UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Supplementary submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone

Inspector-General of Intelligence and Security

23 November 2018

Introduction

On 14 November, the Committee published a supplementary submission of Department of Home Affairs (submission 18.3). That supplementary submission responds to some of the matters raised in the Inspector-General of Intelligence and Security (IGIS) submission to the inquiry (submission 52) concerning proposed amendments to the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) in Schedules 2 and 5 to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill).

IGIS welcomes the Department's indication that it is considering the matters raised in the IGIS submission, and intends to engage with IGIS.[1] IGIS also welcomes the explanations given by the Department of the ways in which some of the new powers are intended to be exercised. IGIS notes that the suggestions made in our submission for some targeted amendments could help to ensure that the legislation gives clear effect to, and does not unintentionally exceed, the stated intent. This could facilitate effective compliance with, and robust oversight of, the new measures.

Key issues

IGIS makes this supplementary submission to address a number of issues raised by the Departmental submission in explaining why certain provisions are considered necessary, and why certain suggested amendments are considered unnecessary. These issues are outlined below, and concern the interpretation of existing and new provisions of the *ASIO Act*.

Computer access warrants (Schedule 2)

(1) Telecommunications interception (TI)*:* The stated case for the proposal to require all computer access warrants to authorise the use of force against persons and things for the purpose of carrying out TI appears to rely on a need to use force to enter premises for the purpose of conducting TI. The use of force to enter premises is authorised under existing provisions.

(2) Post-warrant concealment powers: The effective reduction of existing safeguards for activities carried out for the purpose of concealment (and in particular, for activities that are likely to cause material interference with the lawful use of a computer, or material loss or damage to a lawful user of a computer).

(3) Temporary removal of computers and 'other things' from warrant premises: The meaning of 'other things' that can be removed temporarily, and the duration of their removal.

Section 34AAA compulsory assistance orders (Schedule 5)

(4) Reliance on implied limitations and executive discretion as a primary source of the legal parameters on the power to compel persons to render certain assistance to ASIO.

Subsection 21A(1) civil immunities for voluntary assistance (Schedule 5)

(5) A range of issues concerning the issuing and administration of requests, including: proportionality of decisions to confer immunities; maximum duration; oral requests, variation and revocation; and interaction with ASIO warrants and technical assistance requests.

Notification and reporting requirements

(6) The importance of notification and reporting requirements to the effective oversight of extended warrant powers, powers to compel assistance, and to confer immunities from liability.

1 Department of Home Affairs, *Supplementary Submission 18.3*, p. 16 at [73], and p. 20 at [105].

1. ASIO's computer access warrants (Schedule 2)

1.1 Telecommunications interception: use of force

Issue

Schedule 2 proposes to amend the *ASIO Act* to enable computer access warrants to authorise ASIO to conduct TI for the purpose of doing any thing specified in the warrant.[2]

IGIS identified a number of potentially unintended consequences arising from this power, including that it would attract the operation of existing provisions that require all computer access warrants to authorise the reasonable and necessary use of force against persons and things for the purpose of doing the acts specified in the warrant. IGIS noted that this would be a material expansion of ASIO's existing TI powers under the *Telecommunications (Interception and Access) Act 1979* (*TIA Act*), as warrants issued under the *TIA Act* do not authorise the use of force against persons or things.[3]

Departmental submission

The Departmental submission appears to suggest that there is a need for ASIO to use force against persons and things for the purpose of conducting TI, stating that:

> *[I]t is long standing practice that entry onto premises may be necessary where it would be impractical or inappropriate to intercept communications in respect of a device otherwise than by using equipment installed on specified premises.*
>
> *This may be due to technical reasons connected with the operation of the service or the telecommunications system of which the service is part, or because the execution of the computer access warrant as a result of action taken by an officer of a carrier might jeopardise the security of the investigation. Accordingly, it is reasonable and necessary to ensure that law enforcement officers undertaking these activities can do so with appropriate authorisations around the use of force.*[4]

IGIS comment

The above explanation appears to conflate a case for using force to enter premises with a case for using further force to carry out TI at those premises once entry is gained. Existing paragraphs 25A(5A)(a), 27A(2)(a) and 27J(3)(d) of the *ASIO Act* already authorise the use of force to enter premises (provided that entry to premises is specified in the relevant warrant).

It is not apparent from the above explanation why an authorisation to use force is needed ***specifically*** for the TI component of a warrant operation (and particularly the use of force against persons) ***in addition to*** the existing authorisation of the use of force for the purpose of entering premises at which an interception activity may be carried out. IGIS oversight of ASIO's TI warrants under the *TIA Act* has not identified any cases in which ASIO has been unable to execute a TI warrant because it could not use force against a person or a thing to conduct an interception activity.

---

2 Schedule 2, items 6 and 11: new ss 25A(4)(ba) and 27E(2)(ea).

3 IGIS, *Submission 52,* pp. 42-43.

4 Department of Home Affairs, *Supplementary Submission 18.*3, p. 6 at [19].

The above explanation also refers to the reasonableness and necessity of ***law enforcement officers*** being authorised to use force against persons and things for the purpose of conducting TI. It should be noted that the power to use force under the *ASIO Act* is not limited to law enforcement officers whose assistance is made available to ASIO.

1.2 Post-warrant concealment powers

Issue

Schedule 2 proposes to amend the *ASIO Act* to extend ASIO's powers to undertake acts that are reasonably necessary to conceal actions done under a warrant. This includes a power to undertake specified intrusive activities for the purpose of concealment. The power to engage in these concealment-related activities extends beyond the duration of a warrant. It does not require the Attorney-General to specifically authorise concealment but rather applies to all warrants issued.[5]

IGIS identified that the one of the new concealment powers is not subject to equivalent limitations and prohibitions on the exercise of the same power for the purpose of accessing and manipulating data held in, or accessible from, a computer. This is the power to use a computer or a communication in transit, including adding, copying or deleting data.[6] The new concealment powers do not contain equivalent limits to those in existing subsections 25A(5), 27A(1)(a) and 27E(5) of the *ASIO Act,* which provide as follows:

- it is only lawful to do any thing that is likely to materially interfere with, interrupt or obstruct a communication in transit if it is ***necessary*** to do one or more of the things authorised in the warrant; and
- it is ***not lawful*** to do any thing that is likely to cause material loss or damage to other persons lawfully using a computer.

Departmental submission

The Departmental submission indicates that the non-application of the existing limitations and prohibitions in subsection 25A(5) (and equivalent provisions ins sections 27A and 27E) to concealment activities under the new powers is considered 'necessary to maintain operational integrity through the manipulation of data'. The submission also indicates that the non-application of the existing safeguards to the new concealment powers is considered to be reasonable and proportionate because 'the purposes for which they are abrogated are very limited'.[7]

5 Schedule 2, items 7, 8 and 12: new ss 25A(8), 27A(3C) and 27E(6).

6 IGIS, *Submission 52,* pp. 48-49.

7 Department of Home Affairs, *Supplementary Submission 18.3,* p. 11 at [50].

IGIS comments

Removal of safeguards from existing concealment powers

As noted in the IGIS submission, existing paragraphs 25A(4)(c), 27A(1)(a) and 27E(2)(f) of the *ASIO Act* currently enable the Attorney-General to authorise ASIO to undertake certain concealment activities while a computer access warrant is in force. Leaving aside the uncertainty about how the existing concealment provisions will interact with the new concealment powers while a warrant is in force,[8] it is notable that the existing concealment provisions ***are subject to*** the limitations and prohibitions on actions likely to cause material interference, or material loss or damage, in existing subsections 25A(5) and 27E(5) and existing paragraph 27A(1)(a), which applies subsection 25A(5).

It is unclear from the above justification why an effective reduction of existing safeguards is needed, especially with respect to the removal of the prohibition on concealment activities that are likely to cause material loss or damage to lawful computer users. In conducting oversight of ASIO's computer access warrants, IGIS has not identified circumstances in which ASIO has been unable to carry out a concealment activity in reliance on existing paragraphs 25A(4)(c), 27A(1)(a) or 27E(2)(f) due to the limitations and prohibitions in subsections 25A(5), 27A(1) and 27E(5) on acts that are likely to cause material interference, loss or damage to lawful computer users.

Compliance and oversight implications

The non-application of existing safeguards to the new concealment powers may also make compliance and oversight difficult. The same or substantially similar activities would be governed by different legal standards based on the specific purpose for which those activities were conducted.

For example, if ASIO sought to use a computer or a communication in transit to gain access to relevant data, it would be subject to the existing limitation on causing material interference and the prohibition on causing material loss or damage. However, if ASIO sought to use a computer or a communication in transit for the purpose of concealing its activities under a warrant (or further concealing its concealment-related actions) then no specific limitations and prohibitions would apply. This may create confusion and compliance risk among officers executing warrants, particularly if these persons need to perform 'access' and 'concealment' related activities in close proximity.

Breadth and duration of new concealment powers

Given the considerable duration and breadth of the new concealment powers, IGIS is doubtful that concealment can be characterised as a 'very limited' purpose for which acts likely to cause material interference, loss or damage can be authorised without the existing, specific limitations.

Concealment activities could be carried out for a prolonged period of time, covering the duration of the warrant (up to six months) and 28 days after its expiry, or at the earliest time thereafter that is reasonably practicable. As the concealment powers extend to the subsequent concealment of concealment-related activities, it is conceivable that post-warrant concealment activities could be carried out for an extended period of time beyond 28 days after the expiry of the warrant.

8 As noted in IGIS, *Submission 52,* p. 48.

Further, the breadth of the definition of a 'computer' in section 22 of the *ASIO Act* means that a single computer access warrant could authorise access to, and concealment activities in relation to, a large number of individual computers. (A 'computer' is defined to mean all or part of one or more computers, computer systems, computer networks, or any combination of these.)

If there is an intention to authorise ASIO to cause material interference without a specific 'necessity' threshold, and to cause material loss or damage to lawful computer users, IGIS would support an extension of the reporting requirement in section 34 to require ASIO to report on concealment activities that cause material loss or damage (in addition to the existing requirement to report on acts that cause material interference). It would also be particularly important for warrant reports to be provided separately to reports on post-warrant concealment activities.[9] This would ensure that post-warrant concealment did not delay the provision of reports on the warrant itself, including notification of material loss or damage caused by concealment activities during the warrant period.

1.3 Temporary removal of computers and 'other things' from premises

Issue

Schedule 2 proposes to enable computer access warrants to authorise the temporary removal of computers and other things from warrant premises, for the purpose of doing a thing specified in the warrant or for the purpose of concealment.[10]

The IGIS submission identified several ambiguities in the new powers and limitations in applicable reporting requirements that would make oversight difficult. This included an observation that the meaning of the 'other things' that may be removed from premises is unclear. IGIS also suggested that consideration is given to a requirement to limit the period of time for which ASIO may remove a computer or other thing from premises within the warrant period. (For example, a requirement that removal may only occur for as long as is reasonably necessary to do the particular thing under the warrant that was the purpose of the removal.)[11]

Departmental submission

The Departmental submission indicated the words 'other things' are intended to denote a category of 'things that are, in some way, needed to execute the [computer access warrant]'. It also noted that 'the Attorney-General is empowered to specify conditions relating to the return of the computers and other things' and that the power to temporarily remove a thing is limited to the duration of the warrant.[12]

9 As suggested in IGIS, *Submission 52,* p. 49.

10 Schedule 2, items 5 and 10: new ss 25A(4)(ac) and 27E(2)(da).

11 IGIS, *Submission 52,* pp.43-48, especially at pp. 44-45.

12 Department of Home Affairs, *Supplementary Submission 18.3,* p. 12 at [53].

IGIS comment

Meaning of 'other things' that may be removed from premises

Even if the words 'other thing' were given the interpretation suggested by the Department, this would not remove uncertainty identified in the IGIS submission about whether a particular thing had the requisite nexus with an activity authorised by the warrant. As warrants authorise a wide range of activities, including accessing premises, that nexus would be very broad and unlikely to provide meaningful guidance or limitation on the things that may be removed, especially in advance of their removal. There would also remain legal uncertainty about whether this construction is correct.[13]

IGIS therefore continues to support explicit statutory clarification of the 'other things' that can be removed from premises in addition to computers (for example, by creating a class of things in the nature of computer peripheral devices, which would include data storage devices and electronic equipment). Alternatively, the temporary removal power could be limited to the purpose of doing specific things under a warrant that are for the direct purpose of gaining access to relevant data held in the target computer and subsequent concealment of those activities (for example, the acts authorised by paragraphs 25A(4)(a), (ab) and (b) and equivalent provisions in sections 27A and 27E).

Duration of temporary removal

IGIS agrees with the reasoning implicit in the Departmental submission that new paragraphs 25A(4)(ac) and 27E(2)(da) confer a 'compound' power to remove ***and*** then return computers and other things. That is, the power to remove a computer or other thing would be is conditional on its subsequent return, and both actions must be done during the warrant period.

The comments raised in IGIS's submission are directed to a different issue. A maximum removal period equivalent to the total duration of the warrant may be a protracted length of time (up to six months). The removal period for post-warrant concealment activities may be open-ended (28 days after expiry of the warrant, or the earliest practicable time thereafter). To ensure the proportionate exercise of the removal power, IGIS continues to support further statutory parameters on the duration of removal ***within*** the warrant period or post-warrant concealment period.

In particular, new paragraphs 25A(4)(ac) and 27E(2)(da) could be made subject to similar conditions to those in existing subsections 25(4C) and 27D(5) in relation to the removal of things from premises under an ASIO search warrant. This would mean that a computer or other thing may only be removed for as long as is reasonably practicable to do the act or thing that is the purpose of removal. Or, if the return of the computer or other thing would be prejudicial to security after this time, it may only be retained until its return would no longer be prejudicial. In addition to providing clarity, such conditions may help to ensure that the limits of the new temporary removal powers are not unavoidably breached if a computer or other thing could not be returned while a warrant is in force because this would cause prejudice to security.

---

13 In particular, the words 'other thing' could be construed by reference to the preceding word 'computer', or by reference to the purpose of the warrant to authorise access to relevant data held in the target computer. On this interpretation, the 'other thing' would need to have a direct connection with ***a computer on the premises***, or the ***target computer specified in the warrant***. This is ***narrower*** than a nexus with the general purpose of 'executing the warrant' by doing one of the authorised things. Significant ambiguity may therefore remain, which may complicate compliance and oversight.

2. Compulsory assistance orders to ASIO (s 34AAA, Schedule 5)

Issue

New section 34AAA proposes to confer a new coercive power on ASIO via a scheme of 'assistance orders' under which the Attorney-General may, at ASIO's request, issue an order requiring certain persons to assist ASIO in accessing data held in, or accessible from, a computer or data storage device that is accessed or seized by ASIO under warrant.[14] The IGIS submission identified a number of ambiguities and apparent limitations in safeguards to the issuing and execution of these orders.[15]

Departmental submission

The Departmental submission commented on some of the matters raised in the IGIS submission, noting that it was continuing to consider the matters raised by IGIS.[16] Its initial comments indicated:

- there is an intention for assistance orders to be available in relation to persons who are unknowingly or unintentionally involved in activities that are prejudicial to security;[17]
- there is no intention for assistance orders to authorise the deprivation of liberty or inhumane treatment of persons who are providing assistance under compulsion;[18]
- the requirements in new subsection 34AAA(3) for assistance orders to specify certain conditions (the place a person must attend including the compliance period) are intended to be ***additional safeguards*** to be applied only if a computer is not on warrant premises, rather than essential matters to be specified in all orders. This seems to be based on an intention that if a computer is ***not*** removed from premises, 'it is implicit that the person will provide assistance at the time of the warrants executions and in a manner consistent with the issued warrant';[19]
- the requirements for a person to be served with an assistance order, and for any compliance period to commence no sooner than the time of service, are considered to be 'implicitly provided for' in elements of the offence for non-compliance in subsection 34AAA(4);[20] and
- the Department intends to work with the IGIS to determine if further amendments are needed to enable effective oversight of the potential for multiple coercive powers, including assistance orders, to be exercised against a person in relation to the same or substantially similar matters.[21]

14 Schedule 5, item 3.

15 IGIS, *Submission 52,* pp. 59-67.

16 Department of Home Affairs, *Supplementary Submission 18.3,* p. 16 at [73].

17 Ibid, p. 7 at [26] and p. 19 at [99]-[100].

18 Ibid, p. 16 at [75]-[76].

19 Ibid, p. 19 at [101]-[102].

20 Ibid, p. 20 at [103].

21 Ibid, p. 20 at [104]-[105].

IGIS comment

Persons who are unknowingly or unintentionally involved in prejudicial activities

IGIS is assisted by the Department's confirmation that assistance orders are intended to be available in relation to persons who are unknowingly or unintentionally involved in activities that are prejudicial to security. This may mean that orders could be issued in relation to a very broad range of persons. (For example, telecommunications carriers and carriage service providers and others in the communications supply chain whose provision of services, facilities or equipment may unknowingly enable users to engage in communications to advance prejudicial activities.)

As noted in the IGIS submission, the basis upon which a person is said to be 'involved in' prejudicial activities will be a factor that IGIS considers in assessing the proportionality of ASIO's requests to the Attorney-General for the issuing of assistance orders, in line with the requirements of paragraph 10.4 of the current *ASIO Guidelines.* The nature and degree of a person's involvement in prejudicial activities will also be material to an assessment of the propriety of ASIO's actions in considering whether to request the issuing of an order subject to conditions, and if so, the substance of those conditions. Consequently, IGIS continues to support the updating of the *ASIO Guidelines* to provide specific guidance on proportionality and other matters with respect to assistance orders.

Safeguards against arbitrary deprivation of liberty, including access to the IGIS

IGIS welcomes the statement of policy intention that assistance orders should not authorise the detention or arbitrary deprivation of liberty of the persons who are compelled to attend a specified place to provide information or assistance to ASIO. IGIS suggests that the Committee considers whether the Bill contains adequate safeguards to ensure that the power cannot be exercised in a manner contrary to the stated intent.

The Departmental submission also appears to indicate that statutory safeguards relating specifically to access to the IGIS are considered to be unnecessary, such as requirements for ASIO to inform a person of their right to complain to IGIS; and to ensure that the person has access to facilities to make such a complaint while attending a place under compulsion. This was said to be because 'information pertaining to lodging complaints against ASIO with the IGIS is freely available and the IGIS is empowered to inspect requests to the Attorney-General for assistance orders'.[22]

IGIS cautions against assuming that all individuals who come into contact with ASIO under an assistance order will be independently aware of the role of the IGIS and their right to make a complaint. It would also be unsound to assume that persons who attend a place under compulsion will necessarily have access to facilities to contact IGIS to make a complaint about their treatment while they are in attendance.

Further, IGIS's inspection function alone may not be sufficient to ***prevent*** the risk that an order may be executed against a person in a manner results in an arbitrary deprivation of liberty. This is because IGIS inspections are conducted on a retrospective basis (after a warrant, or in this case an assistance order, is issued and executed).

22 Department of Home Affairs, *Supplementary Submission 18.3,* p. 16 at [76].

Consequently, it would also be necessary for there to be a mechanism to ensure that persons who are subject to assistance orders are informed of their right to complain to IGIS while they are attending a place under an order, and to ensure that they have facilities to do so at this time.

Conditions that must be specified in assistance orders

IGIS remains of the view that the requirements in subsection 34AAA(3) are necessary components of ***any*** coercive assistance order that operates in connection with an ASIO warrant; and not merely additional safeguards that are needed only if ASIO has removed a computer from premises.

The Departmental submission suggests that, where a computer is not removed from premises, the essential conditions of the kind listed in subsection 34AAA(3) would in some way be 'implicit' in assistance orders, arising from the terms of the underlying warrant. IGIS considers that reliance on this assumption would raise significant legality and propriety risks.

It would be preferable for section 34AAA to include a statutory requirement for all assistance orders to explicitly state all of the relevant details about a person's compliance obligations, such as the place and time at which the person must attend to give assistance; or other particulars about how the assistance is to be provided, for example, a compliance period for the provision of information. This would ensure that a person who is subject to an order is made aware of his or her obligations and rights; and that these details are placed before the Attorney-General in all requests for orders.

Service requirements

IGIS is concerned that reliance on 'implied' requirements for the service of orders does not provide certainty about the content of a person's compliance obligations, or ASIO's obligations in relation to requesting and executing orders. IGIS continues to support statutory requirements.

Multiple coercive powers

IGIS would welcome consultation by the Department on this matter. As a starting point, a provision in the nature of section 34D of the *ASIO Act* (requirements for requests for questioning warrants) would provide a useful model for a statutory requirement for ASIO to inform the Attorney-General of previous assistance orders issued or requested in relation to a person, and other coercive powers.

3. Civil immunity for voluntary assistance to ASIO (s 21A, Schedule 2)

Issue

New subsection 21A(1) proposes to authorise the Director-General of Security, or a delegate, to confer civil immunities on persons who voluntarily assist ASIO in the performance of its functions, in accordance with a request made by the Director-General or delegate.[23] The IGIS submission identified a number of apparent gaps and limitations in safeguards in the scope of, and issuing thresholds for, the power to confer civil immunities; and in procedural provisions.[24]

23 Schedule 5, item 2 (and power of delegation in item 1).

24 IGIS, *Submission 52,* pp, 51-59.

Departmental submission

The Departmental submission commented on some issues raised in the IGIS submission, including:

- Section 21A requests are not intended to be used interchangeably with technical assistance requests (TARs) under the *Telecommunications Act* (Schedule 1), although there is no statutory prohibition on the use of section 21A requests in a manner that is contrary to that intent;[25]
- Section 21A requests are not intended to circumvent ASIO's existing warrant requirements;[26]
- The civil immunity is not subject to a specific exclusion of conduct causing serious harm or injury to a person. The Department stated that it considers the existing limitations (directed to loss of or damage to property, and conduct constituting an offence) 'are sufficiently broad to capture instances of meaningful harm to other persons'; as well as the voluntary nature of requests, and the seniority of the Director-General as the person exercising the power to confer immunity;[27]
- It is not considered necessary for requests (and therefore the civil immunity) to be subject to a maximum duration for various reasons relating to: the voluntary nature of requests; the intended exercise of the new power (including in connection with a warrant); and the potential for associated contracts, agreements or other arrangements to specify a compliance period;[28]
- It is not considered necessary to limit the circumstances in which requests can be made orally (namely, if circumstances of urgency would prevent them from being made in writing) because 'the Department is comfortable with the current approach as it provides flexibility for ASIO to issue an assistance request in a format that is most appropriate for the operational circumstances';[29] and
- It is intended that the power to issue a request also contains implied powers to vary or revoke that request (separately to the power in subsection 33(3) of the *Acts Interpretation Act* in relation to the power to revoke or vary decisions made by instrument).[30]

IGIS comments

Relationship of section 21A requests with TARs and special powers warrants

IGIS welcomes the acknowledgement that section 21A requests are not intended to be used interchangeably with TARs, or to circumvent requirements for ASIO to obtain a warrant.

This intent is not implemented by the provisions of section 21A. An express provision would ensure that section 21A requests can ***only*** be utilised in accordance with the policy intent, and that the intended use of section 21A is clearly communicated to all persons who may exercise powers under the provision, or who are affected by the exercise of those powers. It could take the form of a

25 Department of Home Affairs, *Supplementary Submission 18.3,* pp. 16-19 at [78]-[96].

26 Ibid, p. 17 at [85].

27 Ibid, p. 17 at [81]-[84].

28 Ibid, p. 17 at [87]-[88].

29 Ibid, p. 18 at [94].

30 Ibid, p. 19 at [95]-[96].

'relationship with other laws' provision to the effect that a section 21A request cannot be issued in circumstances in which a TAR could be issued; or if ASIO would require a warrant or an authorisation to undertake the relevant activity.

Conduct causing serious personal harm or injury

IGIS remains of the view that a statutory exclusion of conduct causing serious personal harm or injury is needed to provide a clear safeguard to the proportionate exercise of the power to confer civil immunities, which facilitates both compliance and oversight. The provisions of subsection 21A(1) do not support a conclusion that the legislative framework governing the conferral of civil immunities excludes all 'instances of meaningful harm to other persons'. Conduct constituting the tort of negligence would not be excluded from the immunity, since the civil standard for negligence falls short of criminal thresholds, but can result in loss of life and serious personal injury or harm.

The fact that compliance with a request made under subsection 21A(1) is voluntary does not ameliorate the risk that the provision will confer a power to grant immunities for conduct that causes serious harm or injury to third persons. The discretion of the person whose assistance is requested is not a substitute for safeguards to ensure that ASIO's decisions to confer immunities are proportionate; and that ASIO has means to ensure that acts done in reliance on the immunities it has conferred are, and remain, proportionate.

IGIS cautions against relying primarily on the level of seniority of a decision maker in substitution of clear statutory parameters on the exercise of discretion by that person to ensure the proportionality of the decision. This is particularly important where powers conferred on an agency head are delegable to a large number of persons, as is the case for the power to confer immunities under new subsection 21A(1).

Maximum duration

IGIS continues to support a statutory maximum period of effect for the immunities conferred under new subsection 21A(1). The Departmental submission appears to indicate that civil immunities are not intended to operate indefinitely (and may be linked, for example, to the duration of an individual warrant operation; or the terms of a contract made under subsection 21A(4) in relation to conduct engaged in under the request). Attempts to imply a period of effect into a request from the terms of a separate legal instrument such as a warrant or a contract would introduce significant complexity and uncertainty. A statutory maximum period of effect would also provide a mechanism for the periodic re-assessment of whether an immunity remains necessary and proportionate.

Oral requests

IGIS continues to support a default requirement that requests are to be made in writing, unless it would be impracticable for a request to be made in writing due to circumstances of urgency. It is common that powers which authorise activities that would impact significantly on the legal rights of other persons are required to be exercised in writing, unless the decision-maker is satisfied that there would be some kind of operational detriment in giving written authority. It is unclear from the explanation provided in the Departmental submission why a general requirement to make a request in writing, subject to an exception to enable the making of an oral requests in urgent circumstances, would unacceptably limit operational flexibility.

Reliance on implied powers of variation and revocation

There can be significant legal uncertainty about the existence, scope and limits of implied powers to vary or revoke administrative decisions. An express statutory power to vary and revoke section 21A requests (consistent with technical assistance requests in Schedule 1) would be important in providing clarity and certainty to persons who are the subject of requests, and in providing clear and transparent standards against which IGIS could conduct oversight.

4. Notification and reporting requirements (Schedules 1, 2 and 5)

Issue

The IGIS submission and the evidence of the Inspector-General at the public hearing on 16 November identified an absence of reporting and notification requirements applying to the new powers to compel assistance and to confer broad civil immunities in Schedule 1 (concerning ASIO, ASD and ASIS) and Schedules 2 and 5 (concerning ASIO).

IGIS noted that the absence of such requirements (which presently apply to similar powers, including in the *ASIO Act*) would present significant difficulties for the effective oversight of intelligence agencies' actions in exercising the new powers. IGIS suggested that all of the new powers should be subject to periodic reporting requirements; as well as 'per use' notifications to IGIS of the conferral and enlivenment of immunities from legal liability in Schedules 1 and 5.[31]

Departmental submission

IGIS understands that the Department considers reporting or notification requirements to be unnecessary in relation to assistance orders under new section 34AAA and civil immunities conferred under new section 21A, principally because reporting is thought to be an additional level of oversight that is reserved for warrant-based activities. The Departmental submission further indicated that 'mandatory reporting for assistance [requests] under 21A is also unnecessary considering its voluntary nature'.[32]

IGIS comments

IGIS continues to support the inclusion of notification and periodic reporting requirements for the reasons given in the IGIS submission and in oral evidence to the Committee.

Facilitation of efficient and effective oversight

Notification and reporting requirements would enable limited oversight resources to be targeted effectively to areas of identified risk in the exercise of coercive and otherwise intrusive powers. In the experience of IGIS, statutory reporting and notification requirements also promote better record keeping practices by agencies about their exercise of powers.

31 IGIS, *Submission 52,* at [1.4], [.1.5], [1.6], [1.9], [2.1.3], [2.2.4], [2.2.7], [5.1.8] and [5.2.6].

32 Department of Home Affairs, *Supplementary Submission 18.3,* p. 19 at [99]-[100].

Reporting (for example, on a warrant operation after it has concluded; or six monthly reports on special intelligence operations) also assists IGIS to develop a comprehensive understanding of the way in which powers are used; how they have assisted agencies in performing their functions; and to identify systemic compliance issues or risks, ideally at an early stage before there is a need for major remedial action.

Existing statutory notification and reporting requirements for similar intrusive powers

The *ASIO Act* currently contains reporting and notification requirements for intrusive powers of a similar nature to those in new section 34AAA (coercive powers) and subsection 21A(1) (powers to confer immunities from legal liability).

Reporting on coercive powers

ASIO's questioning warrants, like section 34AAA assistance orders, enable ASIO to compel people to provide information that assists ASIO in performing its functions. This includes the compulsion of people who are not personally suspected of involvement in activities prejudicial to security (or of being knowingly or intentionally involved).

Reporting on powers to confer immunities

Further, ASIO's special intelligence operations, like subsection 21A(1) assistance requests, involve the conferral of immunities from legal liability on persons who are providing various forms of assistance to ASIO. Both questioning warrants and special intelligence operations are subject to specific notification and reporting requirements.[33]

It is also notable that the *Intelligence Services Act* prescribes specific notification and reporting requirements for the limited circumstances in which the Directors-General of ASIS, ASD and AGO issue emergency authorisations for their agencies to engage in certain intrusive activities in relation to Australian persons. These activities attract the application of immunities from legal liability in section 14 of that Act and section 476.5 of the *Criminal Code*.[34]

Voluntary nature of s 21A(1) requests

The fact that a person's compliance with a request under subsection 21A(1) is voluntary does not diminish the need for IGIS to have an efficient means of visibility over the legality and propriety of the exercise of powers by intelligence agency officials to confer immunities from legal liability. The degree of intrusion into the legal rights of innocent third parties (by removing their rights to legal remedies for loss or injury) is significant, as is the devolution of that power to agency officials.

A person's participation in an ASIO special intelligence operation (in which they are conferred with civil immunity as well as criminal immunity) is also voluntary. However, statutory reporting and notification requirements apply to those operations. These include specific reporting requirements if immunities for causing loss or damage are enlivened, or if statutory limitations are breached.[35]

33 *ASIO Act*, sections 34ZH, 34ZI, 34ZJ (questioning warrants) and sections 35PA and 35Q (SIOs).

34 *ISA,* subsections 9B(4A), (5) and (6).

35 *ASIO Act*, subsection 35Q(2A).