The Hon Stuart Robert MP
Minister for the National Disability Insurance Scheme
Minister for Government Services

Ref: MS21-000250

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Senator Polley

I write in response to the request of the Senate Scrutiny of Bills Committee in Scrutiny Digest 3 of 2021 for further advice on the Data Availability and Transparency Bill 2020 (the Bill).

I have approved an Addendum to the Explanatory Memorandum to address concerns raised by the Committee and I will arrange for that Addendum to be tabled in the House of Representatives as soon as practicable.

I have provided additional information below in relation to specific issues raised by the Committee.

2.19, 2.20 of Scrutiny Digest 3, 2021. Privacy; significant matters in delegated legislation

The Addendum includes further information about the meaning of the expression 'unreasonable or impracticable' in the context of clause 16(2)(c) of the Bill. The Addendum provides information on where to locate guidance issued by the Australian Information Commissioner (AIC) on privacy and consent matters.

The Committee has requested my advice on why it is necessary and appropriate for guidelines on aspects of the data sharing scheme to have the status of non-legislative instruments that are not subject to parliamentary scrutiny.

The Bill establishes a framework of resources, of scaled legal weight, to assist its interpretation and application. These resources range from fact sheets, guidelines on aspects

of the Bill which entities must have regard to when engaging with the sharing scheme, to legislative instruments subject to Parliamentary scrutiny that set binding legal requirements.

I consider this scaled approach to be reasonable, and necessary to achieve the desired outcome of supporting both best practice data sharing and a graduated approach to enforcing compliance with the Bill. This approach is consistent with that of other principles-based legislative schemes, in particular the AIC's powers and framework of instruments to support understanding of, and compliance with, privacy law. It is also supported by findings from a review of the *Public Interest Disclosure Act 2013*, which found a principles-based, graduated approach to regulation to be well adapted to achieving cultural change in data handling, and to driving fair and outcomes-focussed conversations between regulators and decision makers.[1]

I understand from the AIC's experience that it is desirable from a regulatory perspective to have guidelines which entities must regard as an interim step between general guidance and legislative instruments.[2] Learning from this experience, the approach taken in the Bill enables the National Data Commissioner to produce both informal guidance material, and more formal "guidelines". Scheme entities must have regard for the guidelines however they are not binding. The guidelines do not alter the law but provide clear guidance from the Commissioner about their view of law applied and better practice. It is not appropriate for such guidance to be disallowable. Data codes made by the Commissioner, and rules made by the Minister, are binding on scheme entities and are legislative instruments subject to disallowance.

2.23 of Scrutiny Digest 3, 2021. Privacy; Appropriateness of not including an explicit requirement that, where possible, the sharing of data is done in a way that does not allow an individual to be identified

I note that the Data Principle, described in clauses 16(7) and (8) of the Bill, explicitly requires that sharing of personal information is to be minimised, and ensures only data that is reasonably necessary for an authorised project is shared. This approach promotes a culture of safe sharing, in which sharing is done in a way that does not identify people where possible, while maintaining technically-neutral drafting.

2.26 of Scrutiny Digest 3, 2021. Privacy; Appropriateness of not requiring minimum standards for ethics approvals for private entities seeking to use data that includes personal information where no ethics processes would ordinarily apply

The Addendum clarifies that the ethical frameworks identified in the Explanatory Memorandum applies to all human research projects, including potential projects within the data sharing scheme. The Addendum clarifies that data custodians will be able to consider or require ethics processes to be covered in data sharing agreements in circumstances where no ethics processes would ordinarily apply.

---

[1] Independent review conducted by Mr Phillip Moss AM (15 July 2016), part 3 [94-95]: Review of the Public Interest Disclosure Act 2013.

[2] See recommendation 16 of the Submission by the Office of the Australian Information Commissioner on the Privacy Act Review – Issues Paper, 11 Dec 2020.

2.33 of Scrutiny Digest 3, 2021. Privacy; appropriateness of complaints mechanisms available to individuals, including visibility of privacy complaints about the data sharing scheme to the National Data Commissioner

The Addendum will note the expectation that Commonwealth regulators, including the AIC, will work cooperatively with the National Data Commissioner in relation to matters of common interest. This would include the AIC providing information to the National Data Commissioner about privacy issues and complaints that are relevant to the sharing of public sector data under the Bill.

2.39, 2.40, 2.41 of Scrutiny Digest 3, 2021. Accreditation; significant matters in delegated legislation

The Addendum includes additional information about the content of the rules to be made in relation to accreditation.

2.48 of Scrutiny Digest 3, 2021. Broad delegation of investigatory powers

The approach taken in the Bill in relation to monitoring and investigation powers aligns with the standard framing of regulatory powers and authorisations set out in the *Regulatory Powers (Standard Provisions) Act 2014*, and with the Office of Parliamentary Counsel's *Drafting Direction No. 3.5A*.

2.53, 2.54 of Scrutiny Digest 3, 2021. Reversal of evidential burden of proof

The Addendum includes the information I have previously provided to the Committee about the rationale for the reversal of the evidential burden of proof.

I thank the Committee for raising concerns about the Bill to my attention.

Yours sincerely

Stuart Robert

The Hon Christian Porter MP
Attorney-General
Minister for Industrial Relations
Leader of the House

25 FEB 2021

MS21-000110

Senator Helen Polley
Chair, Senate Standing Committee for the Scrutiny of Bills
Parliament House
Canberra ACT 2600
scrutiny.sen@aph.gov.au

Dear ~~Chair~~ Hel

I refer to a letter to my office of 4 February 2021 from the Secretary of the Senate Scrutiny of Bills Committee (the Committee) drawing my attention to the Committee's request for advice in its *Scrutiny Digest 2 of 2021* about certain provisions of the Fair Work Amendment (Supporting Australia's Jobs and Economic Recovery) Bill 2020 (the Bill).

My advice in response to issues raised by the Committee is set out below.

Delegated legislation

The Committee seeks advice about why it is appropriate for certain matters to be prescribed by delegated rather than primary legislation.

Model National Employment Standards (NES) interaction term

I note that existing substantive provisions governing the interaction of the NES and enterprise agreements are contained (relevantly) at sections 55, 56 and 61 of the *Fair Work Act 2009* (the Act). The proposed model NES interaction term, which proposed subsection 205A(3) requires the Fair Work Regulations 2009 (the Regulations) to prescribe, would be declaratory of these provisions and explain their effect. The model term cannot modify the effect of the Act's substantive provisions. In this context, it is appropriate for the term to be prescribed by the Regulations, consistent with existing arrangements for model dispute settlement and consultation terms.

Casual Employment Information Statement

The Committee observes that significant matters should be included in primary legislation rather than in legislative instruments. In this context, I note that key requirements for the content of the Casual Employment Information Statement (the Statement) and employers' obligation to provide it to new casual employees, would be stipulated in the Act. Matters the Statement must contain are set out in proposed subsection 125A(2), including the meaning of 'casual employee', when an employer's offer for casual conversion must be made, circumstances in which an offer for casual conversion need not be made, and the FWC's ability to deal with disputes. The regulation-making power in proposed new subsection 125A(4) is supplementary to these legislative requirements and is consistent with existing arrangements for the Fair Work Information Statement in subsection 124(4). The regulation power only ensures that content, form and provision requirements can quickly be supplemented (but not diminished), should this be necessary in future. The content of the Fair Work Information Statement is similarly specified in the Act supplemented by the regulation power to encompass additional matters.

Treatment of additional agreed hours

The Bill would amend the Act to enable an employer and part-time employee to make an additional hours agreement where an identified modern award applies. Such agreements can provide for an employer to offer, and for a part-time employee to accept or reject, additional hours at ordinary rates of pay in certain circumstances. Under proposed subsection 168Q(2), additional agreed hours generally do not attract overtime payments.

An employee's ordinary hours of work are important for the calculation of various minimum entitlements. Proposed subsection 168Q(4) ensures that an employee's additional agreed hours are treated as ordinary hours of work for the purposes of applicable penalty rates, minimum paid leave entitlements under the NES, and the definition of ordinary time earnings in subsection 6(1) of the *Superannuation Guarantee (Administration) Act 1992*. Proposed paragraph 168Q(4)(e) would enable the Regulations to prescribe other such purposes, should this be necessary in future.

Procedural fairness

The Committee sought justification for the proposed amendment to subsection 607(1), which would enable the Fair Work Commission (FWC) to conduct an appeal or review without a hearing, provided it takes into account the views of persons making submissions in the matter as to whether this is appropriate (removing the requirement for parties' consent to dispense with an oral hearing). The Committee suggested this may limit the right to procedural fairness.

This amendment was sought by the President of the FWC, the Hon Justice Iain Ross AO. The President considers the current requirement for the parties' consent unduly restrictive, as it prevents the FWC from dealing with appeals in the most appropriate way, with consequent delays and increased costs to parties.

The FWC is generally not required to hold a hearing in performing functions or exercising powers, except as required by the Act, but is of course bound by the requirements of procedural fairness. The obligation to afford procedural fairness (and specifically, an opportunity to be heard) does not necessarily require an oral hearing: *Minister for Immigration and Border Protection v WZARH* [2015] HCA 40 at [33], [63]. Whether an oral hearing (as distinct from an opportunity to provide written submissions) is required depends on the circumstances. Generally, an oral hearing would be required (for example) where disputed facts need to be resolved or there is otherwise evidence of a kind that needs to be able to be tested.

The amendment to subsection 607(1) relates to appeals against and reviews of decisions. Unlike first instance proceedings in which oral hearings may be needed in the context of contested evidence, on appeal or review such questions may not arise for consideration by a Full Bench of the FWC. There will be circumstances where fairness necessitates the oral hearing of an appeal. The FWC is expected to exercise its discretion in light of the requirements of procedural fairness in particular cases, having regard to the parties' views.

Application and Commencement

The Committee sought advice on the necessity of application and commencement clauses for certain provisions in proposed clauses 45 and 46 of Division 2, Part 10, Schedule 7 to the Act and the extent to which this may adversely affect individuals.

Clause 45 would enable applications to the FWC to vary an existing enterprise agreement to resolve uncertainty or difficulty arising from the new definition of casual employment and the entitlement to convert from casual to full-time or part-time employment. This will provide certainty for employers and employees about their rights and obligations by ensuring that agreements work effectively with legislative changes, and is modelled on similar transitional provisions concerning the NES (e.g. following the introduction of family and domestic violence leave in 2018).

Clause 46 provides application provisions for the new definition of casual employment in proposed section 15A, arrangements for offsetting casual loading payments against claimed leave and other entitlements, and various consequential changes relating to casual employment. These provisions provide certainty of rights and obligations, fairness between parties as to outstanding entitlements, and uniform, clear treatment of casual employment across the Act.

The effect of new subclauses 46(1) and 46(3) appearing in the Bill at Schedule 7, Part 10, Division 2, is to apply the statutory definition of 'casual employee' in new section 15A to existing employees who meet the definition by virtue of the nature of their contract of employment, but not to an employee who (before commencement) a court has definitively determined is not casual, or who converted to full-time or part-time employment. This approach ensures certainty of rights and obligations (reflecting the parties' agreement expressed in the relevant contract in question).

Proposed new Division 4A of Part 2-2 of the Act contains new arrangements for conversion from casual to full-time or part-time employment. Subclause 46(5) applies Division 4A to periods of employment starting before, on or after commencement of the Bill. This gives existing employees access to conversion by ensuring their pre-commencement service counts for the purpose of eligibility for an offer of (or request for) conversion.

New section 545A enables amounts payable by an employer to a person for leave and other entitlements to be offset by the amount of casual loading previously paid to an employee to compensate for the absence of such entitlements. Courts can reduce an employee's claim for relevant entitlements by an amount equal to the proportion of the loading amount the court considers appropriate. Subclauses 46(6) to (8) apply this rule to entitlements that accrue, loading amounts paid, and periods of employment arising, before, on or after commencement. This provides for consideration of payments made to employees for the same period of service as a potential claim for entitlements under the NES. The approach provides fairness by ensuring employees receive their correct entitlements, but not so as to require employers effectively to pay for entitlements twice.

The Bill would make consequential amendments to the Act to clarify how conversion from casual to full-time or part-time employment affects NES entitlements. New subclause 46(9) provides that a reference to a period of employment as a casual employee in various NES provisions (concerning annual leave, paid personal/carer's leave and notice of termination and redundancy pay) applies to a period of employment starting before, on or after commencement of the Bill. This ensures certainty and clarity about periods of casual employment and merely confirms, for avoidance of doubt, the long-standing position that casual employees are not entitled to these NES benefits.

The Bill would also define 'regular casual employee' and repeal the current definition of 'long term casual'. New subclause 46(10) provides that a reference to regular casual employee in certain provisions of the Act (including those governing eligibility to request flexible working arrangements, and for the entitlement to unpaid parental leave and protection from unfair dismissal) applies to periods of employment starting before, on or after commencement of the Bill. This does not change entitlements or obligations, but ensures that references to casual employment are consistent throughout the Act.

I trust this advice is helpful, and thank the Committee for its consideration of the Bill.

Yours sincerely

The Hon Christian Porter MP
Attorney-General
Minister for Industrial Relations
Leader of the House

The Hon Alan Tudge MP

Minister for Education and Youth

Ref: MC21-001327

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Parliament House
CANBERRA ACT 2600

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

Dear Senator Helen

Thank you for your letter of 25 February 2021 seeking my advice in relation to a number of issues raised by the Senate Standing Committee for the Scrutiny of Bills (the Committee) regarding the Family Assistance Legislation Amendment (Early Childhood Education and Care Coronavirus Response and Other Measures) Bill 2021 (the Bill).

Significant matters in delegated legislation – proposed emergency Business Continuity Payments (BCPs)

The Committee observes that a number of matters relating to the administration of business continuity payments under the proposed section 205C (emergency BCPs) are to be provided for in delegated legislation (specifically, the Minister's rules made by the Minister under section 85GB of the *A New Tax System (Family Assistance) Act 1999* (Family Assistance Act)). The Committee seeks my advice as to:

- why it is considered necessary and appropriate to leave significant matters such as the manner in which (emergency BCPs) may be made and the determination of circumstances in which a debt will be due to the Commonwealth to delegated legislation
- whether the Bill can be amended to include at least high-level guidance regarding these matters on the face of the primary legislation.

As noted in the Explanatory Memorandum to the Bill, the purpose of emergency BCPs is to 'extend the range of strategies available to the Australian Government to respond to disasters and emergencies', by 'expanding the circumstances in which business continuity payments can be made to approved child care providers'.

To put these amendments in context, the Government moved quickly at the start of the COVID-19 pandemic to put in place the Early Childhood Education and Care Relief Package, (Relief Package) which operated from 6 April to 12 July 2020. The foundation of the Relief Package was the payment of BCPs to approved providers under the existing mechanism in Division 6 of Part 8A of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Family Assistance Administration Act).

The current section 205A of the Family Assistance Administration Act requires that the Minister make Minister's rules prescribing the circumstances in which those BCPs are payable (paragraph 205A(1)(c)), and the method of determining the amount of those payments (paragraph 205A(2)(a)), and permits the Minister's rules to 'prescribe any other matters relating to making (BCPs)', (paragraph 205A(2)(b)).

The Hon Dan Tehan MP, former Minister for Education, amended the *Child Care Subsidy Minister's Rules 2017* (Minister's Rules) with effect from 6 April 2020 to enable those BCPs to be paid—see the *Child Care Subsidy Amendment (Coronavirus Response Measures No. 2) Minister's Rules 2020* (F2020L00406).

However, the current provisions are not well-adapted to enabling BCPs to be paid in emergency circumstances, BCPs are designed largely to enable payment during temporary outages of the information technology systems that support the payment of Child Care Subsidy (CCS), and otherwise assume the ordinary operation of the family assistance law and the CCS scheme. The other amendments to the family assistance law in Part 6 of Schedule 1 to the Bill reflect some of the consequences of utilising BCPs under the current section 205A to provide funding to approved providers in emergency situations.

The proposed section 205C, which will enable the payment of emergency BCPs, does leave a number of matters relating to those BCPs to be specified in the Minister's Rules. Nevertheless, the section endeavours to set as much detail as reasonably practicable for a discretionary payment mechanism that is intended only to be triggered in response to emergencies.

In particular, paragraphs 205C(1)(a) and (b) set out overarching criteria for the payment of emergency BCPs. The definition of 'emergency or disaster' in subsection (2) links to existing definitions for disaster responses payments under the social security law (noting that other emergencies can be specified in the Minister's Rules). Subsections (3) and (4) set out minimum administrative requirements with which the Secretary must comply when paying emergency BCPs. Beyond these matters, it is not clear what other guidance on the content of the Minister's Rules would be suitable for inclusion in the primary legislation, even at a high level.

The nature of emergency BCPs requires that there be considerable flexibility in their implementation and administration. Any scheme for the payment of emergency financial assistance must be inherently able to be fine-tuned and adapted to the needs of responding to the emergency in question. The assistance must be properly targeted to achieve its intended policy outcome of supporting those in need, and it must also work in conjunction with any other actions or supports that are being undertaken in response to the emergency.
A Government response to an emergency involving the payment of emergency BCPs is neither a 'one-size-fits-all' nor a 'set-and-forget' scheme.

Consequently, it is essential that the criteria for eligibility for emergency BCPs, the amounts of payment, and the period in relation to which they are payable, be left to subsidiary legislation. In this respect, section 205C does not depart from the existing section 205A, and is consistent with the operation of legislative provisions in relation to other emergency payments, including disaster recovery allowance (see Part 2.23B of the *Social Security Act 1991* (Social Security Act), esp. s 1061KA), and the Australian Government Disaster Recovery Payment (see Part 2.24 of the Social Security Act).

I note that, unlike BCPs payable under section 205A of the Family Assistance Administration Act, emergency BCPs payable under section 205C will be subject to the internal and external review processes available for most decisions of the Secretary under the family assistance law, further ensuring there is appropriate accountability for those decisions.

Significant matters in delegated legislation – BCPs paid during the Relief Package to be debts in circumstances prescribed in Minister's Rules

The Committee also seeks my advice as to why it is appropriate for the Minister's Rules to set out circumstances in which the BCPs paid during the Relief Package are to be debts. This question relates to the provision at item 36 of Schedule 1 to the Bill.

It should be noted that items 36 and 37 of Schedule 1 operate together. As the Explanatory Memorandum explains, item 37 of Schedule 1 is intended to ensure that BCPs paid during the Relief Package do not need to be automatically offset against other child care payments to approved providers under section 205B of the Family Assistance Administration Act.

Normally, BCPs are not debts, as they must be entirely offset against other payments to providers under section 205B. However, in circumstances where those BCPs are not being offset—as would be the case for BCPs paid during the Relief Package as a consequence of the provision at item 37 of Schedule 1 to the Bill—there does need to be some facility for the Commonwealth to recover those BCPs in appropriate circumstances. These could be where the amount of a BCP paid to a provider exceeded the amount prescribed in the Minister's Rules, or the provider was not eligible for a particular BCP that was paid to them. For example, a provider may have been paid a supplementary amount of BCP under section 60F of the Minister's Rules, but was not eligible for that supplementary amount in accordance with the *Early Childhood Education and Care Relief Package Payment Conditions* published by the Department of Education, Skills and Employment that were in force at the time.

As the Relief Package was implemented rapidly at the start of the COVID-19 pandemic, and was continually adapted during its operation to meet the evolving needs of the early childhood education and care sector, the risk of incorrect payments of BCPs was always recognised and factored into the Government's planning. Some incorrect payments were identified during and after the Relief Package, and the Department instituted quick and effective recovery processes. Once the incorrect payments were notified to the providers concerned, most providers voluntarily paid back the excess amounts.

Because the prospect of recovering BCPs paid during the Relief Package is a one-off and the circumstances in which those BCPs may need to be recovered may be quite specific to a small number of providers, and given the almost complete recovery of incorrect payments to date, there is no need for permanent amendment to the family assistance law to address the issue. Indeed, there may yet be no need for the Ministers' Rules to be amended to provide for any BCPs paid during the Relief Package to be debts. The provision at item 36 of Schedule 1 to the Bill is a reserve power that will enable specific overpayments of those BCPs to be recovered in the event that is necessary.

As mentioned in the Explanatory Memorandum in relation to item 36 of Schedule 1, if Minister's Rules are made to give rise to debts, the existing laws and processes for raising and recovering family assistance law debts must be followed.

Retrospective validation of certain Minister's Rules

The Committee seeks my advice as to:

- why retrospective validation is sought in relation to paragraphs 8(1)(h) and (i) and section 47AA of the Child Care Subsidy Minister's Rules 2017; and
- whether any persons are likely to be adversely affected by the retrospective validation of the provisions, and the extent to which their interests are likely to be affected.

Paragraph 8(1)(h) of the Minister's Rules precludes an individual being eligible for CCS for a session of care provided by an approved child care service during the period of the Relief Package, from 6 April to 12 July 2020.

Section 47AA of the Minister's Rules imposes a condition on the approval of an approved provider that it not charge fees during the period of the Relief Package, and paragraph 8(1)(j) precludes an individual being eligible for CCS for a session of care provided by an approved child care service of a provider that contravened section 47AA (that is charged fees for the session of care).

These provisions were inserted in the Minister's Rules by the *Child Care Subsidy Amendment (Coronavirus Response Measures No. 3) Minister's Rules 2020* (FL202000490). The Explanatory Statement for that instrument states in relation to the provisions:

> *These amendments are intended to ensure that, as part of the Early Childhood Education and Care Relief Package, child care providers are not able to charge fees and receive associated CCS during the period that BCP is payable. In combination with other financial assistance measures announced by the Government, including JobKeeper Payment, extension of absence days and CCCF-SC [grants under the Community Child Care Fund – Special Circumstances program], the Early Childhood Education and Care Relief Package BCP has been structured to ensure the viability of the early childhood education and care sector in circumstances where the COVID-19 pandemic has resulted in decreases in enrolments and a drop in fee revenue for services.*
>
> *BCPs are made to providers to give a guaranteed income stream, based on a reference period, with providers also able to access supplementary payments in exceptional circumstances as detailed in the Early Childhood Education and Care Relief Package Payment Conditions document. Further, families are offered free child care to encourage them to maintain their enrolments with services and to provide financial assistance to families. Therefore, CCS and ACCS must not be payable due to the stated aim of Government that there are no fees to subsidise.*
>
> *These amendments acknowledge and are intended to cater for dynamic circumstances during the COVID-19 pandemic, and ensure fee-relief for families. The measures are temporary, only applying to the period in respect of which services are eligible for Early Childhood Education and Care Relief Package BCP.*

That is, the provision of fee-free child care was an essential policy outcome of the Government's Relief Package, and as CCS operates as a subsidy for child care fees, no CCS should be payable if no fees are payable. As mentioned in the Explanatory Statement for the amending Rules, a suite of financial support measures were provided to approved providers by Government as an alternative to them charging fees for child care.

Advice to Government indicates that there is a risk that the specific measures enacted by paragraphs 8(1)(h) and (j) and section 47AA of the Minister's Rules may not be fully authorised by the powers in the family assistance law to make Minister's Rules. This risk was acknowledged and accepted at the time the provisions were made, noting the importance of a rapid response to the impacts of COVID-19 on the early childhood education and care sector and the importance of ensuring child care remained open and freely available to children of essential workers, including health workers and others on the front lines of responding to the pandemic.

At the time, a provider's participation in the Relief Package was voluntary—a provider could accept the BCPs that were payable, on condition that they did not also charge fees (and hence no CCS was payable), or could suspend their approval under the family assistance law, and continue to charge fees to their families. Some providers did opt out of the Relief Package and its associated conditions.

The retrospective validation of certain Minister's Rules is not expected to impact families or service providers.

However, the Government recognises the theoretical possibility that imposing a condition on a provider that it not charge fees while in receipt of BCPs and other Government support, or rendering an individual ineligible for CCS while their provider is providing free child care, could amount to an 'acquisition of property' in Constitutional terms. Item 39 of Schedule 1 to the Bill provides that, if that is the case, and the acquisition is not on just terms as required by paragraph 51(xxxi) of the Constitution, the Commonwealth must pay the person reasonable compensation.

Broad delegation of administrative powers – power to administer child care funding agreements

The Committee seeks my advice as to:

- why it is necessary to allow the Secretary's powers under section 85GA of the Family Assistance Act to be delegated to an official of any Commonwealth entity at any level
- whether the Bill can be amended to provide legislative guidance as to the categories of people to whom those powers might be delegated.

The Explanatory Memorandum to the Bill provides a reasonably comprehensive rationale for the amendment to section 221 of the Family Assistance Administration Act that would allow the Secretary to delegate their power under section 85GA of the Family Assistance Act to enter into, vary and administer funding agreements in relation to child care. As noted there, the power is analogous to the powers of accountable authorities in section 23 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and 32B of the *Financial Framework (Supplementary Powers) Act 1997* (FF(SP) Act) to enter into, vary and administer arrangements between persons and the Commonwealth under which payments can be made.

Accountable authorities are able to delegate their powers under section 23 of the PGPA Act and section 32B of the FF(SP) Act to officials of any Commonwealth agency at any level (see, respectively, subsection 110(1) of the PGPA Act and subsection 32D(3) of the FF(SP) Act).

The power in section 85GA of the Family Assistance Act is a routine administrative power to manage Commonwealth grants. Commonwealth grants processes are subject to considerable regulation and oversight through mechanisms that stand outside of the delegation process. I direct the Committee's attention to the significant body of information about the framework for Commonwealth grants management on the Department of Finance's website at www.finance.gov.au.

In practice, the power to administer grants cannot be limited to Senior Executive Services (SES) officers or officers holding particular statutorily-designated positions. Grants administration is a widespread task undertaken at all levels of the Australian Public Service, and limiting decision-making in relation to grants to SES officers would have a significant adverse effect on the efficiency and coordination of grants processes.

In short, limiting the scope of delegation of the section 85GA power to SES officers or officers holding particular designated positions is neither feasible nor, given the established framework for Commonwealth grants, necessary to ensure proper oversight of and accountability for grants management.

I trust this information is of assistance.

Yours sincerely

Alan Tudge

10 / 3 / 2021

The Hon Christian Porter MP
Attorney-General
Minister for Industrial Relations
Leader of the House

MC21-003913

23 FEB 2021

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Parliament House
CANBERRA ACT 2600
scrutiny.sen@aph.gov.au

Dear ~~Chair~~

Thank you for your email of 4 February 2021 from your office regarding the Scrutiny of Bills Committee's consideration of the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 (the Bill). I am pleased to provide the following response to the matters raised in Scrutiny Digest 2 of 2021.

You have requested my advice regarding items in the Bill that contain offence-specific defences which reverse the evidential burden of proof. In particularly, you have identified amendments to the:

- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) (Schedule 1, items 150 and 152, and contingent amendments in Schedule 2, items 28 and 32),
- *Australian Security Intelligence Organisation Act 1979* (ASIO Act) (Schedule 1, items 165-167),
- *Intelligence Services Act 2001* (IS Act) (Schedule 1, items 185-193),
- *Taxation Administration Act 1953* (TA Act) (Schedule 1, item 203), and
- *Australian Human Rights Commission Act 1986* (AHRC Act) (Schedule 2, item 52).

I note that a number of the items identified by the Committee make technical updates to existing offence-specific defences and do not change or shift an existing evidential burden from the prosecution to the defendant (Schedule 1, items 165-167, 185-193 and 203 and Schedule 2, item 32).

The remaining items would create new offence-specific defences to permit the disclosure of information to an Inspector-General of Intelligence and Security (IGIS) official who is performing duties, functions or powers as an IGIS official. These defences impose an evidential burden on a defendant who wished to rely on the defence.

In order to discharge an evidential burden, a defendant would need to point to evidence that suggests a reasonable possibility that they disclosed information to an IGIS official and that the disclosure was part of that IGIS official's duties, functions or powers. This is a relatively low threshold. Moreover, this information would be readily available to the defendant in these matters, as it is likely such a disclosure would have been made through existing IGIS channels.

Where the evidential burden has been discharged, it would then be a matter for the prosecution to disprove beyond reasonable doubt that the relevant defence is satisfied in order to establish the offence.

Conversely, requiring the prosecution to prove the substance of this defence beyond reasonable doubt and without reliance on any evidence from the defendant would impose a disproportionate burden on the prosecution. Moreover, secrecy offences under section 34 of the *Inspector-General of Intelligence and Security Act 1986* (Cth) prevent IGIS officials from disclosing 'any information' obtained in the course of their duties, functions or powers to any person, which could limit the ability of the prosecution to independently obtain information from an IGIS official about whether a disclosure was part of their duties, functions or powers. This secrecy is necessary given the highly sensitive nature of the IGIS's work.

I thank the Committee for its consideration of the Bill and hope this information assists.

Yours sincerely

The Hon Christian Porter MP
Attorney-General
Minister for Industrial Relations
Leader of the House

THE HON ALEX HAWKE MP
MINISTER FOR IMMIGRATION, CITIZENSHIP, MIGRANT SERVICES AND MULTICULTURAL AFFAIRS

Ref No: MS21-000203

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
scrutiny.sen@aph.gov.au

Dear Senator

Thank you for your correspondence of 29 January 2021 requesting advice on the Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020 (the Bill).

The Australian Government introduced the Bill to balance the need to protect confidential information used in making certain decisions under the *Migration Act 1958* (the Migration Act) and the *Australian Citizenship Act 2007* (the Citizenship Act) with the need to preserve the ability of the courts to fulfil their judicial review function under the Constitution in relation to such decisions.

The Bill amends the Migration Act and the Citizenship Act to create a framework for the protection of information provided in confidence by gazetted law enforcement and intelligence agencies and used in character-related visa and citizenship decisions, which includes applications to revoke or set aside such decisions. Criminal intelligence and related information is vital to assess the criminal background or associations of non-citizen visa applicants and visa holders.

In the Scrutiny Digest 1 of 2021, the Committee sought clarification on the following matters:

- adequacy of judicial review
- significant matters in delegated legislation
- parliamentary scrutiny
- evidentiary certificates
- natural justice.

A copy of the detailed response is enclosed.

Thank you for raising this matter.

Yours sincerely

ALEX HAWKE
17/2/2021.

Parliament House Canberra ACT 2600

Annex A – Responses to queries raised by the Committee

STANDING COMMITTEE FOR THE SCRUTINY OF BILLS
Scrutiny Digest 1 of 2021

Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020

Minister's Response

1.54 In light of the committee's scrutiny concerns outlined above, the committee requests the minister's advice as to:

• whether the bill can be amended to allow the court to disclose part of the secret information in circumstances where partial disclosure could be achieved without creating a real risk of damage to the public interest;

The Bill proposes amendments to the *Migration Act 1958* (the Migration Act) and the *Australian Citizenship Act* 2007 (the Citizenship Act) to create a framework for the protection and controlled authorised disclosure of information provided in confidence by gazetted law enforcement and intelligence agencies and relied upon in character-related visa and citizenship decision-making (protected information). The framework will enable the Minister to authorise the disclosure of protected information to specified persons or bodies, such as a tribunal or a Commonwealth officer after consultation with the gazetted agency which provided such information. It also empowers the High Court, Federal Court of Australia and the Federal Circuit Court (the Courts) to order the Minister to disclose information to it if satisfied that the information is protected information and it is for the purposes of the proceedings before the Court in relation to a relevant character-related decision.

In practice, law enforcement and intelligence agencies provide confidential information to the Department of Home Affairs (the Department) on the basis that it can be protected from disclosure. This is because, if such information were disclosed, there would be a real risk that there would be damage to the public interest and jeopardise the capabilities of law enforcement and intelligence agencies – and potentially compromise active investigations. Therefore, it is the agencies themselves who designate the information as confidential because of the intrinsically sensitive nature of its contents and scope.

Criminal intelligence and related information is vital to assess the criminal background or associations of non-citizen visa and citizenship applicants and visa holders. The measures in this Bill will ensure that information – disclosed in confidence by law enforcement and intelligence agencies for use in visa and citizenship decision-making – is appropriately protected.

Given the highly sensitive nature of confidential information and the identities of the gazetted agencies, partial disclosure of the information or giving the gist of the information to the applicant or their legal representative could damage the public interest. Further, it is open to gazetted agencies to communicate information which they may indicate is not communicated in confidence. Where this occurs, the information would not be subject to the protected information framework and so may (subject to other relevant laws) be subject to full or partial disclosure, or disclosure of a summary, as appropriate.

The Minister considers that the current approach in the Bill is appropriate and that any consideration of whether to disclose part of the protected information would be duplicative and unnecessary: the same risks of damage to the public interest would arise from partial and full disclosure given the sensitive nature of the information in question.

Nonetheless, the Bill will provide for greater judicial oversight in visa and citizenship decisions that rely on confidential information. The amendments allow the Courts to access all relevant information that was considered by the Minister (or delegate) when that decision was made.

The Bill will provide safeguards for the applicant by allowing the Courts to decide how much weight to give to the confidential information that has been submitted in evidence. This allows the Courts to weigh up a number of factors, including fairness to the applicant and the public interest, in using this information in review of visa and citizenship decisions. Practically, this may include a situation where the Court has determined not to disclose the information, which would include not disclosing the information to the applicant. Even so, the Court is to weigh up a number of factors when assessing what weight to give to evidence, including unfair prejudice to an applicant by not having access to the confidential information, as well as the public interest.

• whether the gazetted intelligence and law enforcement agencies which may make use of the proposed scheme should be outlined in primary legislation or at least in delegated legislation subject to parliamentary disallowance, given the importance of balancing the constitutional right of an individual to meaningful judicial review with the interest of keeping certain information connected with law enforcement secret;

The Bill amends sections 5(1) and 503A-503C of the Migration Act and introduces new section 52A-52C of the Citizenship Act to provide a framework for the disclosure of confidential information provided by gazetted law enforcement and intelligence agencies for consideration in character-related visa and citizenship decisions.

The gazetted intelligence and law enforcement agencies are defined in the Bill at section 503A(9) of the Migration Act (which is identical to the current section 503A(9) of the Migration Act). The same definition applies within the context of the Citizenship Act. Gazetted agencies include Australian and foreign law enforcement or intelligence bodies which are listed in the Gazette. A war crimes tribunal established under international arrangements of law may also be a gazetted agency and is not required to be listed in the Gazette.

The Australian and foreign law enforcement or intelligence bodies which are gazetted agencies are currently listed in Gazette Notice 16/001 made pursuant to section 503A(9) of the Migration Act which was signed by Minister Dutton on 22 March 2016 and commenced on 1 April 2016. Gazette Notice 16/001 is published on the Federal Register of Legislation.

As such, the gazetted agencies are publicly identifiable. Effectively, this means that affected persons are on notice as to the identities of intelligence and law enforcement agencies that may communicate confidential information to the Department for use in character-related visa and citizenship decision making.

This may help affected persons and their representatives understand where the confidential information may be sourced and to put forward relevant matters for the consideration of the Court. As such, it is not necessary to list the gazette agencies in either primary or delegated legislation.

• whether proposed subsection 52C(5) of the *Australian Citizenship Act 2007* and proposed subsection 503C(5) of the *Migration Act 1958* could be amended to provide that the list of matters relevant to assessing the risk to the public interest is non-exhaustive;

The measures in the Bill are necessary to strengthen the Government's ability to uphold public safety and the good order of the Australian community through character-related decisions made under both the Migration Act and the Citizenship Act.

These measures will enhance the ability of decision-makers to use confidential information to manage the risk of certain individuals of character concern, where there may otherwise be insufficient information to underpin a decision. The changes help ensure that these individuals who pose a risk to public safety will be prevented from entering or remaining in Australia, or acquiring Australian citizenship (which offers additional rights and privileges and further permanency), by providing a framework which protects the confidential information from harmful disclosure. Regardless of which agencies provide information under the proposed amendments, the Courts must determine if disclosure of confidential information would create a real risk of damage to the 'public interest', having regard to a series of matters specified in the Bill or specified in the regulations (if any, and only those matters). It is appropriate that the list of matters the Court can have regard to (if relevant) in subsections 52C(5) of the Citizenship Act and 503C(5) of the Migration Act is exhaustive, as it provides clarity and certainty for the Court in exercising its functions.

The scope and content of the matters listed in those sections also reflects and emphasises the sensitive nature of the information, and the need for careful consideration to be given as to whether it would create a real risk of damage to the public interest if disclosed more widely, including to the applicant in judicial review proceedings. It should be noted that it is the relevant intelligence and law enforcement agency which designates the information as confidential because of the sensitive nature and the list of matters acknowledges and reflects this characterisation.

The potential disclosure of confidential information outside the framework of the Bill also poses an unacceptable risk to the intelligence capabilities, operations and sources of law enforcement and intelligence agencies – including active investigations. This risks jeopardising the trusted relationship between the Department and law enforcement and intelligence agencies.

The Bill provides that the Courts may give such weight in the substantive proceedings to the information as the Court considers appropriate in the circumstances. Such circumstances may involve a situation where the Court has determined not to disclose the protected information. This allows the Courts to weigh up a number of factors, including unfair prejudice to an applicant by not having access to the confidential information and the public interest. This provides clear

safeguards for the applicant's interests in any proceedings and places these safeguards within the control of the Court.

• the appropriateness of allowing 'other matters' relevant to assessing the risk to the public interest to be specified in regulations;

This can be effected through amendments to the *Australian Citizenship Regulation 2016* (the Citizenship Regulation) or *Migration Regulations 1994* (the Migration Regulations), as appropriate. Regulations made under Part 9 of the Migration Act or under the Citizenship Act are disallowable and subject to Parliamentary scrutiny.

It is noted that paragraphs 52C(5)(h) of the Citizenship Act and 503C(5)(h) of the Migration Act provide a mechanism for other matters to be specified under these subsections. These paragraphs were included in the Bill to provide flexibility going forward.

Given the rapidly evolving and complex security challenges, these amendments are necessary to protect confidential information shared between the Department, law enforcement and intelligence agencies, and to uphold public and national security interests. Protection of sensitive and confidential information also supports broader strategies to counter terrorism, transnational crime and related activities.

As such, if Parliament passes the Bill, the Department will monitor the operation of the protected information framework provided for in the Bill and, if deemed desirable or necessary to assist the Court in determining whether to disclose the confidential information, to specify further matters for the Court to have regard under subsections 52C(5) of the Citizenship Act and 503C(5) of the Migration Act. This can be effected through amendments to the *Australian Citizenship Regulation 2016* (the Citizenship Regulation) or *Migration Regulations 1994* (the Migration Regulations), as appropriate. As amendments to these Regulations are disallowable, they will be accompanied by a Statement of Compatibility with Human Rights and subject to parliamentary scrutiny.

• whether, given the effect the secrecy provisions may have on the practical ability of the court to ensure power is exercised subject to jurisdictional limitations, proposed subsection 52B(8) of the *Australian Citizenship Act 2007* and proposed subsection 503B(8) of the *Migration Act 1958* can be amended to provide that the minister has an obligation to consider the exercise of the power to allow disclosure of information supplied by law enforcement or intelligence agencies, including to specified tribunals undertaking merits review of relevant decisions.

Section 503A of the Migration Act was introduced by the *Migration Legislation Amendment (Strengthening of Provisions relating to Character and Conduct) Act 1998*. Under section 503A, the Department was able to rely upon confidential information provided by law enforcement and intelligence agencies to inform character test based visa decisions under the section 501 provisions of the Migration Act. The current framework in section 503A – 503D permits the Minister to protect information from disclosure during merits review as it relates to character-related visa decisions. This is unaffected by the High Court decision described below.

This Bill addresses a High Court decision in which the Court held that the then

Minister for Immigration and Border Protection could not be prevented by section 503A of the Migration Act from being required to divulge certain confidential information to the High Court or the Federal Court of Australia in order to review character test based visa decisions.

The Bill will provide the Minister with discretionary powers to disclose the confidential information (having consulted the relevant gazetted agency) to specified persons, bodies, tribunals or courts.

Given the sensitive nature of protected information, and the Minister's power under the Migration Act's current framework to protect protected information from disclosure during merits review, it is not appropriate for this legislation to require the Minister to have a duty to consider whether to authorise disclosure of that information to Tribunals undertaking merits review of relevant decisions.

Information which falls within the protection of the Bill's framework is, by its nature, highly sensitive. This is because it is information communicated to the Department by its intelligence and law enforcement agency partners on the condition that it is treated as confidential. It is the agencies that have designated the information as confidential and therefore requiring protection under the Bill's framework. As noted above, such agencies have been consulted on the Bill's framework and have provided their support for it. As such, it is appropriate for the Minister not to have a duty to consider whether to authorise disclosure of such information (subject to consultation with the relevant agency).

As noted elsewhere, the Bill is designed to strengthen protection for confidential information provided by law enforcement and intelligence agencies. The Bill will ensure confidential information can be used in certain character-related visa and citizenship decisions without the risk of disclosure unless a Court determines that disclosure would not create a real risk of damage to the public interest.

If the applicant is unsuccessful before a Tribunal, judicial review of that decision is always available. The framework of the Bill is such that the Court can exercise its judicial functions in order to conduct an effective judicial review which has regard to, amongst other things, the interests of the applicant.

The framework of the Bill provides a mechanism which allows the Court to require disclosure of the relevant protected information to it and a further mechanism for the Court to consider whether it can disclose the protected information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest.

Specifically, the framework will provide that during judicial review, the Courts may order the Minister to disclose confidential information to it that was relevant to the visa decision (that is, the Minister will not have a discretion not to comply in this circumstance). If protected information is provided in evidence, a party to the proceedings may make submissions to the Court on the use which should be made of the information and the impact disclosure of that information may have, if that party is aware of the content of the information and has not obtained the information unlawfully or in circumstances that would found an action for breach of confidence.

As noted elsewhere, the Bill provides that the Courts may give such weight in the substantive proceedings to the information as the Court considers appropriate in the

circumstances. Such circumstances may involve a situation where the Court has determined not to disclose the protected information. This allows the Courts to weigh up a number of factors, including unfair prejudice to an applicant by not having access to the confidential information and the public interest. This provides clear safeguards for the applicant's interests in any proceedings and places these safeguards within the control of the Court.

1.59 In light of the above, the committee requests that proposed subsection 52A(3) of the *Australian Citizenship Act 2007* and proposed subsection 503A(3) of the *Migration Act 1958* be amended to omit the prohibition on the production or giving of confidential gazetted agency information to 'a parliament or parliamentary committee'.

I note and appreciate the Committee's concern. The Committee notes that the Senate has well-established processes allowing the Executive to make claims for public interest immunity, which would, if the claim were successful, prevent the release of confidential information.

A Minister's claim for public interest immunity in relation to protected information before Parliament would be broadly assessed by weighing up the harm to the public interest in disclosing that information against Parliament's claim to know particular things about government administration, so that the Parliament can perform its proper function of scrutinising, and ensuring accountability of, the government.

The Bill provides that neither a Commonwealth officer nor the Minister can be required to produce protected information to, or give the information in evidence before, Parliament or a parliamentary committee. This reflects the current provisions of s503A(2)(c) and (d).

Given the sensitive nature of the confidential information provided by intelligence and law enforcement agencies and the potential damage to the public interest if such information is disclosed, relying on public interest immunity may not provide the kind of comprehensive protection required for the full range of confidential information provided by law enforcement and intelligence agencies to support character-related decisions. This is crucial given the sensitive nature of the confidential information and the importance of the Department's information sharing relationships with intelligence and law enforcement agencies, as well as the potential damage to the public interest if such information is disclosed.

As previously noted, the Bill provides a framework for the protection and controlled disclosure of sensitive information provided on condition of confidentiality by gazetted law enforcement and intelligence agencies for use in character-related visa and citizenship decision-making. Protection of sensitive and confidential information also supports broader strategies to counter-terrorism, transnational crime and related activities.

The Bill provides a framework which empowers the Court to require disclosure of the relevant protected information to it and a further mechanism for the Court to consider whether it can disclose the protected information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest. This allows the Courts to review effectively the Executive's decision-making specified in the Bill.

1.69 In light of the above, the committee requests the minister's advice as to:

• why it is considered necessary and appropriate for evidentiary certificates to be prima facie evidence of the fact that information was communicated to an officer by a gazetted intelligence or law enforcement agency;

The Bill is designed to strengthen protection for confidential information provided by law enforcement and intelligence agencies and used in character-related visa and citizenship decision making. The Bill will ensure confidential information can be used in such decisions, without the risk of disclosure, unless a Court determines that the information should be disclosed to it during relevant substantive proceedings and further determines that disclosure would not create a real risk of damage to the public interest.

The framework in the Bill protects information which is:

- communicated to an authorised Commonwealth officer by a gazetted agency on the condition it is treated as confidential information; and
- relevant to the exercise of certain powers under the Citizenship Act (as set out in paragraph 52A(1)(b)) and the Migration Act (as set out in paragraph 503A(1)(b)).

Highly sensitive information must meet these two tests in order to benefit from the protections set out in the Bill's framework.

Practically, it may be difficult to prove that information is "relevant to the exercise" of one of the identified statutory powers without putting that information in evidence before the Court in a way that would be accessible to the applicant. Given the highly sensitive nature of this information, this would not be appropriate. Similar difficulties can arise in proving that information was provided by a gazetted agency, given that the name of that agency cannot be disclosed by reason of section 52D of the Citizenship Act and section 503D of the Migration Act. It is further noted that the provisions of sections 52C(1) of the Citizenship Act and 503C(1) of the Migration Act are such that it is for the Court to be satisfied that information is protected information by falling within the ambit of sections 52A and 503A of those Acts. It is therefore the role of the Court to assess and give weight to the evidence before it when considering whether it is so satisfied, which includes evidentiary certificates.

The capacity to lead hearsay evidence to prove that information falls within the relevant sections, and to use a certificate to provide prima facie evidence that information was provided by a gazetted agency is therefore crucial to allowing the Court to exercise its functions and simultaneously protect highly sensitive and confidential information. As noted above, it remains within the control of the Court to disclose the information to, amongst others, the applicant if it determines that disclosure would not create a real risk of damage to the public interest.

• why it is considered necessary and appropriate to provide that the rules of natural justice do not apply to the consideration or exercise of the power for the minister to make a declaration to allow the disclosure of information; and

The Bill strikes an appropriate balance between protecting the public interest and providing fairness to the applicant.

- The Bill will allow confidential information provided by law enforcement and intelligence agencies to be considered by the Courts while preventing its further disclosure where it would create a real risk of damage to the public interest.
- The Bill will provide safeguards for the applicant by allowing the Courts to decide how much weight to give the confidential information in judicial review, and to further disclose this information when there is no real risk of damage to the public interest.

The Bill does not remove natural justice from character-related visa and citizenship decision making processes. Rather, natural justice is owed at the stages in the process in a way that strikes an appropriate balance between protecting the public interest (by protecting confidential information provided by intelligence and law enforcement agencies) and providing fairness to the affected person. As noted elsewhere, protected information is highly sensitive and is designated as confidential and therefore requiring protection under the Bill's framework by the agencies which have communicated it to the Department.

Access to merits and judicial review rights will not be affected by the Bill. As noted elsewhere, and noting the sensitive nature of protected information, the current framework under section 503A – 503D of the Migration Act permits the Minister to protect protected information from disclosure during merits review of character-related visa decisions. If the Minister does authorise disclosure of protected information to, for example, a Tribunal, in accordance with sections 52B(1) of the Citizenship Act and 503B(1) of the Migration Act, then the Tribunal will have obligations to afford natural justice during any relevant merits review subject to the obligations imposed upon it by sections 52B of the Citizenship Act and 503B of the Migration Act.

An affected person has the right to access judicial review of a Tribunal's decision. If so, the framework in section 52C of the Citizenship Act and section 503C of the Migration Act will be enlivened. This framework provides a mechanism which allows the Court to require disclosure of the relevant protected information to it and a further mechanism for the Court to consider whether it can disclose the protected information to the applicant (amongst others) if doing so does not create a real risk of damage to the public interest. In this way, the Court can exercise its judicial functions in order to conduct an effective judicial review which has regard to, amongst other things, the interests of the applicant.

Additionally, the Bill will allow the Courts to admit confidential information into evidence and to decide how much weight to give to that evidence. This will allow the Courts to weigh up a number of factors, including unfair prejudice to an applicant by not having access to the confidential information and the public interest.

The balance reflected in the Bill will enable law enforcement agencies to continue to provide confidential information to the Department to make fully informed visa and citizenship decisions on character grounds, while providing fairness to applicants seeking merits or judicial review of a departmental decision. This is essential to the

Government's core business of regulating, in the national interest, who should enter and remain in Australia, and who should be granted Australian citizenship and the privileges which attach to it.

• why it is considered necessary and appropriate for proposed section 52J to provide that proposed sections 52G and 52H are exhaustive statements of the natural justice hearing rule in relation to review of a decision by the Administrative Appeals Tribunal; and

Amendments to the Citizenship Act in proposed section 52G will enable the Minister to prevent the disclosure of certain sensitive information or documents to the Tribunal relating to citizenship decisions under merits review where the Minister certifies that disclosure of that information or document would be contrary to the public interest, including for reasons relating to the defence, security or international relations of Australia, or because it would involve the disclosure of deliberations or decisions of the Cabinet or a committee of the Cabinet.

Further amendments to the Citizenship Act in proposed section 52H apply to information or documents:

- which the Minister has certified the disclosure would be contrary to the public interest (for any reason other than those set out in section 52G); or
- given to the Minister in confidence.

The Department may give such documents or information to the Tribunal, but must notify the Tribunal that section 52H applies to the documents or information, and may give written advice about the significance of the documents or information. The Tribunal may have regard to any matter in the documents or information during the relevant merits review and has a discretion to disclose any matter in the documents or information to, amongst others, the applicant for merits review.

These measures will strengthen the framework for the protection and use of confidential information in merits review in the Citizenship Act that is substantially the same as that in the Migration Act.

Sections 52G and 52H of the Citizenship Act are based substantially on sections 437 and 438 of the Migration Act. Section 422B(2) of the Migration Act provides that sections 416, 437 and 438, insofar as they relate to Division 4 of Part 7 of the Migration Act (conduct of merits review by the Administrative Appeals Tribunal), are taken to be an exhaustive statement of the requirements of the natural justice hearing rule in relation to the matters they deal with.

Section 52J provides that, for the purposes of the review of a decision by the Tribunal, sections 52G and 52H are taken to be an exhaustive statement of the requirements of the natural justice hearing rule in relation to the information or documents to which those sections apply. Section 52J does no more than provide consistency of approach between the Citizenship Act and the Migration Act as it relates to the disclosure of certain information under a non-disclosure certificate framework.

Providing an exhaustive statement of the natural justice hearing rule provides the Tribunal and the applicant with clarity and certainty as to the precise nature of the natural justice obligations owed.

If the applicant is unsuccessful at merits review, judicial review of that decision may be sought and the Court will determine whether the Tribunal exercised its powers lawfully, including its obligations as they relate to the natural justice hearing rule.

In all other circumstances, information is subject to the normal requirements of the natural justice hearing rule.

1.73 In light of the above, the committee requests the minister's detailed advice as to why it is considered necessary and appropriate to leave matters relevant to the court's determination of whether to disclose information for judicial review to delegated legislation.

As noted, this can be achieved through amendments to the Citizenship Regulation or the Migration Regulations, as appropriate. Regulations made under Part 9 of the Migration Act or under the Citizenship Act are disallowable. They will be subject to Parliamentary scrutiny.

The measures in this Bill will ensure that sensitive information – disclosed in confidence by law enforcement and intelligence agencies – is appropriately protected. Protection of sensitive and confidential information supports broader strategies to counter-terrorism, transnational crime and related activities.

As such, paragraphs 52C(5)(h) of the Citizenship Act and 503C(5)(h) of the Migration Act provide a mechanism for other matters to be included in subsections 52C(5) and 503C(5) if specified in relevant regulations. These paragraphs were included in the Bill in order to provide flexibility.

If Parliament passes the Bill, the Department will monitor the operation of the protected information framework provided for in the Bill. If deemed desirable or necessary to assist the Court in its task of determining whether to disclose protected information, appropriate Regulations to include further matters for the Court to have regard in subsections 52C(5) of the Citizenship Act and 503C(5) of the Migration Act may be made. This flexible approach allows the matters in subsections 52C(5) of the Citizenship Act and 503C(5)(h) of the Migration Act to reflect changing circumstances and evolving security challenges, and this will assist the Court accordingly.

THE HON JOSH FRYDENBERG MP
TREASURER

Ref: MS21-000195

Senator Helen Polley
Chair
Senate Standing Committee for the Scrutiny of Bills
Parliament House
CANBERRA ACT 2600

Dear Senator Polley

National Consumer Credit Protection Amendment (Supporting Economic Recovery) Bill 2020

Thank you for your letter on behalf of the Senate Standing Committee for the Scrutiny of Bills (the Committee) regarding the *National Consumer Credit Protection Amendment (Supporting Economic Recovery) Bill 2020* (the Bill).

In that letter, the Committee has sought my advice as to:

- why it is considered necessary and appropriate to leave certain details to delegated legislation;
- whether the Bill could have been amended to prescribe at least broad guidance in relation to certain matters;
- why it is considered necessary and appropriate to leave to delegated legislation the prescription of circumstances in which it will be a defence to the offence or civil penalty provision; and
- why it is proposed to use offence specific defences (which reverse the evidential or legal burden of proof).

Significant matters in delegated legislation, 133DB

The proposed amendments to the *National Consumer Credit Protection Act 2009* (the Credit Act) introduced by item 60 and 65 of Schedule 1 to the Bill would amend section 133DB of the Credit Act (which requires licensees to give projections of equity before providing credit assistance or entering a credit contract). The amendments provide that licensees must show a consumer a comparison of the consumer's stated expected aged care costs with equity projections before providing credit assistance for a reverse mortgage, entering into a reverse mortgage, increasing the credit limit of a reverse mortgage or making an unconditional representation about the consumer's eligibility. The comparison must be shown to the consumer in person or in a way prescribed in the regulations (133DB(1)(b)(ba)). Non-compliance with the obligations to provide comparisons of equity projections and aged care costs is subject to criminal offences in addition to civil penalties (Subsections 133DB(1) and (2) of the Credit Act).

Parliament House Canberra ACT 2600 Australia
Telephone: 61 2 6277 7340 | Facsimile: 61 2 6273 3420

Leaving to delegated legislation the prescription of circumstances the manner of giving comparison of equity projection and aged care costs to a consumer to delegated legislation

Regarding proposed subsection 133DB(1)(b)(ba) of the Credit Act, the committee has asked why it is considered necessary and appropriate to leave the manner of giving the comparison of the equity projection and aged care costs to a consumer to be specified in delegated legislations; and whether the Bill can be amended to include at least high-level guidance regarding these matters on the face of the primary legislation.

As outlined in the explanatory memorandum, the Bill is part of the Government's economic response to the COVID-19 pandemic. It is appropriate for the manner of giving the information to be specified in regulations even though a contravention of the obligation can result in a civil and criminal penalty. This provides the necessary flexibility for the Government to respond quickly to address circumstances of concern as they arise and to make timely amendments including where necessary to deal with new and emerging risks and mitigation strategies related to COVID-19. For example; during the COVID-19 pandemic it may not be possible or preferable to require a licensee to show information to a consumer in person because of the level of community transmission of the virus in Australia at any one time and/or collective governments' responses to it (including restrictions on the movement of people to contain the spread of the virus). Moving beyond the pandemic, prescription by legislative instrument also facilitates adaptation to new and emerging technologies. In practice, this will accommodate innovation in the reverse mortgage sector while ensuring consumers receive the same level of protection across all modes of communication. Prescription by legislative instrument is necessary because of the changing nature of the subject matter.

This power is therefore appropriate and necessary to deal with situations where the operation of the Bill may produce unintended or unforeseen results that are not consistent with the policy intention for the consumer protection regime, for example, unnecessarily putting consumers and the Australian community at risk.

This regulation-making power provides the necessary flexibility for the Government to respond quickly to address circumstances of concern that arise and to make timely amendments. Therefore, although it may be desirable to place all of the details in primary legislation, I consider that it is necessary and appropriate to place specificity in delegated legislation as, given the nature of the reforms, this retains the ability to respond to unforeseen issues that could affect the ability for consumers to transact safely as well as accommodate future advances in business communications.

As regulations, the prescribed circumstances would be considered by the Federal Executive Council and subject to disallowance by the Parliament. Consistent with standard practice, the Government envisages undertaking consultation before making any regulations under this power to minimise the risk of unintended consequences. It is intended to rely on this justification.

While technically possible, the Government's intent was not to provide high level guidance on the face of the primary legislation for when it is appropriate to exercise the power to make regulations for the purpose of 133DB(1)(b) of the Credit Act is to ensure that the power is sufficiently broad to accommodate unforeseen circumstances.

Significant matters in delegated legislation, section 133EA (non-ADI credit standards)

The proposed amendments to the Credit Act in item 67 of Schedule 1 to the Bill would insert new section 133EA into the Credit Act. Proposed section 133EA would allow the Minister to determine non-ADI credit standards. Obligations in Part 3-2 of the Credit Act to assess whether credit is

unsuitable will no longer apply in relation to certain types of credit conduct. Instead, where this conduct is engaged in by ADIs, it will be regulated primarily by existing prudential standards made by legislative instrument by APRA under the *Banking Act 1959* (Banking Act). Where this conduct is engaged in by non-ADI credit providers, it will be regulated by the non-ADI credit standards.

The policy intent of these reforms is to ensure that ADIs continue to comply with APRA's prudential lending standards requiring sound credit assessment and approval criteria, while key elements of APRA's ADI lending standards are adopted and applied to the new non-ADI framework.

Adopting elements from the APRA lending standards for the non-ADI standards ensures a level playing field between ADIs and non-ADIs in the new credit framework. The setting of non-ADI standards in subordinate legislation enables them to be made consistently with the standards APRA requires of ADIs in APS 220 Credit Risk Management, which is itself subordinate legislation. Therefore, just as the ADI regime in APS 220 provides flexibility for APRA to update these requirements over time, it is necessary that a similar flexibility is afforded for the non-ADI standards to be dynamically updated in line with changes to the ADI regime. Requiring changes to be made to primary legislation to align APS 220 and the non-ADI Standard would result in periods of inconsistent regulatory frameworks, affording a competitive advantage to one of the sectors. This would be contrary to the Government's commitment to encourage and facilitate competition in the financial system.

As an independent prudential regulator, APRA maintains control of the content of their prudential standards and is able to dynamically update them as the regulatory landscape evolves and demands it. Therefore, it is critical that APRA has the flexibility currently afforded by the Banking Act to enable it to make changes to its prudential standards.

The Minister's power is already limited to determining systems, policies and processes that the non-ADI credit provider must have for engaging in non-ADI credit conduct.

If the non-ADI standards were contained in primary legislation or were amended to further limit the Minister's powers, this could constrain the scope of changes APRA could practically make to its prudential standards without disturbing the level playing field between ADIs and non-ADIs and may require significant deferral of changes to APRA's standards to enable primary legislation to amend the non-ADI credit standard framework.

Significant matters in delegated legislation, 133CD

The amendments in Schedules 2 and 6 to the Bill make amendments to the Credit Act relating to the regulation of small amount credit contracts (SACCs) and consumer leases. These amendments include prohibiting a licensee from entering into a SACC if the repayments under the contract would not be of equal amounts or would be repaid on an irregular basis (Schedule 2, item 12, proposed section 133CD), and prohibiting unsolicited communication about SACCs in certain circumstances (Schedule 2, item 12, proposed section 133CF).

The purpose of these provisions is to increase the consumer protections that apply in relation to SACCs by prohibiting behaviour by licensees that has historically resulted in harm to consumers. For example, allowing unequal payments or irregular repayment periods for SACCs permits licensees to lengthen the period of the SACC and therefore receive additional monthly fees.

The prohibitions in the Bill are broad and high-level so as to ensure effective coverage of the provisions, however there may be circumstances where unanticipated but legitimate behaviour by licensees would breach the provisions but not result in harm to consumers. To ensure that

non-harmful behaviour is not captured by the prohibitions on unequal SACC repayments or certain unsolicited communications about SACCs, the Bill allows for delegated legislation to be made that specifies circumstances when the provisions would not be breached.

In the case of the prohibition on unequal and irregular SACC repayments, the Bill allows for one circumstance in which otherwise unequal repayment periods are taken to be equal, namely that regular payments that fall on non-business days may be paid on the previous or next business day and will still be taken to be equal (see Schedule 2, item 12, proposed section 133CD(4) of the Credit Act). However, there may be other unforeseen situations when otherwise unequal repayment periods should also be taken to be equal. Allowing ASIC to make an instrument that sets out the conditions where this will be the case ensures that businesses and consumers are not inappropriately penalised by the high-level prohibition.

The Bill also includes a general and broad prohibition on any communication that includes an offer to enter into a SACC or an invitation to apply for a SACC to a consumer has ever been a debtor under a SACC (including to consumers who currently have a SACC). As noted in the explanatory memorandum this prohibition is intended to stop licensees from making unsolicited communications to vulnerable consumers and to ensure that consumers freely choose to enter into a SACC rather than being prompted to apply. This is an important part of the consumer protection provisions in the Bill, as the Review of the Small Amount Credit Contract Laws found that consumers can be directly targeted with invitations to enter into a new SACC when they are particularly vulnerable, such as around Christmas or when their current SACC is about to end. The prohibition on unsolicited communication is drafted at a high-level to only apply to certain targeted invitations to specific consumers (for example, by SMS or email), however the regulation-making power ensures that any unforeseen kinds of communication that do not cause harm to consumers can be excluded from the prohibition.

At this time it is not expected that ASIC would make an instrument setting out when unequal repayment periods are taken to be equal, nor that regulations would be made to permit communication that would otherwise be in breach of new section 133CF. However, the power to make delegated legislation is important in both of these instances to allow the law to respond appropriately to rapidly changing business practices and not unfairly penalise legitimate business behaviour.

Significant matters in delegated legislation, proposed sections 323B and 323A

Leaving the prescription or determination of avoidance schemes and matters relevant to making a conclusion that a scheme is an avoidance scheme to delegated legislation, proposed section 323B

Proposed section 323B of the Credit Act outlines a number of matters that must be considered in determining whether there is an avoidance purpose in addition to the regulation-making power provided by proposed paragraph 323B(1)(c) of the Credit Act. The regulation-making power recognises that industry participants may develop new avoidance practices which may require the Government to specify additional matters that must be considered in determining whether the relevant avoidance purpose exists. Not including the regulation-making power will jeopardise the ability of the law to achieve its purpose of prohibiting schemes that prevent a contract from being a small amount credit contract or a consumer lease.

Not including high-level guidance regarding schemes that will be presumed to be entered into for an avoidance purpose on the face of the primary legislation, proposed section 323C

Proposed section 323B of the Credit Act outlines a number of matters that are key indicators of whether there is an avoidance purpose. The instrument making powers in proposed subsection

323C(1) reflects historical experience that avoidance schemes tend to proliferate quickly. The instrument making powers ensure that either the Government or ASIC can respond quickly and effectively to evolving practices as needed.

Proposal to confer on ASIC the broad power to exempt schemes from the operation of the prohibition on avoidance schemes in section 323A, and the absence of high level guidance

The power for ASIC to, by legislative instrument, exempt a scheme or class of schemes from all or specified parts of the prohibitions set out in proposed section 323A of the Credit Act ensures that ASIC can appropriately deal with schemes that do not cause harm to consumers or regulated industry participants and have legitimate non-avoidance purposes. A broad power is needed in order to capture the full array of schemes that might arise and to ensure that non-harmful business practices are not subject to the prohibition. In the absence of a broad power legitimate arrangements may be inappropriately subject to the prohibitions in proposed section 323A of the Credit Act. Providing high level guidance in the primary law might operate to inappropriately restrict the application of the power and prevent it from applying to unforeseen schemes.

Burdens of proof, proposed section 323C

Placing the legal burden of proof on the defendant by including presumptions in relation to civil penalty provisions

In the context of proposed section 323C of the Credit Act, placing the legal burden of proof on the person is appropriate as it will be within the knowledge for the person, opposed to ASIC to establish that it would not be reasonable to conclude that there was a relevant avoidance purpose. For example if the scheme in question does have a legitimate (non-avoidance) purpose, that matter would be known to the person. Although not strictly relevant, this approach is consistence with the guidance provided by pages 50-52 of the *Guide to Framing Commonwealth Offences* which was referred to by the Committee. It should also be noted that the presumption applies only in civil cases. Not reversing the legal burden of proof will jeopardise the ability of the law to achieve its purpose of prohibiting schemes that prevent a contract from being a small amount credit contract or a consumer lease.

Not reversing the evidential, rather than legal, burden of proof

In the context of proposed section 323C of the Credit Act, merely reversing the evidential burden of proof is not sufficient as it will likely fall to ASIC to establish that it would not be reasonable to conclude that there was a relevant avoidance purpose. This is inappropriate as it will be considerably easier for the person, opposed to ASIC to establish that it would not be reasonable to conclude that there was a relevant avoidance purpose. Not reversing the legal burden of proof will jeopardise the ability of the law to achieve its purpose of prohibiting schemes that prevent a contract from being a small amount credit contract or a consumer lease.

Significant matters in delegated legislation; Reversal of evidential burden of proof, 133DB

Proposed paragraphs 133DB(1)(ba) and (bb) of the Credit Act establish a civil penalty for failure to provide a consumer with a comparison of equity projections and the consumer's expected aged care costs before entering into a reverse mortgage or providing other specified advice or services in relation to a reverse mortgage. Currently, subsection 133DB(2) of the Credit Act also makes it an offence to engage in conduct that breaches requirements in subsection 133DB(1). Proposed subsections 133DB(4A) and (4B) provide exceptions (offence-specific defences) to the civil penalty

and offence, providing that the offence does not apply if: another person has already given the required comparison; or circumstances prescribed by the regulations exist.

The criminal offence carries a maximum penalty of 50 penalty units and the civil penalty provision applies a civil penalty of 5000 penalty units.

Leaving to delegated legislation the prescription of circumstances in which it will be a defence to the offence or civil penalty provision of failing to comply with requirements to provide material to a consumer

As outlined above, this Bill is in response to the Government's economic response to the COVID-19 Pandemic. Given the unpredictability of outbreaks of the virus and related government regulatory responses, it is appropriate to leave to delegated legislation the prescription of circumstances in which it will be a defence to the offence or civil penalty provision of a licensee failing to comply with requirements to provide information to a consumer (133DB(1)(b) and (ba)). Equally, this regulation-making power provides the enduring flexibility for Government to support advancements in technology which achieve efficiencies for business while providing an appropriate level of consumer protection. This will help consumers and businesses safely transact during the COVID-19 pandemic while also facilitating long-term technological improvements in business communications which can benefit both consumers and licensees. As regulations, the prescribed circumstances would be subject to disallowance by the Parliament. Consistent with standard practice the Government envisages undertaking consultation before making any regulations under this power to minimise the risk of unintended consequences.

Using offence-specific defences (which reverse the evidential burden of proof)

Proposed subsection 133DB(4A) of the Credit Act provides for specific circumstances in which there will not be a contravention of subsection 133DB(1)(ba)-(bb) and (2). Subsection 133DB(4B) of the Credit Act provides for specific circumstances (prescribed in regulations) in which there will not be a contravention of subsection 133DB(1)(ba)-(bb) and (2). In a preceeding against a licensee in relation to 133DB, the defendant will bear the evidential burden that these specific circumstances occurred to successfully make out the defence.

The Attorney-General's Department's Guide to Framing Commonwealth Offences, Infringement Notices and-Enforcement Powers (September 2011) (the Guide) provides that a matter should only be included in an offence-specific defence (as opposed to being specified as an element of the offence), where it is peculiarly within the knowledge of the defendant and it would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter. It is intended to rely on this justification.

In accordance with the Guide, it is appropriate that the defendant bears the evidential burden for providing a defence. This is because it would be peculiarly within the mind of the defendant, and the defendant would be better positioned to readily adduce evidence, that they reasonably believed that another person had already shown the consumer in person the comparison described in subparagraph 133DB(1)(ba)-(bb) of the Credit Act and given the consumer a printed copy of the comparison; or circumstances prescribed by the regulations under subsection133DB(4B) existedthat justified the defendant not providing the consumer with a comparison of equity projections and the consumer's expected aged care costs before the defendant entered into a reverse mortgage or providing other specified services in relation to a reverse mortgage. The alternative would be that the prosecution has to adduce evidence to the contrary. In addition to this, the defendant only has an evidential burden which is less onerous than the legal burden.

It is intended to rely on this justification for the reversals of the evidential burden of proof in proposed subsections 133DB(4A) and (4B) of the Credit Act which provide exceptions (offence-specific defences) to the civil penalty and offence provisions. This reversal of the evidential burden of proof is proportional, necessary, reasonable and in pursuit of a legitimate objective.

Although it would have been technically possible to make amendments along the line described by the Committee, the Government's preferred approach was, and remains to provide for such details in the subordinate legislation for the reasons stated above.

Thank you for bringing your concerns to my attention.

Yours sincerely

THE HON JOSH FRYDENBERG MP

15 / 3 / 2021

Senator the Hon Michaelia Cash
Minister for Employment, Skills, Small and Family Business
Deputy Leader of the Government in the Senate

Reference: MC21-005963

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Parliament House
CANBERRA ACT 2600
Scrutiny.Sen@aph.gov.au

Dear Chair,

I am writing in response to Senate Scrutiny of Bills Committee's (the Committee) request for further advice on the National Emergency Declaration Bill 2020 and the National Emergency Declaration (Consequential Amendments) Bill 2020, as set out in its Scrutiny Digest 3 of 2021. I am responding to the Committee's request in my capacity as Acting Attorney-General.

In its Scrutiny Digest, the Committee sought further advice as to the appropriateness of amending certain sections of each of the Bills. I have enclosed additional information in response to the further matters raised by the Committee, which I trust will be of assistance.

I note that the Bills passed both Houses of the Parliament and received the Royal Assent in December 2020 and, accordingly, are now the National Emergency Declaration Act 2020 and the National Emergency Declaration (Consequential Amendments) Act 2020.

Yours sincerely

Senator Michaelia Cash
Acting Attorney-General
Minister for Employment, Skills and Small and Family Business
Deputy Leader of the Government in the Senate

Encl. Additional information in response to the Senate Standing Committee for the Scrutiny of Bills *Scrutiny Digest 3 of 2021.*

Perth
44 Outram Street, West Perth WA 6005
Ph 08 9226 2000

Canberra
Parliament House, Canberra ACT 2600
Ph 02 6277 7610

Response to Senate Standing Committee on the Scrutiny of Bills
Scrutiny Digest 3 of 2021

The Senate Standing Committee on the Scrutiny of Bills (the Committee) requests the Attorney-General's further advice in relation to a number of matters in the National Emergency Declaration Bill 2020 (at paragraphs [2.79] and [2.84]) and the National Emergency Declaration (Consequential Amendments) Bill 2020 (at paragraph [2.102]). These Bills have passed both Houses of Parliament and received Royal Assent on 15 December 2020.

The Government is continuing to consider opportunities to strengthen and improve frameworks relating to the management of national emergencies, including through the Senate Standing Committee on Legal and Constitutional Affairs' inquiry into the operation of the *National Emergency Declaration Act 2020* (which is due to report by 30 June 2021). This will allow further consideration to be given to the amendments proposed by this Committee, as well as engagement with key stakeholders, before any concluded views are reached.

The following information is also provided in response to the Committee's requests for more detailed advice.

National Emergency Declaration Act 2020 (NED Act)

Power for delegated legislation to modify primary legislation (Henry VIII clause)

The Committee reiterated its request for advice as to the appropriateness of amending the NED Act to provide that:

- determinations made under section 15 cease to be in force after three months, and
- before making a determination under section 15, a minister must be satisfied that Parliament is not sitting and is not likely to sit within two weeks after the day the determination is made.

In its *Scrutiny Digest 18 of 2020*, the Committee observed that a determination made under section 15 will cease either on the day specified in the determination or may continue while a national emergency declaration is in force (including any extensions of the period in which the declaration is in force). This approach was intended to ensure that Commonwealth support could be provided without interruption and with certainty in an emergency deemed to be of national significance, including where a declaration is extended because the emergency is ongoing beyond the initial three month period.

In light of the Committee's comments, consideration will be given to whether it is appropriate to amend the NED Act to include further safeguards around the making of determinations under section 15, including through time limitations, while maintaining the policy objective of the provision to empower ministers to reduce 'red tape' requirements in legislation where this would benefit the public, or a section of the public, during or following a national emergency.

Tabling of reports

The Committee reiterated its request for advice as to the appropriateness of amending paragraph 17(4)(a) of the NED Act to provide that reports on the exercise of powers and the performance of functions in relation to a national emergency declaration must be given to the Minister responsible for administering the NED Act as soon as practicable, and in any case not later than 14 days after the national emergency declaration ceases to be in force.

The Committee also reiterated its request for the Attorney-General's advice as to the appropriateness of amending subsection 17(5) of the NED Act to provide that:

- the reports must be tabled in each House of the Parliament as soon as practicable, and in any case not later than 14 days after the Minister receives the reports, and
- the reports are to be presented in accordance with procedures in each House for the presentation of documents out of sitting in circumstances where the reports are ready for presentation, but the relevant House is not sitting.

As noted by the Committee, section 17 of the NED Act includes requirements for relevant Ministers to report on the exercise of powers or the performance of functions under national emergency laws, and provides timeframes and presentation requirements for those reports. These reporting requirements were included as an important safeguard to ensure that national emergency declarations and the powers and functions that may be used once a declaration is in force are effective, proportionate and subject to appropriate oversight.

In light of the Committee's comments, consideration will be given to the appropriateness of amending the NED Act to provide for more specific requirements around the tabling and presentation of reports to ensure that there is appropriate Parliamentary accountability, particularly outside of sitting periods.

National Emergency Declaration (Consequential Amendments) Act 2020 **(Consequential Amendments Act)**

Significant matters in non-disallowable delegated legislative instruments

The Committee reiterated its request for advice as to the appropriateness of amending the *Telecommunications Act 1997* to:

- provide that an emergency declaration made under subsection 313(4D) is subject to parliamentary disallowance; and
- set out at least high-level guidance in relation to when an emergency may be declared under subsection 313(4D).

The intention of the amendments to the *Telecommunications Act 1997* (as amended by the Consequential Amendments Act) is to provide a clear legislative basis for requiring telecommunications providers to give the Commonwealth, states and territories such help as is reasonably necessary during emergencies. These amendments provide industry with a clear legislative basis for providing assistance and ensure they do not incur civil liability while doing so.

Subsection 313(4D) is intended to allow the Minister to declare emergencies where, in all of the circumstances, it is appropriate that industry participants be subject to a duty to give such help as is reasonably necessary for the purposes of preparing for, responding to or recovering from the emergency. Section 313(4D) would enable the Minister to act rapidly in unforeseen emergencies that, while serious, are not subject to a national declaration or state or territory emergency or disaster declaration, where the Minister would not otherwise be able to leverage the capability of carriers.

As noted by the Committee, subsection 313(4F) of the NED Act provides that while a section 313(4D) declaration is a legislative instrument, it is not subject to disallowance. This exemption from disallowance is intended to provide certainty and ensure that telecommunications providers can act expeditiously and with confidence that their assistance will not incur civil liability where circumstances are rapidly evolving.

Further consideration will also be given to whether high-level guidance could be provided in relation to when an emergency may be declared under subsection 313(4D) to provide additional certainty to the Parliament as well as carriers, carriage service providers and carriage service intermediaries about circumstances in which authorities may assistance.

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

Ref No: MC21-005020

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
scrutiny.sen@aph.gov.au

Dear Senator

I refer to correspondence dated 4 February 2021 from Mr Glenn Ryall, Committee Secretary, of the Senate Standing Committee for the Scrutiny of Bills (the Committee), regarding the Committee's consideration of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

As set out in the Committee's Scrutiny Digest No. 2 of 2021, the Committee has requested additional information on the Bill. I have considered this request and my response is provided at Attachment A.

I thank the Committee for the opportunity to clarify these matters, and for its important work in considering legislation before Parliament.

I trust that the information provided will assist the Committee in its consideration of the Bill.

Yours sincerely

PETER DUTTON 23/02/21

Attachment A

Response to the Senate Standing Committee for the Scrutiny of Bills - *Scrutiny Digest 2 of 2021*

Security Legislation Amendment (Critical Infrastructure) Bill 2020

Significant matters in delegated legislation

The regulatory framework that would be established by the Bill relies on delegated legislation where necessary, and often to facilitate for the specific detail of requirements in the Bill be flexible and adjustable in order to minimise regulatory impost on business while maintaining an appropriate security framework. The Minister for Home Affairs is not permitted, when making rules, to exceed the principles set out in the primary legislation and all rules are subject to parliamentary scrutiny and disallowance.

The Committee has requested further advice as to why it is considered necessary and appropriate to leave the matters identified in paragraph 1.82 of Scrutiny Digest 2/21 to delegated legislation. These matters will be dealt with in turn below.

a. *Relevant Commonwealth regulator*

Schedule 1 to the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill) proposes to insert a definition of 'relevant Commonwealth regulator' into section 5 of the *Security of Critical Infrastructure Act 2018* (the Act). The term is to be defined as:

(a) a Department that is specified in the rules; or
(b) a body that is:
(i) established by a law of the Commonwealth; and
(ii) specified in the rules.

This term is used to identify the relevant entity in respect of which certain functions and obligations to be introduced by the Bill attach, including:

- the recipient of annual reports in relation to critical infrastructure risk management programs (new paragraph 30AG(2)(b) of the Act)
- the body that must also be consulted by the Secretary prior to issuing a notice in relation to a statutory incident response plan (paragraph 30CB(4)(b)), cyber security exercise (paragraph 30CM(5)(b)), or vulnerability assessment (paragraph 30CU(3)(b)), and
- the body that may take certain enforcement actions in response to alleged contraventions of the regime, such as applying for civil penalty orders (subsections 49(2)-(3)) or accepting enforceable undertakings (subsections 49(3A)-(3B)).

A central principle underpinning the Bill is the need to avoid unnecessary regulatory burden. Where a Commonwealth regulator exists, or comes into existence, who is better positioned to regulate a particular class of critical infrastructure assets rules may be made to specify that regulator as a 'relevant Commonwealth regulator' for the purposes of the Act. Where appropriate, this will avoid the regulatory burden that

may arise from the responsible entity for an asset having to engage with multiple regulators as well as leveraging the sectoral expertise of particular regulators to the greatest extent possible.

The ability to specify regulators through rules provides the necessary flexibility to adjust, as appropriate, to evolving regulatory arrangements and ensure engagement with the Commonwealth Government is streamlined to the greatest extent possible. For example, as sector-specific rules to prescribe required content for critical infrastructure risk management programs are developed for the purpose of section 30AH through a co-design phase with industry, and refined into the future, there needs to be an appropriately flexible mechanism to ensure the most appropriate regulatory body can be identified in step with the evolving requirements specified in the rules.

However, it is important to note that the rules will exclusively be used to specify the most appropriate regulator in the Commonwealth, with the primary legislation conferring all relevant powers on that regulator. That is, and for the avoidance of doubt, the rules are only used in this context for the determination of administrative arrangements through which the Commonwealth can use those powers which are provided through the primary legislation.

b. Commonwealth owned critical infrastructure assets

The Government's general policy is that the measures and powers in this Bill should not apply to assets that are Commonwealth owned (except where owned by a government business enterprise). Commonwealth assets are already subject to detailed management and governance frameworks that are designed to maintain security and resilience. For example, Commonwealth assets are subject to the Protective Security Policy Framework (PSPF) which requires government departments and agencies to implement certain security measures. The Australian Government is also in a position to provide active assistance should these assets be subject to a serious cyber incident.

However, new subsection 9(2A) of the Act provides exceptions to this principle and outlines circumstances where Commonwealth owned assets may be critical infrastructure assets and, as a result, subject to certain measures and powers in the Bill.

Paragraphs 9(2A)(c)-(d) outline that an asset that is owned by the Commonwealth or a body corporate established by a law of the Commonwealth may be a critical infrastructure asset if:

- the asset is declared under section 51 of the Act to be a critical infrastructure asset (paragraph (c)), or
- the asset is prescribed by the rules for the purposes of paragraph 9(1)(f) (paragraph (d)).

These provisions are intended to futureproof the Act and ensure appropriate and necessary action can be taken under the Act should existing security measures for Commonwealth assets be ineffective or the unique nature of an asset render the existing security measures inappropriate. This approach aligns with, and relies on, the existing rule-making power in section 9 of the Act which was introduced to ensure that the law can adapt to changes in the threat environment and criticality of assets and infrastructure. Specifically, existing paragraph 9(1)(f) provides the Minister for Home Affairs with a rule making power to prescribe additional assets to

be a critical infrastructure asset.

c. *Definitions of certain critical infrastructure assets*

The Bill would allow the Minister for Home Affairs to make rules to prescribe requirements for, or specify an asset to be:

- a critical liquid fuel asset (new section 12A of the Act)
- a critical freight infrastructure asset (new section 12B)
- a critical freight services asset (new section 12C)
- a critical financial market infrastructure asset (new section 12D)
- a critical broadcasting asset (new section 12E)
- a critical banking asset (new section 12G)
- a critical insurance asset (new section 12H)
- a critical superannuation asset (new section 12J)
- a critical food and grocery asset (new section 12K), and
- a critical domain name system (new section 12KA).

Similar to the current approach taken in the Act, and wherever appropriate and reasonable, the Bill would rely on qualitative and quantitative criteria to define certain subcategories of critical infrastructure assets.

The nature of the assets to be captured in the Bill means that it is not always possible to include a static threshold in the primary legislation. Specifically, what is considered to be critical in some sectors will continue to evolve for a variety of reasons including changes to the market, technology and interdependencies.

In these circumstances, it is appropriate to have mechanisms available via delegated legislation to ensure that the definitions can evolve to guarantee that the measures and powers only apply to those assets that are considered to be critical in each sector at any given time.

Importantly, the primary legislation appropriately limits, and provides transparency over, the types of rules that can be made for each of the subcategories listed above by providing that the rules can only be made in relation to narrow and discrete parts of the definitions. This ensures that delegated legislation cannot be used to introduce any unnecessary, unrelated and inappropriate requirements. For example, in relation to liquid fuel refineries, new paragraph 12A(2)(b) of the Act ensures that any additional requirements provided in the rules are to capture those refineries as critical infrastructure assets that are critical to ensuring the security and reliability of a liquid fuel market.

The use of subordinate legislation in this context replicates the approach that was taken in the existing Act. For example, section 10 of the Act as currently in force allows the Minister for Home Affairs to make rules to prescribe requirements for an electricity generation station to be critical to ensuring the security and reliability of electricity networks or electricity systems in a particular State or Territory.

d. *Responsible entities*

New section 12L of the Act, as to be inserted by the Bill, would provide the definition of 'responsible entity' for each class of critical infrastructure asset. The definition has been separated into twenty five subsections representing the twenty-two classes of assets listed in the definition of critical infrastructure asset (see new subsection 9(1)),

as well as assets that are prescribed under paragraph 9(1)(f), assets that are declared to be critical infrastructure assets under section 51 by the Minister or assets that are systems of national significance. This definition replaces the current definition of responsible entity in the section 5 of the current Act, to accommodate the new classes of critical infrastructure assets.

The term 'responsible entity' is used throughout the Bill, and current Act, to identify the entity with whom certain obligations sit. Responsible entities are those entities with ultimate operational responsibility for the asset. These entities have effective control or authority over the operations and functioning of the asset as a whole (even if they do not have direct control over a particular part of the asset), and are in a position to engage the services of contractors and other operators.

Importantly, new section 12L of the Act would provide the Minister with the ability to make rules to override the responsible entity for a specific category of critical infrastructure asset identified in this section, and prescribe another entity to be the responsible entity. The assets that are likely to be captured by this Bill are operating in a constantly evolving environment which may change the type of entity that is considered to be the responsible entity. Further, the unique circumstances of a particular asset may mean that the responsible entity may differ from the responsible entity of general application for that class of critical infrastructure asset.

This rule making power provides the necessary flexibility to deal with changes to the operating environment of critical infrastructure assets and to ensure that the regulatory measures in the current Act (the Register obligations at Part 2) and in this Bill (specifically those contained at Part 2A and Part 2B) would continue to only apply to those entities that are best positioned to fulfil the obligations.

e. *Application provisions – Part 2 of the Act*

New paragraph 18A(1)(a) of the Act provides that the obligations relating to the Register of Critical Infrastructure Assets (the Register) at existing Part 2 of the Act apply to those critical infrastructure assets that are specified in the rules made by the Minister for Home Affairs, as well as assets that are currently regulated by the Act and assets privately declared under section 51 of the Act. This effectively works as an 'on switch' through which the Minister can ensure the obligations contained in the Part only apply in appropriate situations.

The consistent feedback from consultation with industry was that Government should consider the appropriateness of existing regulatory arrangements and only apply the obligations in the Act, and the Bill, to those assets that are not already subjected to similar and effective requirements or arrangements. The rule making power at paragraph 18A(1)(a) is a direct response to this feedback received from industry and allows the Government to take a nuanced approach to the application of the obligations in the Act which accommodates interactions with current and future regulatory regimes.

New subsection 18A(3) of the Act outlines that the rules may provide that, if an asset becomes a critical infrastructure asset, Part 2 of the Act does not apply to the asset during the period beginning when the asset became a critical infrastructure asset (paragraph (a)) and ending at a time ascertained in accordance with the rules (paragraph (b)). This is intended to provide the ability to offer a delayed commencement or 'grace period' in the future when an entity becomes a critical infrastructure asset to which Part 2 applies, allowing them a reasonable period to adjust their business. This will permit equality between assets that are regarded as

critical infrastructure assets at the time the rules are made who may benefit from a delayed commencement of those initial rules, and those who later become a part of that cohort.

Importantly, new section 18AA of the Act requires that the Minister consult on the content of any rules that are intended to be made under section 18A. Draft rules will be published on the Department of Home Affairs' website and persons will be invited to provide a submission in response to the proposal. Before making any rules, the Minister will be legislatively required to consider any submissions that were received. This provides additional transparency and ensures industry are afforded an opportunity to provide any information that may be relevant to the Minister's decision to make rules and activate the Register obligation.

f. Application provision – Part 2B of the Bill

Similarly to paragraph 18A(1)(a) – discussed above – new paragraph 30AB(1)(a) of the Act provides that the obligations relating to the critical infrastructure risk management program (the risk management program) in new Part 2A of the Act only apply to those critical infrastructure assets that are specified in the rules made by the Minister for Home Affairs. This effectively works as an 'on switch' through which the Minister can ensure that the obligations in this Part only apply in appropriate situations.

As noted above, during consultation sessions with industry, concerns were raised that the risk management program may duplicate existing obligations in some sectors. Industry encouraged Government to consider the appropriateness of any existing and relevant regulatory obligations, and suggested that the risk management program should only apply in circumstances where it is required.

The rule making power at new paragraph 30AB(1)(a) of the Act is a response to the feedback received from industry and allows the Government to take a nuanced approach to the application of the obligations in this Bill. As discussed at paragraph 532 of the explanatory memorandum, this rule making power allows for the risk management program to apply in relation to assets that are not already subjected to a comparable and effective obligation:

> *In determining whether to make rules to apply the obligations to certain critical infrastructure assets, the Minister is likely to consider whether any existing requirements or arrangements appropriately deliver the same outcomes as intended by the critical infrastructure risk management program. This reflects the range of regulatory obligations that exist in relation to the various critical infrastructure assets, as well the obligations that may exist in relation to future critical infrastructure assets that are identified, and the Government's commitment to avoid duplicating regulation. Should these alternative regimes be found wanting, this mechanism provides a default option to ensure the security objectives can be achieved.*

New subsection 30AB(3) of the Act outlines that the rules may provide that, if an asset becomes a critical infrastructure asset, Part 2A does not apply to the asset during the period beginning when the asset became a critical infrastructure asset (paragraph (a)) and ending at a time ascertained in accordance with the rules (paragraph (b)). This is intended to provide the ability to offer a delayed commencement or 'grace period' in the future when an entity becomes a critical infrastructure asset to which the Part 2A applies, allowing them a reasonable period

to adjust their business. This will permit equality between assets that are regarded as critical infrastructure assets at the time the rules are made who may benefit from a delayed commencement of those initial rules, and those who later become a part of that cohort.

Importantly, new section 30ABA of the Act requires that the Minister to consult on the content of any rules that are intended to be made under section 30AB. Draft rules will be published on the Department of Home Affairs' website and persons will be invited to provide a submission in response to the proposal. Before making any rules, the Minister will be legislatively required to consider any submissions that were received. This provide additional transparency and ensures industry are afforded an opportunity to provide any information that may be relevant to the Minister's decision to make rules and activate the Risk Management Program for an asset.

g. Requirements of critical infrastructure risk management programs

New section 30AH of the Act sets out the definition of a critical infrastructure risk management program. This definition is relevant to the obligations in new Part 2A of the Act, which require responsible entities for certain critical infrastructure assets to adopt, maintain, comply with, review and update a risk management program.

Subsection 30AH(1) provides that the plan must be a written program, the purposes that the program must achieve, and provides that the program must comply with such requirements (if any) as are specified in the rules. The Explanatory Memorandum for the Bill explains:

> *These rules will be used to provide further requirements on how the principles based obligations set out in subparagraphs [30AH] (1)(b)(i)-(iii) are to be implemented. Noting the array of critical infrastructure assets that may be subject to the obligation to adopt and maintain a critical infrastructure risk management program, now and into the future, this mechanism will be crucial for ensuring the program is implemented in a risk-based and proportionate manner for each industry sector while still achieving the desired security outcomes and avoiding any unnecessary burden. The Department will co-design these rules with industry and states and territories on a sector-specific basis.*

The requirements for risk management programs to be contained in the rules will outline matters that responsible entities must address to be compliant with the obligations in the Act, ensuring their actions are reasonable, proportionate and appropriate. These rules are expected to contain specific requirements which reflect the latest understanding of the threat environment, best practice security practices, industry maturity and the operating and regulatory context of critical infrastructure assets. Therefore, by their nature, these rules will need to be amended in a timely manner, as appropriate, to ensure they remain fit for purpose. Further, providing this degree of flexibility, while ensuring that the significant elements of the regime are set out in primary legislation, would enable the Government to achieve its objective of ensuring robust security practices are in place which do not impose undue regulatory burden.

This approach will also remove complexity from the regulatory framework by allowing sector-specific rules to be developed which address the specific circumstances of particular classes of assets, and as a result reducing unnecessary regulatory burden. This simplified approach can also be expected to ultimately increase the level of understanding about responsibilities and obligations and, ultimately, compliance with regulatory expectations.

h. Requirements for reports notifying of cyber security incidents

New Part 2B of the Act sets out obligations on responsible entities for certain critical infrastructure assets to notify the Government of particular cyber security incidents. Paragraphs 30BC(1)(c) and 30BD(1)(c) will provide that the respective report relating to the cyber security incident must include such information (if any) as is prescribed by the rules. The ability for the rules to set out such matters is necessary and appropriate for ensuring that the appropriate details of the incident are provided to Government while retaining flexibility to adjust the requirements to adapt to changes over time. These changes may include technological changes which alter industries ability to detect and analyse compromises as well as particular indicators the Government may require to visibility to facilitate the necessary analysis of the reports. This flexibility in the procedural requirements associated with these reports will allow the Government to avoid undue regulatory impost associated with reporting cyber security incidents.

i. Enhanced Cyber Security Obligations

The Bill provides that rules may be made for the following purposes relevant to the enhanced cyber security obligations in new Part 2C of the Act:

- Paragraph 30CJ(1)(e) – An incident response plan must comply with requirements (if any) which are specified in the rules.
- Paragraph 30CN(1)(f) – A cyber security exercise must comply with requirements (if any) which are specified in the rules.
- Paragraph 30CS(c) – An evaluation report, in relation to a cyber security exercise that was undertaken in relation to a system of national significance must comply with requirements (if any) which are specified in the rules.
- Paragraph 30CY(1)(e) – A vulnerability assessment must comply with requirements (if any) which are specified in the rules.
- Paragraph 30DA(c) – A vulnerability assessment report, in relation to a vulnerability assessment that was undertaken in relation to a system of national significance must comply with requirements (if any) which are specified in the rules.

It is necessary and appropriate to allow for administrative components of the plans, exercises, reports, and assessments to be specified by rules in order to allow the requisite flexibility to adjust procedural matters in order to avoid undue regulatory burden on industry. The rules however do not alter the purposive components of the respective definitions, but merely permit rules to be made where necessary to supplement the definitions with necessary detail.

Incorporation of external materials existing as in force from time to time

Schedule 1 of the Bill proposes to introduce new subsection 30AN(3) which provides, for rules made for the purposes of section 30AH, that:

> *Despite subsection 14(2) of the* Legislation Act 2003, *the rules may make provision in relation to a matter by applying, adopting or incorporating, with or without modification, any matter contained in a standard proposed or approved by Standards Australia as in force or existing from time to time.*

In effect, rules made to specify requirements for a critical infrastructure risk

management program may refer to the latest version standards proposed or approved by Standards Australia.

The Committee has requested further advice as to:

- **whether standards incorporated into the rules will be made freely available to all persons interested in the law, and**
- **further detail as to why it is considered necessary and appropriate to apply the standards as in force or existing from time to time, rather than when the instrument is first made.**

A common request from industry throughout the consultation process on this Bill was that the framework should, wherever possible, be consistent, and evolve, with existing industry best practice in order to reduce regulatory burden while achieving the desired security outcomes.

The provision in new subsection 30AN(3) of the Act is included to allow for the direct recognition of accepted and reputable standards. Standards Australia is a peak standards development body – developing standards, or adopting international standards, across a range of topics which represent best practice specifications, procedures and guidelines. Therefore a mechanism to facilitate the incorporation of such standards meets the expectation that the regulatory framework reflects best practice and minimises regulatory impost on industry.

The underlying objective of new Part 2A of the Act is to ensure current and appropriate risk management programs are in place for critical infrastructure assets, and therefore it is vital that any requirements for such programs adapt overtime to changing security contexts. In light of this, the provision also recognises that these standards are regularly reviewed and updated to keep pace with emerging technology, risks, threats, etc., ensuring that the regulatory framework remains up to date and fit for purpose. A requirement to update the rules every time a specified standard is changed would be administratively burdensome and would likely result in the law falling behind industry best practice which is at odds with the principles underpinning the reforms.

Nevertheless the use of this provision will depend on the outcome of the co-design process the Government has committed to undertake with industry in developing the rules. Importantly, section 30AH permits rules to be made for different purposes to support the risk management program obligations.

Firstly, the rules may be used to provide 'safe harbour' by deeming certain actions to meet the obligations in the Act. Rules made for the purposes of subsection 30AH(9) may specify action that is deemed to be action that minimises or eliminates any material risk that the occurrence of a specified hazard could have a relevant impact on the asset. In practice, this would allow rules to be made which deem specified action, such as compliance with a particular standard, to meet aspects of the obligation. However, the entity would be free take alternative actions so long as they can ultimately demonstrate that their legal obligations have been met. In effect, compliance with standards specified in these types of rules is not mandatory as the entity will be free to pursue an alternative approach to ensuring regulatory compliance.

Alternatively, the rules may be used to establish mandatory requirements. For example, rules made for the purposes of paragraph 30AH(1)(c) may establish mandatory requirements for the critical infrastructure risk management program. The

Government recognises the importance of accessibility for mandatory requirements for fair and effective functioning of the regime.

It is not possible to pre-empt the outcome of industry co-design, and potential application, adoption or incorporation of standards and the accessibility of those standards. However, if rules that incorporate standards are being considered, there are important safeguards to ensure the costs associated with accessing those standards is considered by the Minister.

Firstly, new section 30AL of the Act requires the Minister to conduct consultation prior to making or amending rules. Should consultation not be possible due to the immediacy of circumstances, section 30AM provides that consultation must occur as part of a review of the rules.

Secondly, new paragraphs 30AH(6)(b) and (c) of the Act require the Minister to have regard to the costs that are likely to be incurred by responsible entities in complying with rules specifying requirements for a critical infrastructure risk management program, and the reasonableness and proportionality of the requirements. This mandates consideration of issues such as costs associated with accessibility. Should the Minister consider making rules in this context which apply, adopt or incorporate standards proposed or approved by Standards Australia, consideration will be given to the accessibility of those standards by the regulated population and other persons interested in the law, such as responsible entities for assets which may become critical infrastructure assets in the future.

Finally, the Government has committed to undertaking regulatory impact statements for rules made for the purposes of new section 30AH of the Act. This provides another opportunity for the industry to advise Government of any cost implications of the incorporation of standards.

Ultimately, the accessibility of the standards will need to be considered on a case by case basis. The Minister or relevant Commonwealth regulator may consider entering into an agreement with Standards Australia to facilitate relevant standards being made available at no direct cost to users for example, on request or via the portal on the Department's Critical Infrastructure Centre's website. Such arrangements are supported by the Standards Australia Distribution and Licensing Policy Framework.[1] Standards Australia are also currently developing new online products planned to be rolled out in 2021. These include new paid subscription models to access to standards. This model follows other product and subscription models for other forms of online content where users pay smaller, ongoing fees for a range of digital services across a wider range of products. These models seek to provide greater value to consumers through the provision of increased choice, accessibility and use via digital technologies. Alternatively, and in light of the factors discussed above, it may be considered appropriate for the regulated population to incur the costs of accessing the standards.

Without prejudicing consultation, and therefore without the necessary context, the safeguards included in the legislation provide an appropriate balance of supporting industry's desire for existing standards to be incorporated and mandating processes to ensure any costs to industry or Government are considered. It is considered any

---

[1] Standards Australia, *Distribution and Licensing Policy Framework*, November 2019, accessible at <https://www.standards.org.au/getattachment/8b8551a9-e580-4dce-a6d7-6b953b44bf31/Standards-Australia-Distribution-and-Licensing-Policy-Framework-2019.pdf.aspx?lang=en-AU>.

potential regulatory costs associated with this approach would be minimal compared to the costs associated with generating new standards despite existing, and widely accepted, standards.

Broad delegation of administrative power

Sections 23 and 53 of the *Regulatory Powers (Standard Provisions) Act 2014* (the Regulatory Powers Act) provide that an authorised person may be assisted by other persons in exercising powers or performing functions or duties under Part 2 (monitoring powers) and Part 3 (investigation powers), respectively, if that assistance is necessary and reasonable, and another Act empowers the authorised person to be assisted. A person assisting may exercise these powers or perform these functions for the purposes of assisting an authorised person to monitor a provision or to investigate the contravention of a civil penalty or an offence provision. New subsections 49A(14) and 49B(12) of the Act respectively empower an authorised person to be assisted by other persons.

The Committee has requested further advice as to:

- **why it is considered necessary and appropriate to confer investigatory powers on any 'other person' to assist an authorised person; and**
- **whether the bill can be amended to require that any person assisting an authorised person have the expertise appropriate to the function or power being carried out.**

The amendments to the Act in the Bill do not confer or delegate any investigatory powers to the 'person assisting'. Instead, under subsections 49A(14) and 49B(12), an authorised person may be assisted by 'other persons', where necessary and reasonable, in that authorised person's exercise of investigatory powers.

These provisions are directly linked to the Regulatory Powers Act. As the Explanatory Memorandum for the Regulatory Powers (Standard Provisions) Bill 2014 explains, under paragraph 53(1)(a) of that Act, the role of a person assisting an authorised person is to undertake assistance tasks at the direction of an authorised person. Further, an 'other person' can only assist if it is necessary and reasonable to do so. The assisting person must act under the direction of the authorised person and any valid actions of the person assisting will be taken to be those of the authorised person.

The intent of these provisions is that a person assisting an authorised person does not themselves exercise any powers or functions delegated or conferred under the Act but operates under direction and it is the authorised person who would be exercising the investigatory powers under the Regulatory Powers Act. Under the Act, as amended by the Bill, it is considered necessary and reasonable for an authorised person exercising monitoring and investigation powers to be assisted by another person, for example, for administrative or practical assistance with evidential material on the premises. It is envisaged that a person assisting an authorised person would be undertaking (at the direction of an authorised person) tasks such as assisting to make copies of voluminous records or documents and carrying evidential material seized from the premises.

Given a 'person assisting' does not exercise any delegated or conferred powers or functions under the Act, it is not necessary for the Act (as amended by the Bill) to require that a person assisting have the appropriate knowledge and expertise.

THE HON PETER DUTTON MP
MINISTER FOR HOME AFFAIRS

Ref No: MS21-000237

Senator Helen Polley
Chair
Senate Scrutiny of Bills Committee
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Chair

Thank you for the Senate Scrutiny of Bills Committee's letter dated 29 January 2021 requesting my response in relation to the scrutiny of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020.

I note the Committee has sought further information regarding the bill to address some of its scrutiny concerns.

My response for the Committee's consideration is attached. I appreciate the extension until 1 March 2021 in which to provide this response.

Yours sincerely

PETER DUTTON 19/02/21

Response to the Senate Standing Committee for the Scrutiny of Bills

Scrutiny Digest 1 of 2021

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

Authorisation of coercive powers

1.109 The committee requests the minister's detailed advice as to:

a. why categories of persons eligible to issue data disruption and network activity warrants should not be limited to persons who hold judicial office

In the Bill, the power to issue data disruption warrants and network activity warrants is conferred on an eligible judge or a nominated Administrative Appeals Tribunal (AAT) member. These issuing authorities may grant the warrant if (amongst other things) they are satisfied that there are reasonable grounds for the suspicion founding the application for the warrant. This independent scrutiny of warrant applications is an important mechanism in ensuring that only warrants that are reasonable and proportionate are issued.

AAT members have the experience and skills necessary to issue data disruption warrants and network activity warrants

Both AAT members and judges play critical roles as independent decision-makers in authorising investigatory powers in the current regimes in the *Surveillance Devices Act 2004* (SD Act), as well as in the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Nominated AAT members issue surveillance device warrants and computer access warrants under the SD Act, and have played a key role in issuing interception under the TIA Act since 1998. The skills and experience of AAT members make them suitable to assess applications for data disruption warrants and network activity warrants, and whilst doing so, to make independent decisions on the compliance of those applications with the legal requirements in the Bill.

To be nominated as an AAT member for the purposes of issuing warrants under the SD Act, a person must have been enrolled as a legal practitioner for at least five years. In accordance with the existing framework, the Bill recognises that the complex decision-making involved in authorising the new powers in the Bill requires the independence offered by the AAT members and judges who already issue other warrants under those Acts and have the skills and experience to do so.

AAT members are independent decision-makers

The power to issue warrants is conferred on issuing authorities in their personal capacity (*persona designata*) as a means of ensuring accountability in the course of a sensitive investigation or law enforcement procedure. *Persona designata* functions are not an exercise of the formal judicial or administrative powers of a court or tribunal. Rather these issuing authorities are acting as independent decision-makers.

The AAT is not independent of government in the same way that the judiciary is the subject of a separation of powers (though some members of the AAT are also judges). Rather, the AAT's independence arises from its role in reviewing the merits of administrative decisions made under Commonwealth laws.

The independence of the AAT is also demonstrated in the process for the termination of a member's appointment. AAT members who are not judges can only have their appointment terminated by the Governor-General, and this termination can only be made on specific grounds, such as proven misbehaviour or the inability to perform duties.

The independence of AAT members exercising *persona designata* functions is strongly safeguarded. AAT members are afforded the same protection and immunity as a Justice of the High Court of Australia, and they must provide written consent prior to being authorised to perform *persona designata* functions. Consent also serves to protect an AAT members' independence and autonomy to decide whether or not to exercise *persona designata* powers.

Review of administrative decisions

In the unlikely event of unlawful decision-making, Australian courts will retain their jurisdiction to review administrative decisions, including any decision to issue a warrant, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of subsection 39B(1) of the *Judiciary Act 1903*, or under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). There is an error in the human rights compatibility statement in the explanatory memorandum supporting the Bill, which states that the Bill excludes judicial review under the ADJR Act. This is incorrect, and the human rights compatibility statement will be amended accordingly. These judicial review mechanisms ensure that an affected person has an avenue to challenge the decisions to issue warrants made by any issuing authorities, including a nominated AAT member.

As such, the Government maintains that the persons eligible to issue data disruption warrants and network activity warrants should not be limited to only judicial officers, but should include nominated AAT members, in line with the existing legislation.

b. why it is considered necessary and appropriate to issue each type of warrant for an initial 90-day period as opposed to a shorter period

Each of the three new warrants proposed in the Bill can be issued for an initial period of up to 90 days. As stated in the explanatory memorandum, this is in line with the period for which surveillance device warrants and computer access warrants can be issued in the SD Act. Maintaining consistency in the length of time warrants can be issued allows warrants to be sought in conjunction with one another, and executed during the course of the same investigation or operation.

Importantly, this does not mean that all warrants will be issued for a period of 90 days. The period for which a warrant is in force will be determined by the issuing authority on a case-by-case basis depending on the circumstances of the application.

Data disruption warrants

As noted by the Committee, the explanatory memorandum states that an initial period of up to 90 days for execution of a data disruption warrant is intended to allow for complex, long-term operations. As with all warrants in the SD Act, as well as the other warrants proposed by this Bill, investigations and operations that utilise data disruption warrants will often involve multiple targets that are moving across computer networks, whose identities and locations may be obfuscated by the use of anonymising technologies. The disruption of data must be carried out in a targeted manner where any damage or loss of data is proportionate and necessary, an assessment of which takes agencies time to consider. In addition, as with the other warrants in the Bill, data disruption warrants are necessarily covert. This means that agencies need to assess the best time and methods to undertake the activities authorised in the warrant in accordance with circumstances that allow the concealment of these activities.

Network activity warrants

As an intelligence collection tool, it is appropriate for network activity warrants to be in force for an initial period of up to 90 days. The purpose of these warrants is to target criminal networks of individuals that may be comprised of a large number of unknown individuals. Criminal networks, particularly organised crime groups, will often use the dark web and anonymising communications platforms to evade law enforcement surveillance. Moreover, the composition of the network is likely to change from time to time as new participants enter the group and use multiple devices to conduct their criminal activities.

In order to infiltrate these complex and evolving networks, law enforcement will be required to deploy computer access techniques which may take a significant period of time to execute successfully. A maximum period of less than 90 days would, in many cases, not provide law enforcement with sufficient time to obtain access to the computers targeted by the warrant, and collect intelligence on the individuals using those devices, and ensure the operation remains covert.

Account takeover warrants

As with data disruption warrants and network activity warrants, investigations in which account takeovers will be used will often be complex and lengthy operations, requiring covert infiltrations. For

example, the target accounts may belong to high-level forum members who may have hundreds of contacts within forums, which means that there would be multiple avenues of inquiry to pursue during the course of an account takeover.

Moreover, account takeover warrants are designed to be used in conjunction with controlled operations under Part IAB of the Crimes Act. The account takeover warrant would authorise the taking control of the person's account and locking that person out of the account. Any other activities, that would involve engaging in controlled conduct, would be performed under the accompanying controlled operation. Noting the high likelihood that the two powers will be used in conjunction, it is important that the time period for which agencies are authorised to conduct the authorised activities is aligned. An application for a controlled operation can also seek for the authority to be in place for a period of up to three months.

c. why the bill does not require, in relation to all warrants, that the issuing authority must consider whether the warrant is proportionate having regard to the nature and gravity of the offence and the likely value of the information or evidence sought to be obtained, as well as the extent of possible interference with the privacy of third parties

In deciding whether to issue each of the warrants in the Bill, there are certain matters which the issuing authority must take into account. These considerations have been specifically designed with regard to the objective and contemplated operation of each of the warrants.

Proportionality test for data disruption warrants

In order to issue a data disruption warrant, the Judge or AAT member must be satisfied that, amongst other things, the disruption of data authorised by the warrant is justifiable and proportionate with regard to the offences targeted. This is to ensure that in considering whether to issue the warrant, the issuing authority weighs up the benefits of targeting the particular offences that the proposed data disruption seeks to frustrate, with the likely effect that data disruption could have beyond frustrating those offences. Satisfaction that the execution of the warrant is justifiable assists in satisfying the requirement under international human rights law that the limitation on the right to privacy is reasonable and not arbitrary.

A specific requirement that the issuing authority consider the privacy of third parties is not appropriate in the context of data disruption warrants, even though it is appropriate in the context of other electronic surveillance warrants the purpose of which is the gathering of evidence. Data disruption warrants are for the purpose of frustrating criminal activity, including preventing further harm to victims, stopping criminal offences occurring, and re-directing activity so that agencies can take appropriate action. It will not always be possible, at the time of applying for the warrant, for an agency to estimate the full extent to which activity required to undertake data disruption is likely to have an impact on third parties. In light of this, rather than providing for an express privacy consideration the Bill contains a mandatory condition that the issue of a data disruption warrant be justified and proportionate having regard to the offences targeted. To further ensure that these warrants are proportionate to the activity they authorise, the issuing authority must consider the existence of any alternative means of frustrating the criminal activity.

Proportionality test for network activity warrants

In order to issue a network activity warrant, the Judge or AAT member must consider whether the activities authorised by the warrant are proportionate to the likely value of intelligence to be collected, as well as the extent to which the warrant is likely to result in access to data of persons lawfully using a computer. The purpose of network activity warrants is to allow the AFP and the ACIC to target the activities of criminal networks to discover the scope of criminal offending and the identities of the people involved. Due to the complexity of the threats posed by cyber-enabled crime, it is unlikely that agencies will know the identity or location of the offenders involved in the commission of offences to which the network activity warrant is related.

Network activity warrants are an intelligence collection tool and the information collected cannot be used in evidence in criminal proceedings. As such, the considerations for issue of a network activity warrant differ from those in relation to warrants that are issued for the purposes of gathering evidence (for example, computer access warrants in the SD Act). Intelligence collection by its nature is less

targeted than evidence-gathering, and will necessarily involve a larger scope for its target. Using a network activity warrant, the AFP or ACIC may need to collect intelligence on a large number of unknown devices, the users and owners of which are not able to be identified or located, before seeking more targeted warrants that authorise gathering evidence (such as computer access warrants under the SD Act). It will be difficult, if not impossible, for an issuing authority to assess the privacy implications for multiple unknown persons to a sufficient degree to meet the threshold of a specific requirement to consider the privacy of third parties. In any event, the issuing authority must still consider the extent to which the execution of a network activity warrant is likely to result in access to data of persons who are lawfully using a computer. The proportionality test requires that the issuing authority weigh up the anticipated value of the intelligence sought with the activities authorised by the warrant. This ensures that the issuing authority must balance the utility of the network activity warrant in obtaining information about the criminal network against the scale, scope and intrusiveness of the activities authorised by that warrant. To further ensure that these warrants are proportionate to the activity they authorise, the issuing authority must consider the existing of any alternative or less intrusive means of obtaining the information sought.

Privacy consideration for account takeover warrants

For account takeover warrants, the magistrate must consider the extent to which the privacy of any person is likely to be affected. An explicit privacy consideration is appropriate for the issue of account takeover warrants, as it is a targeted evidence gathering power. This is consistent with the approach for existing electronic surveillance powers, such as those in the SD Act.

When deciding whether to issue the warrant, the magistrate must also have regard to the nature and gravity of the alleged offence which founded the application for the warrant. This may involve consideration of the seriousness of the offence and the scale at which the offence has been, or will be, committed.

Consideration of this matter ensures that the magistrate will be able to assess the reasonableness and proportionality of executing the warrant in the circumstances. If the offence to which the warrant is sought is not sufficiently serious to justify the conduct of an account takeover warrant and its impact on privacy, the magistrate may decide not to issue to warrant.

d. the nature of the defects or irregularities that will not lead to the invalidity of actions done under a purported warrant or emergency authorisation

The Bill provides that where information is purportedly obtained under a warrant and there is a defect or irregularity in relation to the warrant, then obtaining the information is taken to be valid if, but for the defect or irregularity, the warrant would be sufficient authority for obtaining the information. These are proposed amendments to existing section 65 of the SD Act, and proposed new section 3ZZVY of the Crimes Act.

A defect or irregularity in relation to a warrant is a minor error in the warrant. Section 65 of the SD Act and proposed new section 3ZZVY of the Crimes Act do not apply to substantial defects that go to the operation, extent or effect of the warrant. A defect or irregularity in this context could not be one that would cause the warrant to operate beyond the scope of what is authorised by the legislation.

The intent of these amendments is not to undermine the oversight and scrutiny of warrant applications, by allowing substantially defective or irregular warrants to remain valid. Rather, these amendments are intended to minimise lawfully obtained information being deemed invalid or unusable solely on the basis of a minor defect or irregularity in an otherwise valid warrant. Some examples of a defect or irregularity in the warrant may include a typographical error, misprint or minor damage to a written form warrant. Such defects or irregularities are minor, and would not affect the warrant's intended operation.

Use of coercive powers without a warrant

1.119 The committee requests the minister's detailed advice as to:

a. why it is considered necessary and appropriate to enable law enforcement officers to disrupt and access data or takeover an online account without a warrant in certain emergency situations (noting the coercive and intrusive nature of these powers and the ability to seek a warrant via the telephone, fax or email)

In emergency circumstances, the activities permitted by a data disruption warrant and an account takeover warrant can be authorised internally. Such authorisations are only available where (amongst other considerations) there is an imminent risk of serious violence to a person or substantial damage to property. The circumstances must be so serious, and the matter of such urgency, that disruption of data or account takeover activity is immediately necessary for dealing with that risk.

The ability to disrupt data under a data disruption warrant, and the ability to take control of an account under an account takeover warrant in emergency situations is important for ensuring that the AFP and the ACIC will be able to respond to rapidly evolving and serious threats in a timely and effective manner. Emergency authorisations are available only in the most extreme circumstances where it is not practicable to apply for a warrant, including applying for a warrant remotely or with an unsworn application. For this same reason, it is essential that applications for emergency authorisations can be made orally, in writing, or by telephone, fax, email or any other means of communication, as they are for situations in which officers need to be able to take immediate action.

Emergency authorisations do not amount to warrants being internally issued. Within 48 hours of an emergency authorisation being given, approval must then be sought by application to a Judge or AAT member (for data disruption) or a magistrate (for account takeovers). At this time, the issuing authority must take into account strict issuing criteria, such as the nature and risk of serious violence to the person and the existence of alternative methods that could have helped to avoid the risk, as well as an assessment of whether or not it was practicable in the circumstances to apply for a warrant instead of an authorisation This provides independent scrutiny of decisions to authorise data disruption and account takeovers in emergency situations.

The use of emergency authorisations for covert investigatory activity is not new. In the SD Act, emergency authorisations have been available for the use of surveillance devices since 2004 (subsection 28(1) of the SD Act), and for access to data held in a computer since 2018 (subsection 28(1A) of the SD Act). In practice, emergency authorisations are utilised very rarely and only in the most serious of circumstances. For example, in the *Surveillance Devices Act 2004 Annual Report for 2019-20*, no law enforcement agencies made an emergency authorisation for the use of surveillance devices or to access to data held in a computer.

The availability of account takeover powers under an emergency authorisation is proportionate and necessary to ensure that these powers can be used where there is an imminent risk of serious violence to a person or substantial damage to property, and urgent action must be taken to deal with that risk.

Emergency authorisations are not available for the activities permitted by the network activity warrant noting the purpose of this warrant in gathering intelligence, rather than responding to time-critical situations.

b. the appropriateness of retaining information obtained under an emergency authorisation that is subsequently not approved by a judge or AAT member

The Bill provides that an eligible Judge or nominated AAT member (for data disruption, new subsection 35B(4) of the SD Act), or magistrate (for taking control of an online account, new subsection 3ZZVC(4) in the Crimes Act) may order that any information obtained from or relating to the exercise of powers under an emergency authorisation, or any record of that information be dealt with in a manner specified in the order. However, the Judge, AAT member or magistrate may not order that such information be destroyed. These provisions reflect existing subsections 35(6) and 35A(6) in the SD Act in relation to emergency authorisations for the use of surveillance devices and access to data held in a

computer. As noted by the Committee, the Explanatory Memorandum states that this Bill provides that this information cannot be destroyed because it 'may still be required for a permitted purpose [under the Act] such as an investigation'. As referenced in the Explanatory Memorandum to the *Surveillance Devices Act 2004* (which introduced existing subsections 35(6)), an example of an investigation for which improperly obtained information should be able to be used, is an investigation into the improper surveillance itself. Further, it is important that information gathered under an emergency authorisation – including one that is not subsequently approved by a judge, AAT member or magistrate – is not destroyed, as destruction of that information may detract from effective oversight of agencies' use of the emergency authorisation powers.

Information gathered as part of an emergency authorisation (including one that is not subsequently approved) is considered 'protected information,' and is subject to strict use and disclosure provisions in both the SD Act (existing section 45) and Crimes Act (proposed new section 3ZZVH). Criminal liability is attached to the unauthorised use or disclosure of 'protected information' and this is another means by which the privacy of individuals will be protected.

c. the appropriateness of enabling law enforcement agencies to act to conceal any thing done under a warrant after the warrant has ceased to be in force, and whether the bill could be amended to provide a process for obtaining a separate concealment of access warrant if the original warrant has ceased to be in force

The Bill makes provision for the AFP and the ACIC to perform activities to conceal any thing done under a data disruption warrant, a network activity warrant and an account takeover warrant. Concealment activities may be carried out at any time while the warrant is in force or within 28 days after the warrant ceases to be in force, or at the earliest time after that 28 day period at which it is reasonably practicable to carry out those concealment activities. A period of longer than 28 days would be required, for example, where a computer being accessed under a network activity warrant is moved by the target and the agency must wait for it to be physically relocated and recovered.

Making provision for concealment activities allows an agency to prevent targets learning that they are under investigation and attempting to impact further efforts to gather evidence or intelligence about their activities. This is because undertaking surveillance activities under these warrants is likely to alter data, or leave traces of activity, on an electronic device or online account. This may allow targets to recognise the lawful intrusion by law enforcement agencies and effectively change the way they communicate for the purposes of evading detection. For example, recognition may lead to reverse engineering police capabilities and methodology leading to individuals avoiding using certain technologies or undertaking counter-surveillance activities.

Accordingly, the concealment of the execution of the warrants in the Bill is vital to the effective exercise of powers and maintaining the covert nature of the investigation or operation. In particular, it is appropriate that concealment activities are able to occur without additional external approval as the concealment activities are incidental to the granting of the original warrant. In the absence of a clear authority to conceal access under warrant, there is significant risk to the exposure of sensitive technologies and methodologies, and to law enforcement outcomes were targets to be notified that a warrant was in force against them.

Importantly, the measures are subject to limitations, safeguards and oversight mechanisms designed to ensure that concealment activities are only undertaken where reasonable, proportionate and necessary. For example, the AFP and the ACIC are required to notify the Inspector-General of Intelligence and Security (IGIS) that a thing was done to conceal access under a network activity warrant after the 28-day period following expiry of the warrant within 7 days after the thing was done (proposed section 49D of the SD Act).

Innocent third parties

1.136 The committee requests the minister's detailed advice as to the effect of Schedules 1-3 on the privacy rights of third parties and a detailed justification for the intrusion on those rights, in particular:

a. why proposed sections 27KE and 27KP do not specifically require the judge or nominated AAT member to consider the privacy implications for third parties of authorising access to a third party computer or communication in transit

There are certain activities which can be authorised by an issuing authority under a data disruption warrant or a network activity warrant which could potentially have an impact on the privacy of third parties. These activities include entering premises and accessing computers and communications in transit, as these could potentially be premises, computers and communications of third parties. Such activities, along with the others listed in sections 27KE (data disruption warrants) and 27KP (network activity warrants), are specifically listed in the legislation because they will often be essential tools in the execution of these warrants. No warrant can authorise activity beyond that which is listed unless it is reasonably incidental to carrying out those actions. Further protections have been inserted in subsections 27KE(7), 27KE(12) and 27KP(6) to ensure that data disruption warrants and network activity warrants cannot authorise other activities.

To safeguard any potential impact on the privacy of third parties, the Bill requires that the issuing authority undertake a proportionality test before deciding to issue a data disruption warrant or network activity warrant. These considerations are described in further detail in earlier answer above at 1.109(c), but are also summarised below.

Data disruption warrants

In order to issue a data disruption warrant, the Judge or AAT member must be satisfied that the activities authorised by the warrant are justified and proportionate with regard to the offences targeted. This is to ensure that the use of these warrants is proportionate to the alleged or suspected offending in all circumstances. In making this determination, the issuing authority may wish to take into account, for example, the scope of the warrant in terms of how many people are affected, the exact nature of the potential intrusion on people's private information, and whether that intrusion is justified by the serious nature of the criminality being targeted. Whilst it may be necessary to access information or property belonging to third parties in order to disrupt data, this must be proportionate to the frustration of the offences targeted. There are also strong protections and safeguards in place to ensure that information is protected and only used appropriately.

Network activity warrants

For a network activity warrant, the Judge or AAT member must consider whether the activities authorised by the warrant are proportionate to the likely value of intelligence to be collected, as well as the extent to which the warrant is likely to result in access to data of persons lawfully using a computer. Whilst it may be necessary to access information or property belonging to third parties, this must be proportionate to the value of intelligence that is collected, and there are safeguards associated with network activity warrants to further protect information.

b. why the requirement that the issuing authority be satisfied that an assistance order is justifiable and proportionate, having regard to the offences to which it would relate, only applies to an assistance order with respect to data disruption warrants, and not to all warrants

As the Committee notes, an eligible Judge or nominated AAT member must be satisfied that disruption of data held in a computer is justifiable and proportionate, having regard to the offences targeted, before granting an assistance order in support of a data disruption warrant. This is because the criterion upon which the granting of an assistance order is assessed reflects that of which the issuing authority must be satisfied when authorising the supporting warrant.

In order to issue a data disruption warrant, an eligible Judge or nominated AAT member must (amongst other things) be satisfied that there are reasonable grounds for the suspicion of the applicant that the disruption of data is likely to substantially assist in frustrating the commission of relevant offences. The eligible Judge or nominated AAT member must also be satisfied that the disruption of data authorised by the warrant is justifiable and proportionate, having regard to the offences targeted (subsection 27KC(1) of the SD Act).

These are similar matters to which an eligible Judge or nominated AAT member must be satisfied of when granting an assistance order in support of a data disruption warrant (subsection 64B(2) of the SD Act). Satisfaction of similar matters at the time of issuing the warrant and the granting of the assistance order ensures that any activity required by an assistance order does not extend beyond the scope of the underpinning warrant.

The same principles apply in relation to the granting of assistance orders supporting network activity warrants and account takeover warrants. Similar matters that must be satisfied at the time of issuing these warrants must again be satisfied at the granting of an assistance order.

In recognition of the impact on privacy of third parties, the issuing authority is required to have regard to certain specified matters when deciding whether to issue the warrant. For network activity warrants, this includes consideration of whether the activities authorised by the warrant are proportionate to the likely value of intelligence to be collected, as well as the extent to which the warrant is likely to result in access to data of persons lawfully using a computer. For account takeover warrants, this includes taking into account the extent to which the privacy of any person is likely to be affected.

Consideration of these matters will inform the issuing authority's decisions to issue warrants, including his or her satisfaction of the matters particular to that warrant and, in turn, inform decisions about whether to grant an assistance order. Ensuring that the issuing authority is required to be satisfied of justifiability and proportionality before a warrant can be issued or assistance order granted is intended to safeguard against any undue impact on privacy.

c. whether the breadth of the definitions of 'electronically linked group of individuals' and 'criminal network of individuals' can be narrowed to reduce the potential intrusion on the privacy rights of innocent third parties

The purpose of network activity warrants is to enable the AFP and the ACIC to better target criminal groups operating online. Network activity warrants will be an essential tool for collecting information about the constitution and methodologies of criminal organisations, and people participating in criminal groups. A key consideration in applying for a network activity warrant under new section 27KK is suspicion on reasonable grounds that a group of individuals is a criminal network of individuals.

A criminal network of individuals is a group of individuals who are electronically linked. An electronically linked group of individuals may be using a shared internet service in common, or may have established their own secure communications networks in order to communicate and conduct their activities. Whilst the number and identity of the group of individuals may not be known, there must be a link between two or more people who meet or communicate electronically. It is essential that the concept of 'electronically linked group of individuals' is broad enough to encapsulate individuals who do not identify as being in a criminal organisation or group, but who are nevertheless operating in a network. An 'electronic link' also accounts for the fact that people may not have a personal relationship with an individual who they are nonetheless communicating with. They do not have to have knowledge of each other's activities. This definition is deliberately broad to capture groups of individuals who, for example, are accessing an illicit dark web marketplace where they are unlikely to consider themselves as members, but rather customers, such as people who are paying to view the live streaming of child exploitation material.

In order for an electronically linked group of individuals to constitute a criminal network of individuals, one or more individuals in the group must have engaged, are engaging, or are likely to engage in conduct that constitutes a relevant offence, or have facilitated, are facilitating, or are likely to facilitate, another person's engagement in conduct that constitutes a relevant offence. The person whose engagement in criminal activity was facilitated by an individual in the group, may or may not be an individual in the group themselves. As noted by the Committee, there is no requirement that every

individual who is part of the criminal network is himself or herself committing, or intending to commit, a relevant offence. This deliberately captures those individuals who are, knowingly or unknowingly, facilitating engagement by another person in conduct constituting a relevant offence. It is important that the concept of 'criminal network of individuals' is broad enough to cover unwitting participants in criminal activity, so that this crucial intelligence can still be collected. For example, a criminal network of individuals may include an individual who owns an IT platform that is, without the knowledge of that person, being exploited by a criminal organisation for illegal purposes.

Use of information obtained through warrant processes

1.143 The committee requests the minister's detailed advice as to:

a. whether all of the exceptions to the restrictions on the use, recording or disclosure of protected information obtained under the warrants are appropriate and whether any exceptions are drafted in broader terms than is strictly necessary

All information collected under the warrants in this Bill is strictly protected. Information is broadly prohibited from being used or disclosed. Where there are exceptions to that prohibition, those exceptions are necessary either to enable the warrants to be effective, or to enable strong oversight and accountability mechanisms, or to enable proper and appropriate judicial processes to be carried out, or to enable information sharing necessary for agencies to carry out their functions or in emergency circumstances. The ability to use and disclose information has been designed to be limited to only that which is necessary.

Prohibition and offences

The Bill classifies data disruption warrant information as 'protected information' under the existing provisions in the SD Act, which currently govern information collected under other warrants in that Act, for example, computer access warrants.

Information gathered under an account takeover warrant is also classified as 'protected information'. This is a new concept in the Crimes Act introduced by the Bill, borrowing from the SD Act so that account takeover warrant information is governed by the same prohibitions and exceptions as most information under the SD Act, including data disruption warrant information.

There is also a prohibition on using and disclosing 'protected network activity warrant information', a new category of protected information introduced by the Bill into the SD Act. Protected network activity warrant information is information obtained under, or relating to, a network activity warrant including information obtained from the use of a surveillance device under a network activity warrant but not including information obtained through interception. This also includes any information that is likely to enable the identification of the criminal network of individuals, individuals in that network, computers used by that network, or premises at which computers used by that network are located. Information that was obtained in contravention of a requirement for a network activity warrant is also captured by this definition.

A person commits an offence if he or she uses, records, communicates or publishes protected information or protected network activity warrant information except in very limited circumstances. The Bill also provides for an aggravated offence if this disclosure endangers the health or safety or any person or prejudices the effective conduct of an investigation.

Exceptions – data disruption warrants and account takeover warrants

The exceptions to the prohibition on using, recording, communicating or publishing information collected under a data disruption warrant and under an account takeover warrant are the same as exceptions in the SD Act that relate to existing warrants, such as computer access warrants.

It is permitted to use, record, communicate, publish, and admit in evidence, protected information where necessary for the investigation of a relevant offence, a relevant proceeding, or the making of a decision as to whether or not to bring a prosecution for a relevant offence (amongst other limited purposes). It is also permitted to use, record, communicate or publish protected information where that information has

already been disclosed in proceedings in open court lawfully, and where the communication of the information is necessary to help prevent or reduce the risk of serious harm.

Information collected under each of these warrants may also be shared with an intelligence agency if the information relates to a matter that is relevant to the agency's functions, and with a foreign country, the International Criminal Court, or a War Crimes Tribunal under international assistance authorisations, and also where authorised by the *Mutual Assistance in Criminal Matters Act 1987* or the *International Criminal Court Act 2002*. It is essential that this information sharing is permitted, in order to facilitate investigations that involve other Australian agencies (for example conducting joint operations) and foreign jurisdictions.

Information may also be shared with the Ombudsman and the IGIS, and between those agencies to allow them to fulfil their oversight responsibilities in relation to the powers in the Bill.

Exceptions – network activity warrants

The exceptions to the general prohibition on using and disclosing protected network activity warrant information are configured differently to those relating to data disruption warrants and account takeover warrants. This is because, as network activity warrants are for intelligence purposes, they cannot be used to gather evidence in investigations, and the information collected generally cannot be adduced in evidence in a criminal proceeding.

Protected network activity warrant information may be used or disclosed if necessary for collecting, correlating, analysing or disseminating, or the making of reports in relation to, criminal intelligence in the performance of the legislative functions of the AFP or the ACIC. The information can also be the subject of derivative use allowing it to be cited in an affidavit on application for another warrant (which will themselves contain protections on information gathered). This will assist in ensuring that network activity warrants can be useful in furthering investigations into criminal conduct made under subsequent warrants.

Protected network activity warrant information cannot be used in evidence in criminal proceedings, other than for a contravention of the secrecy provisions that apply to this intelligence. This is important for ensuring that where a person has unlawfully used or disclosed this information, he or she may be effectively investigated and prosecuted for the offence. The information may also be disclosed for the purposes of the admission of evidence in a proceeding that is not a criminal proceeding. This is intended to allow protected network activity warrant information to be used in other proceedings, such as those that question the validity of the warrant. Therefore, if a case is brought to challenge the decision to issue a warrant, there will be evidence which can be validly drawn upon. These exceptions are intended to protect the rights of persons who are the subject of, or whose information has been collected under, a network activity warrant.

The ability to share information obtained under a network activity warrant with ASIO or an intelligence agency is intended to facilitate joint operations between the AFP and the ACIC and other members of the National Intelligence Community. These agencies currently conduct complex and interrelated intelligence operations, and may need to share information to support activities within their respective functions, in particular those in relation to safeguarding national security. For example, information collected under a network activity warrant about a terrorist organisation may be shared with ASIO if related to ASIO's functions. Information held by ASIO and intelligence agencies, including information obtained under a network activity warrant that is then communicated to those agencies, is protected by strict use and disclosure provisions in the *Australian Security Intelligence Organisation Act 1979* and *Intelligence Services Act 2001*.

To ensure compliance with reporting and record-keeping requirements, the Bill provides that protected network activity warrant information may be used or disclosed for the purpose of keeping records and making reports by the AFP and the ACIC in accordance with the obligations imposed by the Bill. Information may also be shared with the Ombudsman and the IGIS, and between those agencies to allow them to fulfil their oversight responsibilities in relation to the powers in the Bill. These exceptions are important to facilitate effective oversight of the AFP and the ACIC and protect the rights of persons who are the subject of, or whose information has been collected under, a network activity warrant.

Information held by the Ombudsman and IGIS, including information obtained under a network activity warrant that is then communicated to those bodies, is protected by strict use and disclosure provisions in the *Ombudsman Act 1976* and *Inspector-General of Intelligence and Security Act 1986*.

b. why the bill does not require review of the continued need for the retention of records or reports comprising protected information on a more regular basis than a period of five years.

Records comprising protected information in the Bill must be destroyed as soon as practicable if the material is no longer required, and at most within five years of the material no longer being required (unless a relevant officer certifies certain matters that go to the need to keep the material for ongoing activity). As noted by the Committee, the chief officer of the AFP or the ACIC must ensure that information obtained under each of these warrants is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. This is consistent with existing record-keeping and destruction obligations in relation to surveillance device warrants and computer access warrants in the SD Act.

As with information collected under existing warrants in the SD Act, the ability to retain information for five years reflects the fact that some investigations and operations are complex and run over a long period of time. Requiring the security and destruction of records ensures that the private data of individuals accessed under a warrant is only handled by those with a legitimate need for access, and is not kept in perpetuity where there is not a legitimate reason for doing so. The Ombudsman and IGIS are empowered to assess agencies' compliance with record-keeping and destruction requirements as part of their oversight of powers in the Bill.

Presumption of innocence – certificate constitutes prima facie evidence

1.154 As the explanatory materials do not adequately address these issues, the committee requests the minister's detailed advice as to:

a. why it is considered necessary and appropriate to provide for evidentiary certificates to be issued in connection with a data disruption warrant or emergency authorisation, a network activity warrant, or an account takeover warrant

The *Guide to Framing Commonwealth offences, Infringement Notices and Enforcement Powers* notes that evidentiary certificates should generally only be used to settle formal or technical matters of fact that would be difficult to prove by adducing admissible evidence. It is generally unacceptable for evidentiary certificates to cover questions of law, which are for courts to determine.

Evidentiary certificates are able to be issued in relation to acts done by the AFP or the ACIC in connection with the execution of the warrant, or the information obtained under the warrant. The evidentiary certificate regimes in relation to each of the warrants are designed to protect capabilities and methodology being disclosed in court.

Evidentiary certificates will only cover the manner in which evidence was obtained and by whom but not the actual evidence itself. The certificates would only deal with factual matters, being the factual basis on which an officer did any thing in connection with the execution of the warrant, or in relation to the information obtained under the warrant. They would not deal with questions of law that would be properly the role of the courts to determine.

Evidentiary certificates are *prima facie* (that is, certificates issued under the regimes will be persuasive before a court, as distinct from a conclusive certificate that cannot be challenged by a court or defendant). The *prima facie* nature of evidentiary certificates will protect sensitive AFP and ACIC capabilities by preventing prosecutors from being required in the first instance to disclose the operation and methods of law enforcement unless a defendant seeks to dispute the veracity of the methods used to gather information against their interest. The courts will retain the ability to test the veracity of the evidence put before it should there be founded grounds to challenge the evidence.

b. the circumstances in which it is intended that evidentiary certificates would be issued, including the nature of any relevant proceedings

Evidentiary certificates are intended to streamline the court process by reducing the need to contact numerous officers and experts to give evidence during proceedings on routine matters. Evidentiary certificates can be issued by an appropriate authorising officer for a law enforcement officer and assist agencies in protecting sensitive capabilities.

The certificates will cover circumstances where it would be difficult to prove the methods of data collection before a court without exposing sensitive law enforcement capabilities. Methods used to conceal that a warrant has been executed or the methods used to covertly access or disrupt data, or take control of an online account, may be covered by an evidentiary certificate. In a criminal trial, where it may be necessary to establish the provenance of evidence called against a defendant, it may be necessary to rely on an evidentiary certificate to prove that evidence was collected as a result of a warrant.

Evidentiary certificates will be used in respect of the warrant-related activities and handling of information obtained under warrants as they are able to be used with existing surveillance device warrants and computer access warrants in the SD Act. A certificate may be issued, for example, in respect of anything done by a law enforcement officer in connection with the warrant's execution. The certificate may also set out relevant facts with respect to anything done by the law enforcement officer relating to the communication of information obtained under a warrant by a person to another person. A certificate can also set out anything done by a law enforcement officer concerning the making use of, or the making of, a record or the custody of a record of information obtained under the warrant.

These certificates relate to technical questions and not substantial matters of fact or questions of law. For example, it may be that a certain vulnerability within a device was used to execute a warrant. Enquiries into these actions may put at risk existing operations also utilising that vulnerability. Evidentiary certificates to protect capabilities and methodology is critical to maintaining law enforcement's ability to effectively utilise Commonwealth surveillance laws.

c. the impact that issuing evidentiary certificates may have on individuals' rights and liberties, including on the ability of individuals to challenge the lawfulness of actions taken by law enforcement agencies.

The Bill engages certain rights, such as Article 14(2) of the International Covenant on Civil and Political Rights, which provides that everyone charged with a criminal offence should have the right to be presumed innocent until proven guilty according to law. Limitations on this right are permissible when they are reasonable in the circumstances, and maintain the rights of the accused.

The evidentiary certificate provisions in the Bill create a presumption as to the existence of the factual basis on which the certificate is issued which requires the defendant to disprove the matters in the certificate if they seek to challenge them. However, these matters will only be details of sensitive information such as how the evidence was obtained and by whom. This is necessary to protect law enforcement agencies' sensitive capabilities and methodology. Evidentiary certificates will not, however, establish the weight or veracity of the evidence itself which is a matter for the court.

The defendant will not be prevented from leading evidence to challenge a certificate. The nature of a *prima facie* evidence certificate regime provides an ability for the accused to establish illegality — that is, to seek to establish that acts taken in order to give effect to a warrant contravened the legislation should they choose to do so within the boundaries of the judicial framework, and put the party bringing the proceedings to further proof. However, regardless of the evidentiary certificate regime, the prosecution will still have to make out all elements of any offence.

Reversal of evidential burden of proof

1.158 As the explanatory materials do not adequately address this issue, the committee requests the minister's advice as to why it is proposed to use offence-specific defences (which reverse the evidential burden of proof) in this instance. The committee's consideration of the appropriateness of a provision which reverses the burden of proof is assisted if it explicitly addresses relevant principles as set out in the *Guide to Framing Commonwealth Offences*.

The Bill introduces the concept of 'protected information' into the Crimes Act in relation to account takeover warrants, replicating the meaning of 'protected information' in the SD Act. This means that it will be an offence to disclose protected information under the Crimes Act except in limited circumstances. That offence, as well as the associated aggravated offence, are substantively similar to section 45 of the SD Act. The exceptions to the commission of the offences also replicate section 45.

In accordance with subsection 13.3(3) of the *Criminal Code Act 1995,* it is the defendant who must adduce evidence that suggests a reasonable possibility that he or she has not unlawfully used or disclosed protected information. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt (subsection 13.3(4) of the Criminal Code).

The *Guide to Framing Commonwealth Offences* provides that a matter should only be included in an offence-specific defence (as opposed to being specified as an element of the offence), where:

- it is peculiarly within the knowledge of the defendant, and
- it would be significantly more difficult and costly for the prosecution to disprove that for the defendant to establish the matter.

In accordance with the principles set out in the *Guide to Framing Commonwealth Offences*, the Bill places an evidential burden on the defendant because the matter is peculiarly within the defendant's knowledge. The defendant would be best placed to explain his or her motivations when using or disclosing protected information, as to how and why they should be considered to be acting in accordance with one of the exceptions set out in subsections 3ZZVH(3)-(5).

In order for the prosecution to disprove the matter, the prosecution would need to understand the information held by the defendant, including the defendant's state of mind and motivations. This would be significantly more difficult and costly, if not impossible, for the prosecution to disprove.

Broad delegation of administrative powers

1.162 The committee requests the minister's advice as to why it is considered necessary to allow for executive level members of staff of the ACIC to be 'appropriate authorising officers', in particular with reference to the committee's scrutiny concerns in relation to the use of coercive powers without judicial authorisation under an emergency authorisation.

Proposed section 3ZZUX of the Crimes Act allows law enforcement officers of the AFP and the ACIC to apply to an 'appropriate authorising officer' instead of seeking a warrant from a magistrate for the taking control of an online account in certain emergency situations.

In relation to the ACIC, an 'appropriate authorising officer' is the CEO of the ACIC or an executive level member of staff of the ACIC who is authorised by the CEO to be an appropriate authorising officer. This means that an executive level staff member of the ACIC is only able to give an emergency authorisation if they have been authorised to do so by the CEO.

The level of officer in the ACIC able to give an emergency authorisation differs to that in the AFP to reflect differences in the organisational structures and staffing arrangements of those agencies. There may be circumstances where it is necessary and appropriate for the CEO of the ACIC to authorise executive level staff members to give emergency authorisations. For example, where particular resourcing or operational requirements permit. However, such decisions will be made at the discretion of the CEO of the ACIC.