



**THE HON PETER DUTTON MP  
MINISTER FOR HOME AFFAIRS**

Ref No: MS20-001286

Senator Helen Polley  
Chair  
Senate Standing Committee for the Scrutiny of Bills  
Suite 1.111  
Parliament House  
Canberra ACT 2600

Dear Senator

Thank you for your letter dated 11 June 2020 requesting further information on the Australian Security Intelligence Organisation Amendment Bill 2020, and the Committee's subsequent extension of time for a response to 20 July 2020.

My response for the Committee's consideration is enclosed.

Yours sincerely

PETER DUTTON 21/07/20

**RESPONSE TO THE SENATE STANDING COMMITTEE FOR THE SCRUTINY OF BILLS  
SCRUTINY DIGEST 7 OF 2020  
AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION AMENDMENT BILL 2020**

This is a response to issues that the Senate Standing Committee for the Scrutiny of Bills raised in relation to the Australian Security Intelligence Organisation Amendment Bill 2020 (the **Bill**) in its Scrutiny digest 7 of 2020.

The Bill would, if passed:

- repeal the Australian Security Intelligence Organisation's (**ASIO**) current questioning and detention regime set out in Division 3 of Part III of the Australian Security Intelligence Organisation Act 1979 (**ASIO Act**)
- introduce a reformed compulsory questioning framework for ASIO, and
- amend ASIO's tracking device framework to support operational agility, mitigate risk to ASIO's surveillance operatives, and resolve the current disadvantage faced by ASIO when engaging in joint operations with law enforcement agencies by aligning ASIO's approval process with the existing law enforcement process.

***Trespass on personal rights and liberties***

**1.11 The committee therefore requests the minister's more detailed advice regarding whether appropriate safeguards are in place to ensure that any prescribed authorities are independent, noting the significant coercive powers provided to them.**

*The role of the prescribed authority*

The prescribed authority supervises questioning to ensure that the warrant is executed within the confines of the law and may make a number of directions in relation to the conduct of all people involved in the execution of a questioning warrant. A prescribed authority has the same protection and immunity as a Justice of the High Court in the performance of the prescribed authority's duties.<sup>1</sup>

The Bill would introduce measures to ensure the independence of those appointed as a prescribed authority, and avoid perceived and actual conflicts of interest. The independence will serve to protect the rights of the person questioned and ensure a fair questioning process.

*Prescribed authority eligibility*

The strict limits on the people the Attorney-General may appoint as a prescribed authority provides a safeguard for independence. The Attorney-General may only appoint, as a prescribed authority:<sup>2</sup>

- a person who has been a judge in a superior court for at least 5 years who no longer holds a commission as a judge
- a President or Deputy President of the Administrative Appeals Tribunal (**AAT**) who has been enrolled as a legal practitioner for at least 5 years, or
- a person who has been a legal practitioner for at least 10 years and holds a practicing certificate.

---

<sup>1</sup> Australian Security Intelligence Organisation Amendment Bill 2020, Schedule 1, s 34AE.

<sup>2</sup> *Ibid*, s 34AD.

Before appointing a legal practitioner, the Attorney-General must be satisfied that the person has the knowledge or experience necessary to properly perform the duties of a prescribed authority.<sup>3</sup> This additional requirement would ensure that a person is not appointed solely because they have been a legal practitioner for at least 10 years and hold a practicing certificate, but do not otherwise have the necessary knowledge or experience to properly perform the duties of a prescribed authority.

Superior court judges and senior AAT members are entrusted with significant responsibilities in Australia's legal system to act independently, including in their role authorising investigatory powers and reviewing government decisions. Similarly, senior legal practitioners have experience working within the justice system and maintaining standards of professional conduct to act with integrity and avoid conflicts of interest. Legal practitioners have a broad and permanent duty to the administration of justice. Legal practitioners must always act in a manner that demonstrates they are fit and proper to practise law. The consequences for legal practitioners who breach their duties are severe and may include being banned from practice.

As a further safeguard, a person will not be eligible for appointment as a prescribed authority, despite meeting the eligibility requirements, if that person is an ASIO employee or affiliate, the Director-General of Security, an Australian Government Solicitor lawyer, an Inspector-General of Intelligence and Security (**IGIS**) official, or a staff member of a law enforcement agency (including the Australian Federal Police) or an intelligence or security agency.<sup>4</sup> This limitation protects against the potential for partiality, whether conscious or unconscious, if government officials were to exercise the duties of a prescribed authority.

#### *Broadening the pool of potential candidates*

Currently, under section 34B of the ASIO Act, the Attorney-General may appoint retired superior court judges as prescribed authorities, or alternatively, where the number of available prescribed authorities is insufficient, serving superior court judges, or the President and Deputy President of the AAT. The Bill amends the eligibility criteria for the appointment of a prescribed authority to include legal practitioners with the appropriate knowledge and experience, in order to increase the pool of suitable candidates and facilitate the development of institutional expertise in supervising compulsory questioning under a questioning warrant. The Bill provides that serving superior court judges will no longer be eligible for appointment as prescribed authorities.

The current prescribed authority model has presented difficulties, as a number of appointees are unwilling or unable to serve in this capacity for an extended period of time, representing a barrier to the development of institutional expertise in controlling compulsory questioning.

The Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) review of the operation, effectiveness and implications of Division 3 of Part III of the *Australian Security Intelligence Organisation Act 1979 (ASIO Act)* accepted that a model reliant on retired judges may lead to a shortage of persons willing and able to perform the role of the prescribed authority.<sup>5</sup>

#### *There is a mechanism to manage conflicts of interest*

Before appointing any person as a prescribed authority, the Attorney-General must have regard to whether the person engages in any paid or unpaid work, or has any interests (pecuniary or

---

<sup>3</sup> *Ibid*, s 34AD(3).

<sup>4</sup> *Ibid*, s 34AD(2).

<sup>5</sup> PJCIS report on the operation, effectiveness and implications of Division 3 of Part III of the ASIO Act, [3.144].

otherwise) that conflict, or could conflict, with the proper performance of the person's duties as a prescribed authority.<sup>6</sup> Prescribed authorities have an ongoing duty to disclose their interests.<sup>7</sup> The Attorney-General may terminate the appointment of a prescribed authority due to conflicts of interest or potential conflicts of interest (see *Prescribed authorities generally cannot be removed* for further circumstances in which an appointment can be terminated).<sup>8</sup> These requirements are designed to ensure a prescribed authority is free from inducements and capable of acting impartially by minimising the scope for potential conflicts of interest.

*Prescribed authorities generally cannot be overruled*

Prescribed authorities are not subject to directions, and their decisions may only be overruled by the Attorney-General or the Director-General of Security in two limited circumstances:

- where the Attorney-General issues a variation to an existing questioning warrant requiring the subject's immediate appearance where the prescribed authority has previously issued a direction for appearance at a later time,<sup>9</sup> or
- where the subject and the prescribed authority have been excused from further attendance and the Director-General varies or revokes a direction given by the prescribed authority in relation to the use or disclosure of questioning material.<sup>10</sup>

These narrow exceptions are necessary for the efficient execution of questioning under a warrant.

Should the Attorney-General be satisfied that it is reasonable and necessary in the circumstances, the warrant may, despite any direction given by the prescribed authority under section 34DE(1) of Schedule 1 of the Bill to the contrary, require the subject's further appearance for questioning under the warrant, and include an immediate appearance requirement in relation to the further appearance.<sup>11</sup> The ability for the Attorney-General to vary a warrant by requiring a subject's immediate appearance may have the effect of overriding a direction given by the prescribed authority that the subject returns for questioning at a specified time. Rather than complying with the prescribed authority's direction, the subject would be required to appear for questioning immediately when notified of the variation.

From a practical perspective, there may be some circumstances where it may be necessary to require the subject to attend questioning at an earlier time than the time directed by the prescribed authority, or require the subject to reappear for questioning after the prescribed authority has excused or released the subject from further attendance at questioning. For example, this requirement may arise where ASIO receives intelligence that suggests the subject intends to meet with a person involved in their prejudicial activities.

Where the subject and, consequently, the prescribed authority have been excused from further attendance at questioning the Director-General may vary or revoke a direction given by the prescribed authority relating to the use or disclosure of questioning material under section 34DF of Schedule 1 of the Bill. As the prescribed authority's supervision of questioning has ceased, it is necessary to enable the Director-General to vary or revoke such a direction where it is no longer necessary. This is consistent with similar provisions in the *Australian Crime Commission Act 2002* and the *Law Enforcement Integrity Commissioner Act 2006*. Any decision of the Director-General to

---

<sup>6</sup> *Ibid*, s 34AD(5).

<sup>7</sup> *Ibid*, s 34AD(6)-(8).

<sup>8</sup> *Ibid*, s 34AD(9).

<sup>9</sup> *Ibid*, s 34BE(5).

<sup>10</sup> *Ibid*, s 34DF(3)(b).

<sup>11</sup> *Ibid*, s 34BE(5)

revoke or vary a direction relating to the use or disclosure of questioning material is subject to oversight by the IGIS.

*Prescribed authorities generally cannot be removed*

The independence of prescribed authorities is further reinforced by the limited circumstances in which they can be removed. The Attorney-General may only terminate the appointment of a prescribed authority due to:<sup>12</sup>

- misbehaviour
- an inability to perform the duties of a prescribed authority due to physical or mental incapacity
- bankruptcy
- failure, without reasonable excuse, to comply with the obligation to disclose interests, or
- paid or unpaid work, or an interest, pecuniary or otherwise, that, in the Attorney-General's opinion, conflicts or could conflict with the proper performance of the prescribed authority's duties.

This ensures that a prescribed authority cannot be unduly influenced by improper threats of removal from office, or prevented from performing their functions by actual removal, except in limited, and appropriate, circumstances. In this way, security of tenure supports the independence of prescribed authorities.

*There are strict limits on the powers held by the prescribed authority*

In paragraph 1.9, the Committee noted that its concerns are "heightened by the very significant powers that are provided to prescribed authorities under the bill, including allowing for the questioning of children under 14 and the significant limits that can be placed on a person's choice of legal representation by prescribed authorities."

Prescribed authorities cannot permit the questioning of individuals under the age of 14 in any circumstances. Under the Bill, a questioning warrant will have no effect if the subject of the warrant is under 14 years old.<sup>13</sup> A prescribed authority must direct that a person not be questioned if the prescribed authority is satisfied on reasonable grounds the subject is under 14 years old.<sup>14</sup>

The powers of a prescribed authority are strictly limited by the confines of the Bill. A significant proportion of the prescribed authority's role is designed to act as a safeguard for questioning subjects, which act as a check on the prescribed authority's powers. For example, in relation to minors:

- the prescribed authority must explain certain matters,<sup>15</sup> and additional matters relevant to the minor,<sup>16</sup> such as their rights in relation to a lawyer and a minor's representative
- questioning of a minor may only occur for continuous periods of 2 hours or less, separated by breaks directed by the prescribed authority, and<sup>17</sup>

---

<sup>12</sup> *Ibid*, s 34AD(9).

<sup>13</sup> *Ibid*, s 34BC.

<sup>14</sup> *Ibid*, s 34DG.

<sup>15</sup> *Ibid*, s 34DC.

<sup>16</sup> *Ibid*, s 34DD.

<sup>17</sup> *Ibid*, s 34BD(2)(b).

- to facilitate the presence of a lawyer at all times during questioning, the Bill requires the prescribed authority to appoint a lawyer for the subject of a questioning warrant in certain circumstances, such as when a lawyer of choice is not available.<sup>18</sup>

In addition, the prescribed authority does not have a general ability to limit a person's choice of legal representation, although there are specific restrictions. For example, the prescribed authority may:

- prevent the subject from contacting a specific lawyer where the prescribed authority is satisfied, on the basis of circumstances relating to that lawyer, that contact with that lawyer may result in either a person involved in an activity prejudicial to security being alerted that the activity is being investigated, or a record or other thing that the subject has been, or may be, requested to produce in accordance with the warrant being destroyed, damaged or altered,<sup>19</sup> and
- address the disruption of questioning by directing that the lawyer be removed from questioning, if the prescribed authority considers the lawyer's conduct is unduly disrupting the questioning of the subject.<sup>20</sup>

The Bill provides that in these circumstances, the subject may contact another lawyer.

Further, in certain circumstances where the prescribed authority has appointed a lawyer<sup>21</sup> and the subject's lawyer of choice is also present, the prescribed authority must defer questioning to allow time for the appointed lawyer to brief the lawyer of choice, and for the lawyer of choice to provide advice to the subject.<sup>22</sup>

The subject of an adult questioning warrant may not be questioned in the absence of a lawyer, subject to the following limited exceptions:

- the subject voluntarily chooses to be questioned in the absence of a lawyer<sup>23</sup>
- the prescribed authority is satisfied the subject has had a reasonable period to obtain a lawyer and the warrant does *not* contain an immediate appearance requirement, or<sup>24</sup>
- the prescribed authority removes a disruptive lawyer and the subject has had a reasonable period to obtain an alternative lawyer.<sup>25</sup>

Minors must not be questioned in the absence of a lawyer.<sup>26</sup>

#### *Safeguards outside of the Bill*

In addition to the safeguards built into the Bill, ASIO must comply with the Guidelines given by the Attorney-General to the Director-General of Security under section 8A of the ASIO Act.<sup>27</sup>

---

<sup>18</sup> *Ibid*, s 34FC.

<sup>19</sup> *Ibid*, s 34F(4)

<sup>20</sup> *Ibid*, s 34FF(6)

<sup>21</sup> *Ibid*, ss 34FB(2)(a), 34FC(2)(a) and 34FC(3)(b).

<sup>22</sup> *Ibid*, s 34FB(4)(c) and 34FC(4)(c).

<sup>23</sup> *Ibid*, s 34FA(2)(a).

<sup>24</sup> *Ibid*, s 34FA(2)(b) and 34FB(3)(b).

<sup>25</sup> *Ibid*, s 34FA(2)(b) and 34FF(7)(c)(i).

<sup>26</sup> *Ibid* s 34FA(1).

<sup>27</sup> *The Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)*, available at: <https://www.asio.gov.au/sites/default/files/Attorney-General%27s%20Guidelines.pdf>.

The current Guidelines require ASIO, before requesting a questioning warrant, to ensure that in the conduct of its inquiries and investigations:<sup>28</sup>

- the means used to obtain information are proportionate to the gravity of the threat posed and the probability of its occurrence
- the more intrusive the investigation technique, the higher the level of officer required to approve its use
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques, and
- ASIO should conduct inquiries and investigations into individuals and groups:
  - with as little intrusion into individual privacy as is possible consistent with the performance of its functions, and
  - with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest.

Accordingly, all questioning must occur within these guidelines, imposing further safeguards on the prescribed authority questioning model.

In addition, the *Inspector-General of Intelligence and Security Act 1986 (IGIS Act)* authorises the IGIS to inquire into any matter relating to compliance by ASIO with laws of the Commonwealth, the States and Territories or with ministerial directions and guidelines or human rights requirements. The IGIS may also inquire into the propriety of ASIO's actions and the effectiveness and appropriateness of procedures relating to legality or propriety. The IGIS has significant powers to compulsorily obtain information and documents and enter premises, as well as reporting obligations. Sections 9B and 19A of the IGIS Act further provide that the IGIS may enter any place where a person is being questioned or apprehended in relation to a questioning warrant at any reasonable time. This enables the IGIS to be present during any questioning by a prescribed authority to provide an additional layer of oversight.

**1.15 The committee therefore requests the minister's more detailed advice as to:**

- **why it is considered necessary and appropriate to allow the Attorney-General to issue questioning warrants and warrants for the recovery of tracking devices, and**
- **whether the bill can be amended to provide that questioning warrants and warrants for the recovery of tracking devices are instead issued by judicial officers.**

The existing questioning framework in Division 3 of Part III of the ASIO Act requires ASIO to seek the Attorney-General's consent before applying to an issuing authority for the issue a questioning warrant. This multi-step process is inconsistent with the authorisation of other domestic ASIO warrants and not conducive to the efficient or timely execution of a questioning warrant. The Bill would remove the issuing authority role, and provide the Attorney-General with sole responsibility for issuing a questioning warrant.<sup>29</sup> This would include an express power to vary or revoke a questioning warrant, and the ability to authorise the subject's apprehension.<sup>30</sup> In its extensive

---

<sup>28</sup> *Ibid*, at [10.4].

<sup>29</sup> Australian Security Intelligence Organisation Amendment Bill 2020, Schedule 1, ss 34BA and 34BB.

<sup>30</sup> *Ibid*, ss 34BG(1) and 34BE(2).

review of the operation, effectiveness and implications of Division 3 of Part III of the ASIO Act, the PJCIS found it appropriate that the Attorney-General issue questioning warrants.<sup>31</sup>

Section 26G of the Bill will allow ASIO to use tracking devices under an internal authorisation where use of the device will, or is likely to, substantially assist the collection of intelligence in respect of a matter which is important in relation to security. This will bring ASIO's tracking device provisions under the ASIO Act broadly in line with law enforcement agencies' powers under the *Surveillance Devices Act 2004*. An internal authorisation does not authorise interference with the inside of a vehicle or entrance to premises without permission. If recovery of a tracking device installed, used or maintained under an internal authorisation would require entry to premises or interference with the interior of a vehicle without permission, ASIO must obtain a warrant in order to recover the tracking device.<sup>32</sup> For example, if ASIO installed a tracking device on a vehicle when it was located on the street pursuant to an internal authorisation, but the vehicle was later indefinitely relocated to private premises, ASIO would require a warrant for recovery of the device as it would require entry to a private premises without permission.

As the First Law Officer of the Commonwealth with responsibility for the rule of law and oversight of intelligence agencies, the Attorney-General currently issues all other ASIO special power warrants in the ASIO Act. This includes search, surveillance device and computer access warrants. This provides ministerial oversight of the intended use of intrusive powers for national security purposes, and establishes ministerial accountability, a central principle of Australia's parliamentary system. In his Third Report of the Royal Commission on Intelligence and Security, Justice Hope highlighted that Ministers are required to accept clear responsibility for the actions of the intelligence community and are accountable to Parliament for the agencies within it.

The Attorney-General's role is separate but complementary to the provision for independent oversight and review by the IGIS as to the legality and propriety of the activities undertaken by ASIO for national security purposes.

For these reasons, it is not considered appropriate to amend the Bill to provide that questioning warrants and warrants for the recovery of tracking devices are instead issued by judicial officers.

**1.19 In light of the above, the committee requests the minister's more detailed advice regarding whether there are appropriate safeguards in place to protect the personal rights and liberties of persons presenting to a place for questioning. In particular, the committee requests the minister's advice as to whether the bill can be amended to include a defence to proposed subsection 34GD(2) so that the offence will not apply in circumstances where the request was unreasonable or the person was not capable of understanding a request made of them.**

*The Bill includes safeguards to protect the personal rights and liberties of persons attending questioning*

The Bill provides screening measures at the place of questioning which engage the personal rights and liberties of persons presenting to a place for questioning.<sup>33</sup> These measures will apply to anyone (including the subject) who seeks to enter the place where the subject of a questioning warrant is due to appear, or is appearing, for questioning under a warrant, including lawyers and minor's representatives.<sup>34</sup> The police officer may request the person to produce a thing in the person's

---

<sup>31</sup> PJCIS report on the operation, effectiveness and implications of Division 3 of Part III of the ASIO Act, [3.123] – [3.124].

<sup>32</sup> Australian Security Intelligence Organisation Amendment Bill 2020, Schedule 2, s 26R.

<sup>33</sup> *Ibid*, s 34D-34DA.

<sup>34</sup> *Ibid*, s 34D(1).



possession for inspection or examination, including anything worn or carried by the person that can be conveniently removed by the person.<sup>35</sup> This may include requesting the person to remove any items from his or her pockets, or produce items held in an item of baggage for inspection. A police officer may also request the person undergo an ordinary or frisk search to ascertain whether the person is carrying a dangerous item or a communications device.

The screening measures ensure that a person does not possess a communications device or dangerous item. They are necessary for the safety of those involved in questioning, and to prevent the communication or recording of information disclosed during the questioning process.

The Bill includes safeguards to protect the personal rights and liberties of people who present to a place for questioning. This includes:

- a police officer may only conduct an ordinary or frisk search if the officer suspects on reasonable grounds that it is prudent to conduct the search in order to ascertain whether the person is carrying a dangerous item or communications device<sup>36</sup>
- an ordinary search or a frisk search must if practicable be conducted by a police officer of the same sex<sup>37</sup>
- the Bill does not explicitly authorise police officers to use force in the conduct of a search.
- searches are conducted on a voluntary basis (although refusing to comply could result in a failure to appear, which is an offence under section 34GD),<sup>38</sup> and
- that a person has the right to complain to the IGIS, Ombudsman or relevant complaints agency.<sup>39</sup>

#### *Operation of section 34GD(2)*

Section 34GD(1) of Schedule 1 of the Bill provides that the subject of a questioning warrant commits an offence if the subject fails to appear before a prescribed authority for questioning in accordance with the warrant or a direction to appear given by the prescribed authority. A person is taken to fail to appear if the person is refused entry to the place of questioning because the person did not comply with a request to be screened or searched.<sup>40</sup>

Under general principles of the criminal law, fault is required to be proven before a person can be found guilty of a criminal offence. *Fault elements* relate to the defendant's state of mind at the time the physical elements are engaged in, or arise. Under section 5.6 of the Criminal Code, the automatic fault element of conduct is intention.

Consequently, a person who fails to comply with a request from a police officer under proposed section 34D must have *intentionally* done so. It is unlikely that a person who has not understood the request, due to an intellectual disability or inability to speak English, could be proven to have intentionally refused the request. It is therefore not necessary to amend the Bill to provide a defence in circumstance where a person would not be capable of understanding a request made of them.

---

<sup>35</sup> *Ibid*, s 34D(2)

<sup>36</sup> *Ibid*, s 34D(2)(c).

<sup>37</sup> *Ibid*, s 34D(3).

<sup>38</sup> *Ibid*, s 34D(2).

<sup>39</sup> *Ibid*, ss 34DC(1)(i), 34DI.

<sup>40</sup> *Ibid*, s 34GD(2).

### *Reasonableness of police requests under section 34D*

The Bill does not contain an explicit reasonableness requirement for a police officer to request the person undergo a screening procedure or produce a thing in the person's possession for inspection. This is because it is *prima facie* reasonable for a police officer to make these requests of a person before entering the place of questioning. The screening measures ensure that a person does not possess a communications device or dangerous item. The measures are necessary for the safety of those involved in questioning, and to prevent the communication or recording of information disclosed during the questioning process.

Furthermore, a police officer may only request the person undergo an ordinary or frisk search to ascertain whether the person is carrying a dangerous item or a communications device. The police officer must suspect on reasonable grounds that it is prudent to conduct the search in order to ascertain whether the person is carrying a dangerous item or communications device.<sup>41</sup> Accordingly, a reasonableness requirement does apply to the ordinary or frisk search requirements.

### ***Significant matters in non-disallowable delegated legislation***

**1.27 In light of the above, the committee requests the minister's more detailed advice as to:**

- **why it is considered necessary and proportionate to leave the statement of procedures, which will contain significant practical information in relation to the execution of questioning warrants, to non-disallowable delegated legislation, and**
- **whether the bill can be amended to provide that the statement of procedures will be disallowable to allow for appropriate parliamentary scrutiny of the procedures.**

Section 34AF of Schedule 1 of the Bill provides that the Director-General of Security may prepare a written statement of procedures to be followed in the exercise of authority under a questioning warrant. The statement must be drafted in consultation with the IGIS and the Commissioner of the Australian Federal Police, and approved by the Attorney-General. The proposed section would replace current section 34C of the ASIO Act.

The statement is a legislative instrument which supplements the provisions in the ASIO Act with the same legal force. The statement is published on the Federal Register of Legislation, which provides transparency to the public about the procedures with which ASIO must comply.

The purpose of the statement is to set out standard operational procedures in relation to the execution of a questioning warrant, and may include, for example, operational procedures about the questioning of the subject, transportation of the subject, and matters to support the health and wellbeing of the subject. In this way, the statement supports a number of legal requirements on the face of the legislation, such as the requirement in section 34AG of Schedule 1 of the Bill which states that the subject of a questioning warrant must be treated with humanity and with respect for human dignity, and must not be subjected to torture or to cruel, inhuman or degrading treatment. The statement can provide greater detail and guidance than is usually appropriate for primary legislation, which sets out the minimum requirements.

It is appropriate to exclude the statement of procedures from the disallowance provisions because the statement is an internal management tool of government, which provides detailed procedures to ensure compliance with the requirements of the Act. The statement addresses specific security needs.

---

<sup>41</sup> *Ibid*, s 34D(2)(c).

In addition, there is a practical issue that if the statement of procedures is disallowable, and is in fact disallowed, the Attorney-General could not proceed with issuing a questioning warrant. Under section 34BA(1), the Attorney-General may only issue a questioning warrant if satisfied that, among other things, there is a written statement of procedures in force to be followed in the exercise of authority under a questioning warrant. If the statement is disallowed, another statement (substantially the same) could not be made for 6 months from the time of disallowance. Consequently, disallowance may present a barrier to the questioning regime, as questioning matters are likely to be time critical. The purpose of questioning warrants is for ASIO to collect intelligence relating to threats to Australia's security, and this purpose may be defeated if the statement of procedures is disallowable.

### ***Significant matters in delegated legislation***

#### **1.31 The committee therefore requests the minister's more detailed advice regarding:**

- **why it is considered necessary and appropriate to allow the regulation of access to information by lawyers to be left to delegated legislation, and**
- **whether the bill can be amended to include at least high-level guidance in this regard on the face of the primary legislation.**

Section 34FH of Schedule 1 of the Bill mirrors existing section 34ZT of the ASIO Act. Section 34FH provides that the regulations may prohibit or regulate access to information by lawyers acting for a person in connection with proceedings relating to the warrant or the treatment of persons in connection with the warrant. Access to information may only be prohibited or regulated where it has been otherwise controlled or limited on security grounds. This would apply to classified information.

The ASIO Regulation 2016, made under current section 34ZT, requires that access to security information may only be given to the lawyer if the lawyer has a security clearance or the Secretary of the Department is satisfied that giving the lawyer access to information would not be prejudicial to security. The regulation also allows the Secretary of the Department to provide the information subject to conditions about the use, handling, storage and disclosure of the information.

It is necessary and appropriate to regulate access to security classified information in subsequent proceedings, as it is highly sensitive information which, if disclosed, may cause grave damage to the national interest or individuals.

The approach taken by the Bill maintains the approach taken by the existing Division 3 questioning framework, which has worked effectively to date. This provides benefits with respect to consistency and stability of the law.

In both the Bill and the current framework, it is appropriate to include these matters in regulations, as opposed to primary legislation. Regulating access to information by lawyers through the regulations allows for more detailed guidance than could otherwise be provided through primary legislation. In addition, the regulations may be amended more rapidly than primary legislation. This allows the regulations to take into account any critical developments in the protection of national security information in a constantly changing security environment.

### ***Reversal of the evidential burden of proof***

#### **1.37 The committee requests the minister's advice as to:**

- **why it is considered necessary and appropriate to include the specified matters as offence-specific defences, and**

- **the appropriateness of amending proposed section 34GD so that the matters specified in proposed subsections 34GD(4) and (9) are framed as elements of the relevant offence.**

*Offence for failing to comply with a request*

Subsection 34GD(3) of Schedule 1 of the Bill provides that the subject of a questioning warrant commits an offence if the subject is appearing before a prescribed authority and fails to comply with a request to give any information or produce any record or thing. Section 34GD(4) provides an exemption to the offence if the subject does not have the information. These provisions are substantially similar to existing subsections 34L(2) and (3) of the ASIO Act.

In accordance with subsection 13.3(3) of the Criminal Code, it is the defendant who must adduce evidence that suggests a reasonable possibility that he or she does not have the information requested. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt.<sup>42</sup>

As the Committee noted, 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 than for the defendant to establish the matter.

In accordance with the principles set out in the *Guide to Framing Commonwealth Offences*, the Bill places the evidential burden on the defendant because the matter is peculiarly within the defendant's knowledge. This is because the subject would know whether he or she did not have the information ASIO requested. The matter would be significantly more difficult for the prosecution to disprove. In order for the prosecution to disprove the matter, the prosecution would need to understand all the information held by the defendant, and show that the defendant had the piece of information requested. This would be significantly more difficult and costly, if not impossible, for the prosecution to disprove.

*Offence for providing a false or misleading statement*

Subsection 34GD(8) provides that the subject of a questioning warrant commits an offence if the subject makes a statement that, to their knowledge, is false or misleading in purported compliance with a request from ASIO. Subsection 34GD(9) provides an exemption to the offence if the statement is not false or misleading in a material particular. These provisions are substantially similar to existing subsections 34L(8) and (9).

In accordance with subsection 13.3(3) of the Criminal Code, it is the defendant who must adduce evidence that suggests a reasonable possibility that the statement is not false or misleading in a material particular. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt.

As with the defence in section 34GD(4), the defendant is better placed to know whether what they have said is false or misleading in a material particular. For example, if the defendant provides a false statement in an answer to a question, the defendant would be in a better position to know whether the statement is false in a material particular, or whether the false statement was made only in respect of an inconsequential matter.

---

<sup>42</sup> Criminal Code, section 13.1.

The matter would be significantly more difficult for the prosecution to disprove. In order for the prosecution to disprove the matter, the prosecution would need to understand all the information held by the defendant, and show that the defendant had made a false or misleading statement as to a material particular. This would be significantly more difficult and costly, if not impossible, for the prosecution to disprove.

**1.41 The committee therefore requests a detailed justification from the minister for the proposed application of strict liability to certain elements of the unauthorised disclosure offences in proposed section 34GF, with reference to the principles set out in the *Guide to Framing Commonwealth Offences*.**

Subsection 34GF(3) of Schedule 1 of the Bill applies strict liability to the following physical elements of the offences:

- the information indicates the fact the warrant has been issued or a fact relating to the content of the warrant or to the questioning or apprehension of a person in connection with the warrant, and
- the information is operational information.

Consequently the prosecution is not required to prove fault for these elements. The prosecution does not need to establish that the person knew, intended or was reckless to, the nature of the information.

The person's culpability must be established for the remaining elements of the offence. In particular, the act of disclosing information is the substantive element of the offence and carries the fault element of intent. Therefore, to establish the offence, the prosecution must prove that the person intended to disclose information beyond a reasonable doubt.

The *Guide to Framing Commonwealth Offences* provides that applying strict liability to a particular physical element of an offence may be justified where requiring proof of fault would undermine deterrence, and there are legitimate grounds for penalising persons lacking 'fault' in respect of that element. The application of strict liability to the elements in section 34GF is necessary to ensure that a person cannot avoid criminal responsibility because they did not turn their mind to whether the information was operational information or information about the warrant.

Consistent with the *Guide to Framing Commonwealth Offences*, requiring knowledge of these elements would undermine deterrence of the offence. There are legitimate grounds for penalising a person lacking 'fault' in knowing or being reckless to the nature of operational information because the person engaged in conduct which may prejudice a security intelligence operation, and cause harm to Australia's national security. Upon service of the notification of the warrant the subject will be advised of the terms of the warrant both verbally and in writing. This will include their secrecy obligations and associated consequences of breaching those obligations. The prescribed authority will also remind the subject of these obligations at the beginning and end of questioning—this is likely to include information about the gravity of harm associated with an unauthorised disclosure given the operational information that may be disclosed. The subject will also have a lawyer to clarify any concerns about these obligations throughout the course of questioning.

There are legitimate grounds for penalising the lawyer without a fault element as the lawyer will also be reminded of his or her secrecy obligations and the serious consequences of making an unauthorised disclosure. The lawyer would have even more of an understanding of the gravity of harm associated with the disclosure of sensitive operational information.

The Senate Standing Committee for the Scrutiny of Bills has previously concluded that strict liability may be appropriate where it is difficult to prosecute fault provisions, particularly those involving intent. The Standing Committee noted that strict liability had been applied in a range of circumstances, including where it is difficult for the prosecution to prove a fault element because a matter is peculiarly within the knowledge of the defendant.<sup>43</sup> The application of strict liability avoids the evidential difficulties for the prosecution to prove beyond reasonable doubt that the accused knew, intended, or was reckless as to whether the information was operational or about a warrant.

For these reasons, it is not appropriate for the prosecution to be required to prove intention or recklessness in relation to the physical elements of the offence with respect to operational information and information about the warrant.

Notwithstanding the strict liability of these elements in section 34GF, the defence of mistake of fact is available under section 6.1 of the *Criminal Code*. That is, a person is not criminally responsible for an offence that has a physical element for which there is no fault element if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not facts existed, and is under a mistaken but reasonable belief about those facts, and
- had those facts existed, the conduct would not have constituted an offence.

**1.46 The committee therefore requests the minister's more detailed advice regarding:**

- **why it is necessary and appropriate to provide the Attorney-General with a broad discretionary power to determine guidelines regarding the provision of financial assistance in circumstances where there is limited guidance on the face of the primary legislation as to when or how this power should be exercised, and**
- **whether the bill can be amended to provide that the guidelines are legislative instruments subject the parliamentary disallowance.**

Section 34JE allows a subject of a questioning warrant to apply to the Attorney-General for financial assistance. The Attorney-General has a broad power to make written guidelines to be applied in authorising the provision of financial assistance. The broad power is necessary to allow the Attorney-General to take into account a wide variety of circumstances. These provisions mirror current section 34ZX of the ASIO Act, which has worked effectively to date. The existing guidelines are available to the public, through both the AGD website and the relevant Grant Opportunity on GrantConnect.

It is expected that any revised guidelines will remain available to the public and cover procedural issues such as the process for lodging an application and the level of fees available to barristers and solicitors representing the person who is questioned. Given the broad discretion to grant financial assistance, the guidelines enable the Attorney-General to communicate expectations about how the financial assistance process will be managed. The guidelines will not cover substantive matters or affect a person's right to apply for financial assistance. Consequently, it is not appropriate to amend the Bill to provide that the guidelines are legislative instruments.

**1.53 In light of the above, the committee requests the minister's more detailed advice regarding:**

---

<sup>43</sup> Australian Parliament—Senate Standing Committee for the Scrutiny of Bills, *Application of Absolute and Strict Liability Offences in Commonwealth Legislation* (2002), 259.

- **why it is necessary and appropriate for tracking devices to be approved for use by ASIO through an internal authorisation process, noting the potential trespass on personal rights and liberties,**
- **whether proposed subsections 26G(3) and 26H(1) of the bill can be amended to remove the ability to orally request and approve an internal authorisation for the use of a tracking device, and**
- **whether the bill can be amended to require that at least broad guidelines relating to the internal authorisation of the use of tracking devices are contained in a legislative instrument which is subject to parliamentary disallowance.**

*The internal authorisation framework is a proportionate and necessary response to the security environment*

The Bill will enable ASIO to use tracking devices under an internal authorisation, rather than under a warrant, where use of the device does not involve interference with the inside of a vehicle or entry to premises without permission. The Bill will also clarify that ASIO may use tracking devices without a warrant or authorisation in states and territories where it is not unlawful.

The amendments to allow ASIO to use tracking devices under an internal authorisation will bring ASIO's tracking device provisions under the ASIO Act broadly in line with law enforcement agencies' powers under the *Surveillance Devices Act 2004*. The current requirement to obtain a warrant in all circumstances can restrict ASIO from acting with sufficient speed to respond to time critical threats. It also creates a heightened level of risk to ASIO officers due to the need to maintain constant physical surveillance on potentially dangerous subjects where ASIO has insufficient time to obtain a warrant.

The Bill provides robust safeguards to ensure that ASIO's ability to internally authorise the use of tracking devices provides effective control over the use of the surveillance devices powers.

- Internal authorisations may only be granted by senior personnel, being the Director-General of Security or Senior Executive Service ASIO employees or affiliates.<sup>44</sup>
- An internal authorisation may only be issued where the use of the device will, or is likely to, substantially assist the collection of intelligence in respect of a matter which is important in relation to security.<sup>45</sup>
- An internal authorisation does not allow:
  - entry onto premises without permission
  - interference with the interior of a vehicle without permission
  - remote installation of tracking devices or anything authorised under a computer access warrant that is not expressly authorised under an internal authorisation, or
  - the use of a tracking device to listen to, record, observe or monitor the words, sounds or signals of a person.<sup>46</sup>

---

<sup>44</sup> Australian Security Intelligence Organisation Amendment Bill 2020, Schedule 2, s 26G.

<sup>45</sup> *Ibid*, s 26G(6).

<sup>46</sup> *Ibid*, s 26K.

- the Director-General or an SES ASIO employee or ASIO affiliate must take such steps as are necessary to ensure action under the internal authorisation is discontinued where that person is satisfied that the grounds for the internal authorisation have ceased to exist.<sup>47</sup>
- The Director-General must provide the Attorney-General with a written report within three months from when the internal authorisation ceases to be in force (see further details under *Guidelines on internal authorisations* below).<sup>48</sup>
- A warrant is required for the recovery of tracking devices where it would require entry to premises or interference with a vehicle.<sup>49</sup> This creates a further control for circumstances where ASIO needs to engage in a more intrusive activity.

It is a necessary and proportionate response to enable ASIO to use tracking devices under an internal authorisation, rather than under a warrant.

*The ability to orally request and approve internal authorisations does not diminish accountability and should not be removed from the Bill*

The ability to make authorisations orally ensures that ASIO can obtain authorisation in circumstances where time is of the essence. The Bill includes safeguards which ensure that oral authorisations do not diminish accountability. In particular, ASIO must meet the same requirements for oral authorisations as written authorisations, and keep detailed records of the authorisations. The IGIS will retain its powers to inspect ASIO records to ensure that authorisations were properly made within the law.

If the request is made orally, a written record of the request must be made within 48 hours. The record must include:<sup>50</sup>

- the facts and other grounds on which the applicant considers it necessary that the authorisation should be given
- the extent to which the applicant considers that the authorisation will substantially assist the collection of intelligence in respect of the security matter, and
- the period for which the applicant considers the authorisation should remain in force, which must not exceed 90 days.

A written record of an oral authorisation must be made within 48 hours. The record of the authorisation must include:<sup>51</sup>

- the matter that is important in relation to security in respect of which the authorisation is given
- the day and time the authorisation is given
- if the authorisation is given in relation to a particular person—the name of the person (if known) or the fact that the person’s identity is unknown
- if the authorisation is given in relation to an object or a class of object—the object or class of object, and

---

<sup>47</sup> *Ibid*, s 26P.

<sup>48</sup> *Ibid*, s 34AAB.

<sup>49</sup> *Ibid*, s 26R.

<sup>50</sup> ASIO Amendment Bill, Schedule 2, s 26G(5).

<sup>51</sup> *Ibid*, s 26H(5).



- the restrictions or conditions (if any) to which the authorisation is subject.

The Director-General must establish and maintain a register of requests for internal authorisations.<sup>52</sup>

It is therefore not appropriate to amend the Bill to remove the ability for ASIO to request authorisations orally. Oral authorisations allow ASIO to deploy tracking devices quickly when it is necessary to do so, and the Bill provides strong accountability mechanisms.

*Guidelines on internal authorisations are not appropriate or necessary*

It is not appropriate to amend the Bill to create a legislative instrument subject to disallowance containing guidelines relating to internal authorisation. ASIO maintains detailed internal policies for the use of its intrusive powers to ensure that employees and affiliates act with legality and propriety. These policies are continually updated based on changing circumstances and operational experiences. It is not appropriate for them to be legislative instruments, noting they contain classified information regarding ASIO's procedures and tradecraft.

ASIO's responsibilities under the Guidelines under section 8A of the ASIO Act, which are outlined above, provide rules that ASIO must follow in its use of internally authorised tracking devices. The Guidelines are published online for transparency. The IGIS's powers under the IGIS Act, will enable the IGIS to inquire into ASIO's use of internally authorised tracking devices to ensure ASIO acted with legality and propriety. This includes ensuring that ASIO has complied with the ASIO Guidelines.

If the IGIS completes an inquiry into a matter, including matters which relate to ASIO's compliance with the ASIO Guidelines, the IGIS must prepare a report setting out conclusions and recommendations as a result of the inquiry, and give a copy of the report to the head of the Commonwealth agency to which it relates.<sup>53</sup> Where, in the opinion of the IGIS, the head of a Commonwealth agency does not, as a result of the conclusions and recommendations set out in a report, take adequate and appropriate action within a reasonable period, the IGIS may discuss the matter with the Minister for Home Affairs and prepare a report relating to that matter, and give a copy of the report to the Attorney-General and Prime Minister.<sup>54</sup>

The new framework requires the Director-General to provide the Attorney-General with a written report within three months from when the internal authorisation ceases to be in force, outlining the details of:<sup>55</sup>

- the extent to which the authorisation assisted ASIO in carrying out its functions
- the security matter in respect of the authorisation
- the name of any person whose location was determined by the use of the device
- the period which the tracking device was used
- the object on which the device was installed and the premises where the object was located at the time of installation, and
- compliance with restrictions or conditions, if any, stipulated in the authorisation, and variation of the authorisation.

This requirement for the Director-General to report to the Attorney-General in relation to all internal authorisations of tracking devices, in addition to the Attorney-General's role in issuing warrants for

---

<sup>52</sup> *Ibid*, s 26Q.

<sup>53</sup> *Inspector-General of Intelligence and Security Act 1986*, s 22.

<sup>54</sup> *Ibid*, s 24.

<sup>55</sup> ASIO Amendment Bill, Schedule 2, s 34AAB.

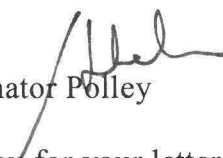
the recovery of tracking devices (if required), provides the Attorney-General with oversight of the authorisation framework.



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

Ref: MC20-011359

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

  
Dear Senator Polley

Thank you for your letter of 18 June 2020, regarding the Standing Committee for the Scrutiny of Bills' consideration of the National Disability Insurance Scheme Amendment (Strengthening Banning Orders) Bill 2020 (the Bill). I appreciate the opportunity to address the issues raised by the Committee as part of its consideration of the Bill, and I provide the following advice:

***Why it is necessary and appropriate to provide the Commissioner with a broad power to ban persons from providing disability services***

The Australian Government is committed to protecting persons with disabilities from violence, abuse, exploitation and neglect. One such protection is to prevent providers and workers who are unsuitable and/or pose a risk of harm to participants from delivering services in the NDIS market. The *National Disability Insurance Scheme Act 2013* (the Act) already provides the NDIS Commissioner with the power to make a banning order prohibiting or restricting a person from providing specified supports or services if the Commissioner reasonably believes that the person is not suitable.

Currently, the Act only allows banning orders against existing NDIS providers and workers. This means banning action cannot be taken against unsuitable providers or workers who are not yet delivering NDIS services because they have not entered the market. This means a provider or worker could potentially enter the NDIS market posing an unacceptable risk to NDIS participants.

The Bill proposes amending the Act to ensure the NDIS Commissioner (the Commissioner) can take appropriate banning action against an unsuitable provider or worker before they enter the NDIS, based on evidence of unsuitability from another sector that delivers services to a vulnerable cohort, for example, aged care or child care.

Without the amendments proposed in the Bill, there is a significant gap in the regulatory arrangements of the NDIS that could undermine the rights of people with disability to live free from abuse, neglect and harm.

Balanced against this, the Act obliges the Commissioner to conduct compliance and enforcement activities in a risk responsive and proportionate manner (paragraph 181D(4)(b)). Therefore, before issuing a banning order, the Commissioner would be expected to consider whether the action would be reasonable, timely and proportionate in relation to the issue in question, what action has been taken previously, and whether there are more appropriate avenues to deal with the issue.

***Whether the bill can be amended to include additional guidance on the exercise of the power on the face of the primary legislation***

Amending the Bill to provide additional guidance on the exercise of the power risks unintentionally narrowing the circumstances in which the Commissioner may make a banning order. This could lead to further unintended gaps in the application of banning orders and risks challenge to the Commissioner's decisions.

In addition, there is already significant guidance in the Act around the exercise of the power. In deciding whether to issue a banning order against a person on the ground that the person is unsuitable, the Commissioner is guided by criteria for assessing the suitability of a person to provide, or be involved in the provision of, services to people with disability that are in the *NDIS (Provider Registration and Practice Standards) Rules 2018* (sections 9 and 10).

Finally, internal and external merits review processes are available to a provider or worker subject to a banning order who disagrees with the Commissioner's decision.

The existing guidance and review mechanisms appropriately balance the Commissioner's ability to protect people with disability and the rights of providers or workers affected by a banning order.

***Why it is necessary and appropriate to leave significant matters, such as what personal information can be included on the Register, to delegated legislation, noting the potential impact on a person's privacy***

The practical effectiveness of a banning order relies on appropriate publication of information about the banned provider or worker on a register accessible to the public.

The matters included in the NDIS Provider Register prescribed by the Rules do not, and will not under the Bill, extend to any highly sensitive or highly personal information about the person subject to the banning order. However, in some instances, such as where an individual or business has a common name, it may be necessary to include information on the NDIS Provider Register to ensure that people with disability and their carers can identify the person who is subject to the banning order. An appropriate amount of identifying information will also avoid confusion with another person against whom banning orders have not been made.

It is highly unlikely that sensitive information would assist in identifying a person. Information on the register would not extend to the nature of the incident that prompted the making of the banning order. However, it may include, for example, a description of the town or area in which the banned person was providing services.

It is necessary to enable a high level of flexibility in relation to the NDIS Provider Register to support the exercise of choice and control by people with disability in response to the developing NDIS market. In this case, the flexibility of enabling additional matters to be prescribed by the rules will allow the Commissioner to respond if situations arise where the person's name and ABN (if any) are insufficient to adequately identify the person.

Any matters prescribed would be directed to objective factors which would avoid confusing the person with someone else, such as the location, nature of services or manner of operation.

Publishing information authorised by rules may impact a person's privacy. However, the overarching aim of a banning order is to protect persons with disability, noting that there must be an objective basis for making the order, and some impact on privacy is necessary to achieve this. The rules are disallowable instruments which are open to scrutiny by the Australian parliament.

The NDIS Provider Register is generally publically available, and persons with disability and their representatives may search to ensure that particular providers or workers are not subject to a banning order. This is an important protection. Similarly, it will be a tool for providers looking to employ workers to ensure the employees they recruit are safe to work with people with disability and provide NDIS services.

In deciding what is to be published, the Commissioner is guided by the principles underlying the provisions in the NDIS Act that preclude the inappropriate disclosure of personal or otherwise sensitive information, as well as privacy legislation. These provisions place appropriate limitations on the Commissioner's discretion to include personal information on the register.

***Whether the Bill can be amended to set out the information that can be included on the Register on the face of the primary legislation***

For the reasons outlined above, it is important for the NDIS Commissioner to have flexibility in relation to the information to be published on the register. Given this, I do not consider it appropriate to include prescription around such information in the primary legislation.

Thank you for bringing these matters to my attention. I trust this information is of assistance to the Committee and I look forward to the Committee's final report.

Yours sincerely

**Stuart Robert**



**Senator the Hon Michaelia Cash**  
Minister for Employment, Skills, Small and Family Business

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

Dear Senator

I refer to correspondence from the Senate Standing Committee for the Scrutiny of Bills (the Committee) seeking my advice in relation to the Payment Times Reporting Bill 2020 (the Bill). I appreciate the Committee's consideration of the Bill and the opportunity to address the issues raised by the Committee.

The Committee has sought my advice on three issues with respect to the Bill. These relate to the broad delegation of investigatory powers, the reversal of the evidential burden of proof and the incorporation of external materials existing from time to time.

**Broad delegation of investigatory powers**

The Committee asked for advice on:

*“why it is necessary to confer investigatory powers on any ‘other person’ to assist an authorised person” and  
“whether it would be appropriate to amend the bill to require that any person assisting an authorised person have the knowledge and expertise appropriate to the function or power being carried out (as is the case with authorised officers under subclause 35(2) of the bill)”.*

The Bill does not confer or delegate any investigatory powers to the ‘person assisting’. Instead, under subsections 31(4) and 32(3) it provides that an authorised person may be assisted by ‘other persons’ in that authorised person’s exercise of investigatory powers.

These provisions are drawn directly from the *Regulatory Powers (Standard Provisions) Act 2014* (the Regulatory Powers Act). As the Explanatory Memorandum for that Act 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 Act.

In the case of the Payment Times Reporting scheme, it is 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 Bill to be amended to require that a person assisting must have the appropriate knowledge and expertise.

### **Reversal of the evidential burden of proof**

The Committee has asked why it is proposed to use an offence-specific defence which reverses the evidential burden of proof in section 46 of the Bill.

Subsection 46(1) provides that an entrusted person will commit an offence if the person uses or discloses protected information in an unauthorised way. Subsection 46(2) creates a defence to the offence in subsection 46(1), if the use or disclosure of protected information was done in good faith and in purported compliance with Part 5 of the Act relating to protected information, or with the Rules.

The rationale for the use of an offence-specific defence in section 46 of the Bill is consistent with the relevant principles set out in the Guide to Framing Commonwealth Offences. As explained in that Guide, it is reasonable and necessary for the burden of proof to be placed on the defendant where the facts in relation to the defence are 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.

In the case of a defence to an offence under subsection 46(1), the defendant is best placed to explain why they should be considered to be acting in good faith and purported compliance with the Act. This is because the defendant is best placed to explain their motivations when engaging in the relevant conduct as to how and why they should be considered to be acting in good faith and in purported compliance with the Act when they disclose protected information. It would also be unnecessary and significantly costly if the prosecution was required to disprove these factors given the prosecution would not have ready access to evidence going to the defendant’s state of mind and motivations.

**Incorporation of external materials existing from time to time**

The Committee has asked “*whether documents incorporated by reference into the Rules will be made freely available to all persons interested in the law*”.

As outlined in the Explanatory Memorandum to the Bill, subsection 58(3) specifies that the definition of a small business in the Rules may apply, adopt or incorporate any matter in an instrument or writing from time to time.

The Payment Times Reporting Small Business Identification Tool (Identification Tool) is an element of the definition of small business contained in subsection 5(1) of the Rules.

The Identification Tool is designed to identify small businesses with an annual turnover of less than \$10 million. The data contained in the Identification Tool will be regularly updated, for example, as small businesses are created, close or their turnover increases to more than \$10 million.

The Identification Tool will reduce the compliance burden for reporting entities by automating the small business identification process. As part of the Identification Tool, a large business will be able to enter supplier information, with the tool identifying whether they need to report payment times for each of their suppliers.

The Identification Tool will be made available on a website. Access to the Identification Tool will be broadly available, subject to appropriate verification and security protocols to ensure that commercially sensitive information contained in the Identification Tool is used for appropriate purposes. The framework by which the Identification Tool will determine which businesses are in or out of scope for the purposes of reporting will be publicly and freely available.

The underlying data for the Identification Tool, including the outcomes of a search by a reporting entity, will only be available to that entity and the Regulator. This is appropriate given the sensitivity of accessing private commercial data, the broader objectives of the scheme, and that we will be giving small businesses the option of opting out of the Identification Tool identifying them as a small business.

I trust this information is of assistance.

Yours sincerely

Senator the Hon Michaelia Cash

25 / 06 / 2020





**The Hon. David Littleproud MP**  
**Minister for Agriculture, Drought and Emergency Management**  
**Deputy Leader of the Nationals**  
**Federal Member for Maranoa**

Réf: MS20-000736

22 JUN 2020

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

scrutiny.sen@aph.gov.au

Dear Senator Polley

Thank you for the Committee Secretary's email of 11 June 2020, regarding the Senate Standing Committee for the Scrutiny of Bills' (the Committee) consideration of *the Primary Industries (Customs) Charges Amendment (Dairy Cattle Export Charge) Bill 2020* (the Bill). I appreciate the time taken to review the Bill and thank you for the opportunity to address the query raised by the Committee.

In paragraph 1.98 of the *Scrutiny Digest 7* of 2020 (the *Digest*), the Committee has requested my advice as to whether a maximum rate of charge that may be imposed on the export of dairy cattle can be included on the face of the Bill.

I acknowledge the scrutiny view of the Committee that it is for the Parliament rather than makers of delegated legislation, to set a rate of tax (paragraph 1.94 refers). Also, that where charges are to be prescribed by regulation, the Committee considers that a maximum charge should be provided on the face of the primary legislation, to enable greater parliamentary scrutiny.

However, in this particular instance, I consider that it is not appropriate or necessary that a maximum charge be specified on the face of the primary legislation because:

- The setting of charges in this particular context (primary industries) is *industry-driven* rather than determined by government. Primary industries are responsible for determining whether to pay a levy/charge, what the levy/charge is imposed on and the purposes for which it is used, as well as recommending what the levy/charge is set at. As a result of the industry-driven nature of the levies system, there is a greater need for flexibility and efficient responses to industry demands. Such flexibility and

efficiency would be undermined by the inclusion of a maximum charge in the primary legislation; and

- The legislation already includes specific safeguards to ensure that arbitrary increases do not occur. In effect, the maximum charge rate that can be imposed will be the rate that is requested by the charge payers themselves, ensuring that charge amounts are not increased in an excessive or undue manner. This provides an appropriate check on power to set rates in delegated legislation, while achieving necessary flexibility and efficiency for industry research and development.

These points are further elaborated on below.

### **Industry driven levy system**

The primary industries levy and charge system is a partnership between government and industry. Primary industries levies and charges are imposed at the request of industry, to allow the relevant primary producers to collectively invest in research and development (R&D) and marketing, biosecurity and residue testing. Primary industries are responsible for determining whether to pay a levy, what the levy is imposed on and the purposes for which it is used. The government's levies policy and the industry-driven process for establishing a levy is set out in the 2009 Levy Principles and Guidelines.

(<https://www.agriculture.gov.au/ag-farm-food/levies/publications>)

Each R&D and marketing component of a primary industries levy or charge is attached to one of the 15 rural research and development corporations (RDCs). The dairy cattle export charge would be attached to Livecorp, the RDC responsible for the livestock export sector. The Australian Government strongly supports this world-leading system. In 2018–19 industry and government invested over \$800 million in the RDCs through levies and matching payments. This comprised over \$500 million in levy payments disbursed for R&D and marketing and almost \$300 million of matching payments.

In 2013, most maximum primary industries charge rates were repealed from the *Primary Industries (Customs) Charges Act 1999*, by the *Primary Industries (Customs) Amendment Act 2013*.

The justification for this amendment is set out in the Explanatory Memorandum for the Primary Industries (Customs) Amendment Bill 2013:

Under the current process, if the government approves a change to a charge rate, the relevant regulations must be amended to impose the new rate. If the proposed charge is above the maximum rate, the Act must also be amended. As amending primary legislation is a lengthy process, the new rate may not come into effect until years after the industry has voted in favour of the change. The delay reduces the responsiveness of the industry and limits the ability of the RDC to provide the level of service needed by the industry.

### **Existing Safeguards**

There are existing safeguards in place to ensure the levy cannot be increased above the \$6 per head requested by industry. Before the Governor-General makes regulations prescribing a charge amount in regulations, the Minister must take into account any relevant

recommendation made to the Minister by Livecorp. Subclause 5(5) of Schedule 2 to the Primary Industries (Customs) Charges Act 1999 specifies that the charge rate cannot be greater than the amount recommended to the relevant Minister by that body.

This safeguard ensures that arbitrary increases do not occur. In effect, the maximum charge rate that can be imposed will be the rate that is requested by the charge payers themselves, ensuring that charge amounts are not increased in an excessive or undue manner.

This safeguard was also inserted by the Primary Industries (Customs) Amendment Bill 2013. The Bill received cross-party support in Second Reading speeches about the Bill, particularly in light of this safeguard feature.

**Consistency across the agricultural levy system**

The Bill does not impose a maximum rate to be set in the primary legislation, which reduces both complexity and regulatory burden while supporting agricultural industries' ability to effectively increase its levy investment. In this regard it is in keeping with the spirit of the Attorney General's Clearer Law principles. The government is currently consulting on changes to streamline and modernise agricultural levies legislation in response to sunseting requirements which will seek amongst other aims, to ensure the legislative scheme is aligned with the Clearer Law principles.

Therefore in the light of all of the above, I advise that it would not be appropriate in this case for the maximum charge to be specified in the primary legislation.

I thank the Committee for its consideration of the Primary Industries (Customs) Charges Amendment (Dairy Cattle Export Charge) Bill 2020, and I trust this advice is of assistance.

Yours sincerely

**DAVID LITTLEPROUD MP**



**The Hon Christian Porter MP**

Attorney-General  
Minister for Industrial Relations  
Leader of the House

MC20-017666

Senator Helen Polley  
Chair  
Senate Scrutiny of Bills Committee  
Parliament House  
CANBERRA ACT 2600  
[Scrutiny.Sen@aph.gov.au](mailto:Scrutiny.Sen@aph.gov.au)

Dear Senator Polley 

I am writing in response to correspondence sent from the Senate Scrutiny of Bills Committee, dated 18 June 2020, requesting further information about the *Privacy Amendment (Public Health Contact Information) Act 2020*.

The correspondence referred to the Committee's *Scrutiny Digest 8 of 2020*, which requested responses to the following questions:

1. *As the explanatory memorandum does not appear to provide a sufficiently detailed justification as to why it is considered necessary and appropriate to impose significant penalties for the offences in proposed sections 94D to 94H, the committee requests the minister's detailed advice as to the justification for the significant penalties that may be imposed under those provisions, by reference to comparable Commonwealth offences and the requirements in the Guide to Framing Commonwealth Offences*

The *Privacy Amendment (Public Health Contact Information) Act 2020* (the Act) was introduced to elevate the interim provisions contained in the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020* (the Determination) into primary legislation. The penalty for non-compliance with a Determination made under the *Biosecurity Act 2015* is imprisonment for five years, a fine of 300 penalty units, or both. These penalties are commensurate with the seriousness of non-compliance, given the Health Minister can only make Determinations under the *Biosecurity Act* during a biosecurity emergency.

The Act maintains the key criminal offences under the Determination and imposes the same penalties of imprisonment for five years, a fine of 300 penalty units, or both. It is important that penalties under the Act mirror those under the Determination to ensure that the same penalty applies to an offence regardless of whether the offence was committed under the Determination or the Act. This approach is consistent with the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, which recommends consistent penalties across legislation.

While the penalties contained in the Act represent unprecedented safeguards for data, the highest possible level of protections are necessary to maintain public confidence in the COVIDSafe app and encourage the installation and use of the app. The COVIDSafe app facilitates effective contact tracing, which is a critical component of Australia's COVID-19 response.

The maximum penalties contained in the Act aim to provide an effective deterrent to the commission of offences under the Act and reflect the seriousness of the offences. While the penalties in the Act are higher than some other penalties imposed under the *Privacy Act 1988*, consistent with the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, this higher penalty is justified because of the serious consequences of the commission of the offence. In addition, the prosecutor and relevant court have the discretion to pursue or impose a range of penalties based on the seriousness of the offence, with only the most serious offences attracting the maximum penalty. Similarly, if prohibited conduct under the Act is investigated as an interference with privacy rather than a criminal offence, the Information Commissioner has discretion to seek a civil penalty proportionate to the seriousness of the interference with privacy.

2. *To clarify the nature and type of information that is collected under the bill, the committee requests the minister's detailed advice as to:*
  - a. *the scope of the information that is collected or generated through the COVIDSafe app, including whether 'COVID app data' includes:*
    - i. *decrypted records of a user's contacts over the previous 21 days, in circumstances where the user has tested positive for COVID-19; or*
    - ii. *data transformed or derived from COVID app data by state or territory health officials; and*
  - b. *when the COVIDSafe app will make a record of a 'digital handshake' between users of the app, and upload that record to the National COVIDSafe Data Store, including:*
    - i. *how close users must be to each other in order for the app to record a 'digital handshake'; and*
    - ii. *how long users must be in proximity to each other for the app to record a 'digital handshake'.*

The following encrypted data is collected or generated through the operation of the COVIDSafe app:

- **Registration data:** this is data collected from a COVIDSafe user when they register for the app, and includes their mobile phone number, name (which can include a partial name or pseudonym), age range and postcode. Based on this information, COVIDSafe generates an encrypted reference code for the app on that device, which is refreshed every 7.5 minutes, enhancing the security of the phone to help protect the privacy of the user.
- **Data collected during a digital handshake:** the COVIDSafe app uses Bluetooth to look for other devices that have the app installed. The details of the contact are securely exchanged between phones through end-to-end encryption. This contact or 'digital handshake' securely logs the other user's encrypted reference code, the date and time of contact, the Bluetooth signal strength of the other COVIDSafe user and the other user's device model. This information is stored locally on the user's device for 21 days before it is deleted.

This period allows for the maximum 14-day incubation period of the coronavirus, and time allowed to confirm a positive test result.

If a user tests positive for COVID-19, they are contacted by a public health official and asked if they consent to upload their encrypted information from their device to the National COVIDSafe Data Store. If the user consents, a public health official sends a unique PIN to the user's app which the user is required to enter on their device to allow the upload to occur. The scope of COVID app data includes decrypted records of a user's contact over the previous 21 days, in circumstances where the user has tested positive for COVID-19, and has consented to upload information to the National COVIDSafe Data Store. Data is only decrypted after it is uploaded to the Data Store.

COVID app data does not include information obtained by state or territory health officials during contact tracing from a source other than directly from the National COVIDSafe Data Store. Any additional information that is collected during the manual contact tracing process will not be COVID app data, even if this information is identical to the COVID app data or is a more complete version of the COVID app data (for example, if a user registered for COVIDSafe with a pseudonym but provided their full name to a state or territory health authority).

The COVIDSafe app collects 'digital handshake' data that is exchanged between users of the app at regular intervals. This contact information is stored on the user's device. Contact information older than 21 days on the device is automatically deleted. It is not technologically feasible to ignore other users' Bluetooth signals beyond 1.5 metres or to limit the collection of Bluetooth signals to 15 minutes contact. This is because the nature of Bluetooth technology means signals can be detected within close proximity and the COVIDSafe app detects the strength of Bluetooth signals rather than the distance. The app estimates the distance between users based on the strength of the Bluetooth signal.

The Government has put in place access restrictions to 'digital handshake' data uploaded to the National COVIDSafe Data Store such that, when a state or territory health official accesses the system, they are only presented with the user's close contacts, defined as contact between users for at least 15 minutes at a proximity approximately within 1.5 metres.

3. *The committee also requests the minister's advice as to how COVID app data will be de-identified, and how the de-identification process will protect the privacy of individuals.*

The Act has been designed to allow only very limited de-identification of COVID app data. Specifically, under paragraph 94D(2)(f), the only de-identified information that can be produced from COVID app data is de-identified statistical information about the total number of COVIDSafe registrations, and this can only be produced by the National COVIDSafe Data Store administrator. This minimises any potential risk of flaws in the de-identification process, or the publication of de-identified information that could be later re-identified.

4. *The committee requests the minister's advice as to whether the offences in section 94H of the Act would apply to making discounts, payments and other incentives (including placing additional requirements or conditions on individuals who have not downloaded the app) contingent on a person downloading or using the COVIDSafe app, or uploading COVID app data to the National COVIDSafe Data Store.*

The Explanatory Memorandum to the Act states that subsection 94H(2) requires that a person cannot cause another person disadvantage by virtue of that person not having COVIDSafe installed, not having COVIDSafe operating on the person's communication device, or not consenting to uploading COVID app data from a communication device to the National COVIDSafe Data Store. The offering of discounts or payments only to persons with the COVIDSafe app installed or in use would likely constitute a disadvantage to a person who does not have the app installed or in use. For example, paragraph 94H(2) specifically provides it is an offence to insist on receiving more monetary consideration for a good or service on the grounds that a person has not downloaded or does not have COVIDSafe in operation, or has not consented to uploading their data to the National COVIDSafe Data Store. Specific conditions or requirements imposed on persons who do not have the COVIDSafe app installed or in use would need to be considered on a case-by-case basis to determine if they would constitute a disadvantage.

5. *Noting that there may be impacts on parliamentary scrutiny where reports associated with the operation of regulatory schemes are not available to the Parliament or published online, the committee requests the minister's advice as to:*
- a. *Why the bill does not require reports prepared by the Health Minister under proposed section 94ZA to be published online; and*
  - b. *Why the bill does not require reports prepared by the Information Commissioner under proposed section 94ZB to be tabled in Parliament*

The Act includes a requirement that the Minister for Health provide a report to Parliament as soon as practicable after each six-month period on the operation and effectiveness of the COVIDSafe app. After these reports are tabled in Parliament they will be publicly accessible online via the Parliament of Australia website. The Information Commissioner is required to publish reports on the Commissioner's performance of functions and exercise of powers under the Act. The Government expects that the Commissioner's report would be similar to the periodic reports the Commissioner publishes on the Commissioner's website about the operation of the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

These reporting requirements underscore the Government's commitment to transparency about the operation and effectiveness of COVIDSafe and the unprecedented privacy and security protections built around the app's data handling. Ensuring the reports prepared by the Minister for Health and the Information Commissioner will be publicly available will also support Parliamentary scrutiny processes.

I hope this information has been of assistance in addressing the Committee's concerns.

Thank you again for writing on this matter.

Yours sincerely

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



## The Hon Darren Chester MP

Minister for Veterans Affairs  
Minister for Defence Personnel

IS20-000002

19 JUN 2020

Committee Secretary  
Senate Standing Committee  
for the Scrutiny of Delegated Legislation  
Parliament House  
CANBERRA ACT 2600

Dear Committee Secretary

Thank you for your invitation to provide information in relation to issues identified in the *Veterans' Affairs Legislation Amendment (Supporting the Wellbeing of Veterans and Their Families) Bill 2020*.

The Committee has sought advice in relation to the following issues identified in the Bill:

- Why it is considered necessary and appropriate to leave the details of the operation of a scheme to provide assistance or benefits to former members to delegated legislation;
- Whether the Bill can be amended to include at least high-level guidance on the face of the primary legislation; and
- The type of documents that it is envisaged may be applied, adopted or incorporated by reference under proposed subsection 268D(4) of the Bill, whether these documents will be made freely available to all persons interested in the law and why it is necessary to apply the documents as in force or existing from time to time, rather than when the instrument is first made.

The following is my response to the issues identified by the Committee:

### Details of operation of scheme to provide assistance or benefits to former members

The proposed provision of assistance or benefits to former members of the Australian Defence Force (ADF) to assist them to transition to civilian work, through the *Military Rehabilitation and Compensation Regulations 2020* will provide the Department of Veterans' Affairs (DVA) with appropriate flexibility to be responsive to the employment related needs of former members. The benefits and assistance are to be provided through the Support for Employment Program.

The embedding of detail of the operation of the program, or future employment related programs, in primary legislation would not allow DVA to be responsive when details of the program such as eligibility criteria, the process for applying for the assistance, and details of the assistance provided need to be quickly changed or updated.



These changes would reflect changes informed by client evaluation of the support or which are required operationally, and would not amend the scope of assistance for which there is authority.

To prescribe these details in the *Military Rehabilitation and Compensation Act 2004* (MRCA) would be to make the smallest required changes (such as to names of employment related training courses) for transitioning veterans, dependant on being passed by Parliament.

The result of prescribing these details in the MRCA would be to leave DVA without the ability to provide employment related training programs which are responsive to, and reflect, the changing requirements of veterans' assistance and training needs and the employment market.

This issue is further compounded with possible uncertainty around Parliamentary sitting periods (as has recently been experienced as a result of COVID-19), and periods of time when Parliament does not sit (such as when it has been prorogued).

Providing the operational detail concerning veteran employment related assistance and benefits, in secondary legislation such as regulations, enables the Department to update the eligibility requirements and the types of pre and post-employment assistance to be provided as required.

The provision of benefits and assistance to former ADF members through delegated legislation is consistent with the method used to prescribe operational details for a range of other forms of assistance or benefits provided to veterans under DVA legislation.

Three such examples are:

1. Current section 268A of the MRCA enables the Military Rehabilitation and Compensation Commission (the Commission) to make a legislative instrument providing family support assistance or benefits to an ADF member or former ADF member, and to provide detail related to the benefits or assistance such as eligibility criteria, conditions on which the benefits or assistance will be granted, and limits (financial or otherwise) on the assistance or benefits, through a legislative instrument.
2. Subsection 286(1) of the MRCA enables the Commission to make a written determination concerning several different aspects of the provision of treatment and pharmaceutical benefits to veterans.
3. Details relevant to the operation of the Veterans' Children's Education Scheme, including eligibility criteria and education allowances, are set out under the *Veterans' Children Education Scheme Instrument 2015 No.R43*. Section 117(5) of the *Veterans' Entitlements Act 1986* refers to a range of aspects of the scheme which the Commission may make provision for, and in relation to, through a written determination.

#### Whether the Bill can provide high-level guidance on the face of the primary legislation

Subject to the Committee's views, reasons which explain and justify why details of the Support for Employment program are most appropriately placed in regulations, can be provided in an Addendum to the Explanatory Memorandum.

Documents envisaged may be applied, adopted or incorporated by reference under proposed subsection 288D(4).

DVA envisages that relevant content from the Support for Employment policy will be possibly adopted or incorporated into the regulations.

Incorporation provisions can be found in other provisions in DVA legislation, such as subsections 268B(5) and 286(6B) of the MRCA. The proposed inclusion of subsection 268D(4) is not inconsistent with this existing practice.

It is necessary and appropriate that the regulations incorporate documents as in force or existing from time to time, to ensure the flexibility of employment related programs to respond to veterans' employment related training needs and provide relevant assistance and benefits which reflect contemporary thinking and research on what former ADF members require to successfully transition to civilian employment.

It is envisaged that the Support for Employment Policy Manual will also be publicly available on DVA's website.

For any further advice concerning this submission the contact officer in DVA is:

Ms Bronwyn Worswick  
General Counsel  
Department of Veterans' Affairs  
Telephone: 0436 803 906  
Email: [bronwyn.worswick@dva.gov.au](mailto:bronwyn.worswick@dva.gov.au)

Yours sincerely

**DARREN CHESTER**