the investigation and prosecution of corporate misconduct offences.

As explained in the Explanatory Memorandum, through the existing use immunity, the extension of section 155 to matters relevant to the making of an acquisition determination in the Bill balances the Commission's need to access information with a natural person's right against self-incrimination by limiting the use of incriminating material supplied by the individual (see paragraph 9.27). The justification for the extension of the removal of the privilege against self-incrimination is because the public benefit in removing the right outweighs the loss to the individual (see paragraph 9.28). The information which would be obtained by the Commission is critical in it performing its regulatory functions, specifically seeking to enforce the obligation to notify and suspend certain transactions subject to Commission review, and ultimately prevent anti-competitive acquisitions that would substantially reduce competition. The material and evidence necessary for the Commission to perform its regulatory function is likely to only be available from certain individuals in an entity (see paragraph 9.29).

It is not proposed to alter existing settings to make provision for a derivative use immunity to prevent any incriminating evidence being used to gather other evidence against the person. Such a change, if it were to apply to section 155 generally, would have broad implications for the Commission's use of its powers under that provision that would extend far beyond matters relevant to making of acquisition determinations. Such a change would be inconsistent with the approach that has been previously accepted by the Committee in relation to legislation governing the Commission in view of the particular difficulties of corporate regulation.

The approach in the Bill to remove the privilege against self-incrimination, make no provision for derivative use immunity and only provide for use immunity is also consistent with the approach in the *Competition and Consumer Amendment (Competition Policy Review) Act 2017* for the extension of the Commission's power to obtain information, documents and evidence in section 155 to cover merger authorisation determinations under the existing merger framework that the Bill is replacing.

The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Multicultural Affairs
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MC24-034940

Senator Dean Smith
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Chair Dean

I write in response to the correspondence received from the Secretary of the Senate Standing Committee for the Scrutiny of Bills, Ms Anita Coles, on 28 November 2024, concerning the Committee's consideration of the recently agreed amendments to the Security of Critical Infrastructure and Other Legislative Amendments (Enhanced Response and prevention) Bill 2024.

I appreciate the time the Committee has taken to consider these amendments and the Bill. My response to the matters raised by the Committee in its Scrutiny Digest 15 of 2024 is provided at Attachment A.

Thank you for raising these matters, and I trust this information is of assistance to the Committee in its further consideration of the amendments.

I have also copied this response to the Attorney-General, the Hon Mark Dreyfus KC, MP, as it also relates to legislation in the Attorney-General's Portfolio.

Yours sincerely

TONY BURKE

13 / 1 / 2025

Attachment A

SENATE STANDING COMMITTEE FOR THE SCRUTINY OF BILLS

Scrutiny Digest 15 of 2024

Cyber Security Bill 2024

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

The Senate Standing Committee for the Scrutiny of Bills (**the Committee**) has requested advice from the Minister for Home Affairs and Minister for Cyber Security in relation to amendments of the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (**the ERP Bill**) that were moved and agreed in the House of Representatives on 19 November 2024. The Committee's initial scrutiny of the amendments is set out in the Committee's *Scrutiny Digest 15 of 2024* (pp. 33-35).

The Committee requests the Minister's advice as to the necessity of removing section 38A from the ASIO Act, in particular why the amendment has become necessary now (noting section 38A was introduced as a safeguard 20 years ago).

In 2018, section 38A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) was amended by the *Home Affairs and Integrity Agencies Legislation Amendment Act 2018*. Since that time, it has been the case that where the Minister responsible for the exercise of the powers listed in section 38A is not also the Minister administering the ASIO Act, section 38A has not been operable, and section 38 was the applicable section. Repealing section 38A therefore clarifies the operation of section 38 and mitigates risks associated with any prior notice or certificate given under section 38 in relation to the powers listed in section 38A.

The Committee requests the Minister's advice as to:

- why the power of the Minister to exclude a matter if it would be prejudicial to the interests of security from the information given to an affected person is insufficient to protect national security risks; and

- how the right to seek review of administrative decisions will be afforded to a person if they are never notified that an adverse ASIO assessment was made against them.

In response to the Committee's comments regarding withholding of notice, the powers referred to in section 38A relate to a range of applications made by persons under the *Telecommunications Act 1997*, or directions made by the Minister administering *the Security of Critical Infrastructure Act 2018* (the SOCI Act Minister).

The operation of these provisions is such that the applicant or person being issued the direction by the SOCI Act Minister would either receive notice the matter is under government consideration, or be issued a direction.

It would not be open to the ASIO Minister to issue a certificate to withhold notice under section 38(2)(a), on the basis that withholding notice is essential to the security of the nation, where the subject has been informed the relevant decision is under government consideration or consideration is being given to issuing a direction. In relation to the powers listed in section 38A, section 38 would therefore only allow the ASIO Minister to exclude certain matters from a security assessment pursuant to a paragraph 38(2)(b) certificate. In this way, section 38 affords the subject of a security assessment the same notification and review rights as under section 38A.