UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

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

Supplementary submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone

Inspector-General of Intelligence and Security

21 January 2019

Introduction

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this supplementary submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Act) with specific reference to Government amendments introduced and passed on 6 December 2018. Information about the role of the IGIS is at **Attachment A**.

This submission responds to an invitation to provide certain additional information following the commencement of the Act on 9 December 2018. It supplements the Inspector-General's correspondence to the Committee of 6 December 2018 (received as submission 1 to this inquiry).

IGIS response to PJCIS recommendation 5 on the Bill

The Inspector-General's correspondence of 6 December 2018 responded to recommendation 5 of the Committee's report on the Bill. The Committee recommended that IGIS and Ombudsman should provide assurances directly to the Committee that the amendments to the Bill agreed to by the Government address their concerns about the matters listed in that recommendation:

- *explicit notification and reporting requirements when issuing, varying, extending or revoking a notice or request under Schedule 1;*
- *limits on the exercise of Schedule 1 powers (including extending prohibition on systemic weakness to voluntary notices, ensuring decision-makers consider necessity and intrusion on innocent third parties when issuing a notice);*
- *defences for IGIS officials; and*
- *clear information sharing provisions.*

IGIS commented, in summary, that:

- Given the urgency, the Government amendments implementing the Committee's recommendations on Schedule 1 (and the matters of defences for IGIS officials and information-sharing as relevant to provisions in Schedules 2 and 5) satisfactorily addressed the concerns raised by IGIS about the particular matters identified in recommendation 5. IGIS also welcomed the further Government amendments to Schedules 2 and 5 (ASIO powers) that addressed some, but not all, of the additional concerns identified in our evidence to the Committee.
- A number of IGIS's other concerns about Schedules 1, 2 and 5 (which were not the subject of specific recommendations in the Committee's report on the Bill) were not implemented in the Government amendments. IGIS noted that, as an interim measure, these matters could be dealt with in the *Minister's Guidelines to ASIO* made under section 8A of the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) pending further reviews. IGIS would oversee ASIO's compliance with the amended guidelines in exercising the new powers.
- Oversight of ASIO's use of the new powers (and to a lesser extent, the use by ASIS and ASD of technical assistance requests) would nonetheless be complex and resource intensive for IGIS.

Implementation of the amendments

Oversight, including resourcing

Information about IGIS involvement to date in overseeing the new powers is provided in a classified annexure. IGIS is also aware that agencies are currently updating, or are intending to update, their internal documentation to support the exercise of the new powers. IGIS anticipates being consulted on these in due course.

While it is too early to comment meaningfully on the whether the provisions are conducive to effective oversight (by reference to practical experience) IGIS has directed resources to developing oversight methodologies for the new powers, and will keep the Committee apprised.

IGIS remains of the view provided in the Inspector-General's evidence to the Committee in 2018 that it will eventually be necessary for IGIS to have approximately five additional staff (full-time equivalent) in order to conduct appropriately thorough and rigorous oversight of the new powers.[1] While this need can be met temporarily from existing resources, this will be difficult to sustain when the *IGIS Act* is amended to confer jurisdiction on IGIS for the oversight of the intelligence functions of a further four agencies in the national intelligence community. It will also be necessary to monitor the adequacy of resourcing and other arrangements continuously, so that IGIS has appropriate access to independent technical expertise.

Amendments to the Minister's Guidelines to ASIO

IGIS has not received any indication from ASIO or the Department of Home Affairs as to whether amendments to the *Minister's Guidelines to ASIO* are being prepared to implement, at least on an interim basis, the large number of matters identified in IGIS's submissions on the Bill that were not included in the Government amendments to the Bill. Without amendments to the Guidelines, these matters remain unaddressed, either directly in primary legislation or in administratively binding guidelines made under the *ASIO Act*. (The key outstanding concerns are summarised below.)

Outstanding IGIS concerns not addressed in the Act

IGIS has a number of outstanding concerns about Schedule 1 (industry assistance scheme), Schedule 2 (ASIO computer access warrants) and Schedule 5 (ASIO power to grant civil immunities to persons providing voluntary assistance, and a new scheme of compulsory assistance orders).

These concerns are detailed in **Attachment B** (Schedule 1) and **Attachment C** (Schedules 2 and 5). Of these, the most significant concerns are about Schedule 5 and to a lesser extent Schedule 2.

Key outstanding concerns in relation to Schedule 5 (assistance to ASIO)

Immunities from civil liability for persons assisting ASIO: ASIO Act, s 21A(1)

- **No proportionality assessment:** The Director-General of Security (or delegate) is not required by the Act to be satisfied that the conferral of civil immunity is reasonable and proportionate, as a precondition to granting the immunity. (This is in contrast to proportionality requirements in the statutory authorisation criteria applying to the Attorney-General for ASIO's special intelligence operations, which also confer civil immunity on participants.)

1 IGIS, *Committee Hansard*, 27 November 2018, p. 5.

- **No exclusion of certain harmful conduct:** The immunity is not subject to an exclusion for conduct causing significant financial loss, or serious physical or mental harm to a person. (The exclusions in s 21A(1) apply only to significant loss of or damage to property, and conduct involving the commission of an offence.)
- **No maximum period of effect:** Requests for voluntary assistance, and consequently the civil immunity, are not subject to any maximum period of effect.

Compulsory assistance orders: ASIO Act, s 34AAA

- **Not all assistance orders are required to specify essential matters:** an assistance order is only required to specify certain essential matters (the compliance period, place of attendance and conditions on the order) if a computer has been removed from premises under a warrant. If a computer is accessed wholly remotely under a warrant, there is no requirement for orders to specify these matters, which may reduce transparency.
- **Arbitrary deprivation of liberty**: there are no express safeguards against the risk that an order requiring a person to attend a place to provide assistance may result in an arbitrary deprivation of liberty.
- **No obligation to cease action taken under an order where issuing grounds no longer exist:** the Director-General of Security is not subject to a statutory requirement to take all reasonable steps to cease executing an assistance order, if he or she is satisfied that the issuing grounds have ceased to exist. (This is in contrast to a statutory obligation in relation to warrants.)

Key outstanding concern in relation to Schedule 2 (ASIO warrants)

- **Limitation on warrant reporting—temporary removals of computers and other things:** Warrant reports under s 34 of the *ASIO Act* are not required to identify specifically whether a computer or other thing was removed from premises. Existing reporting requirements in s 34 will only apply if ASIO makes an assessment that a temporary removal of a computer or thing caused material interference with the lawful use of a computer. This will make it difficult for IGIS to oversee the exercise by ASIO of the new temporary removal powers, including ASIO's decision making about whether a removal caused a material interference.

IGIS views

IGIS continues to support the express inclusion of all outstanding matters in primary legislation or, at least as an interim measure, in Ministerial guidelines made under the *ASIO Act*. It is particularly important for the key issues listed above to be addressed promptly, as they are critical to the effective oversight of the new and expanded powers in Schedules 2 and 5 to the Act.

In conducting its present review of the Act, or potentially in its later statutory review, the Committee may wish to consider whether some or all of these matters should be pursued; and if so, the appropriate vehicle for giving effect to them (both immediately and in the longer term).

IGIS notes that placing these matters solely in Ministerial guidelines has the potential to be more expeditious than legislative means, if those guidelines are made promptly. It may also maximise flexibility in making future amendments to accommodate changes to operational circumstances. However, including at least the key parameters in primary legislation (with further, more procedural details able to be set administratively) may provide a stronger degree of clarity, certainty and parliamentary oversight. (This would include Parliamentary approval of future amendments through the passage of amending legislation, including any proposals to repeal the original provisions.)

Attachment A

Role of the Inspector-General of Intelligence and Security

The IGIS is an independent statutory officer who reviews the activities of the following agencies:

- Australian Security Intelligence Organisation (ASIO);
- Australian Secret Intelligence Service (ASIS);
- Australian Signals Directorate (ASD);
- Australian Geospatial-Intelligence Organisation (AGO);
- Defence Intelligence Organisation (DIO); and
- Office of National Intelligence (ONI) (formerly the Office of National Assessments).[2]

The Office of the IGIS is part of the Attorney-General's portfolio, and was previously located in the Prime Minister's portfolio from its commencement on 1 February 1987 until 10 May 2018. The IGIS is not subject to direction from any Minister on how responsibilities under the *Inspector-General of Intelligence and Security Act 1986 (IGIS Act)* should be carried out. The Office has 27 staff at 21 January 2019.

The *IGIS Act* provides the legal basis for the IGIS to conduct inspections of the intelligence agencies and to conduct inquiries of the Inspector-General's own motion, at the request of a Minister, or in response to complaints. The overarching purpose of the IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.[3] A significant proportion of the resources of the Office are directed towards ongoing inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action. IGIS staff have access to all documents of the intelligence agencies, and the IGIS is often proactively briefed about sensitive operations.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries, the IGIS has strong investigative powers, including the power to require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve classified or sensitive information, and the methods by which it is collected. Conducting an inquiry is resource intensive but provides a rigorous way of examining a complaint or systemic matter within an agency. The Inspector-General also receives and investigates complaints and public interest disclosures about the intelligence agencies. These come from members of the public and from current and former agency staff.

In response to the recommendations of the *2017 Independent Intelligence Review*, the Government announced that, subject to the introduction and passage of legislation, the jurisdiction of the IGIS will be extended to include the intelligence functions of the Department of Home Affairs, Australian Federal Police, Australian Criminal Intelligence Commission and Australian Transaction Reports and Analysis Centre. Resources for the IGIS are being increased to allow the office to sustain a full time equivalent staff of 55 (by 2019-20) and to allow the agency to move to new premises (in 2019).

---

2 *Office of National Intelligence Act 2018* and *Office of National Intelligence (Consequential and Transitional Provisions) Act 2018* (commenced 20 December 2018).

3 See *IGIS Act,* section 8 in relation to the general jurisdiction of the IGIS.

Attachment B

Implementation of IGIS concerns included in recommendations 5 and 17

PJCIS recommendation 5

The Committee recommends that the Bill be amended to incorporate suggestions from the Office of the Inspector-General of Intelligence and Security (IGIS) to strengthen oversight of the powers in Schedule 1 of the Bill, as it applies to the Australian Security Intelligence Service (ASIO), the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD).

This includes:

- ***explicit notification and reporting requirements when issuing, varying, extending or revoking a notice or request under Schedule 1;***

Partially implemented

Addressed in Government amendments

- ✓ Notification of issuing, extending or revoking TAR, TAN or TCN.
- ✓ Notification of IGIS when a TCN consultation request issued.
- ✓ Requirement to inform a DCP of their right to complaint to IGIS in relation to a TAN (but not the execution of a TCN).
- ✓ Provision of assessor's report to IGIS.
- ✓ Classified statutory annual reporting by ASIO (numbers issued).

Not implemented

- × No annual reporting by ASIS and ASD.
  (This could be done administratively. IGIS has not been advised of any commitment to do so.)
- × No notification of IGIS by ASIO, ASIS or ASD if a provider does an act under a TAR, TAN or TCN in reliance or purported reliance on the civil or criminal immunity that causes significant loss, damage, injury or interference with lawful computer use (and annual reporting of statistical information about these instances, on a classified basis if necessary).

- ***limits on the exercise of Schedule 1 powers (including extending prohibition on systemic weakness to voluntary notices, ensuring decision-makers consider necessity and intrusion on innocent third parties when issuing a notice);***

Partially implemented

Addressed in Government amendments

- ✓ Prohibition on TARs requesting the creation or non-remediation of systemic weaknesses or vulnerabilities.
- ✓ Proportionality requirement in issuing, variation and revocation criteria for TARs, TANs, TCNs, including a requirement to consider impacts on some third parties *(however, this is only those persons who are not of interest to intelligence agencies).*
- ✓ Fixed maximum period of effect for TANs and TCNs *(however, this does not apply to TARs, which are only subject to a 90-day maximum if the TAR does not specify an expiry date.).*

Continued

Not implemented

- ✗ No express requirement for persons issuing TARs, TANs and TCNs (as applicable) to consider the potential impacts of an immunity on **all** third parties who may be affected by the DCP's actions under the request or notice; only the those persons who are **not** of interest to ASIO (in relation to TARs, TANs and TCNs) or ASIS or ASD (in relation to TARs).
- ✗ No fixed maximum period of effect for TARs. *(90-day maximum in s 317HA(1) applies only if the TAR does not specify an expiry date. There is no limit on the expiry date that can be specified.)*
- ✗ No statutory clarification of overlap between TARs and ASIO s 21A(1) requests.
- ✗ No further limitations on civil immunities (exclusion of conduct causing serious financial loss, damage to property, personal injury or harm, or an offence).
- ✗ Criminal immunities from computer offences for communications providers under TARs, TANs and TCNs remain broader than those applying to intelligence agencies for the same conduct.
- ✗ No requirement for the Attorney-General to give s 317S procedures for making TCN requests to IGIS, including any amendments to those procedures. *(This could be done administratively, but a statutory requirement would provide greater certainty that this would be done consistently.)*
- ✗ No requirement for ASIO's warrant reports to identify whether a TAR, TAN or TCN was used to request or compel a DCP to do a thing under a warrant.
- ✗ The exception in s 317ZH(4)(f) would allow ASIO to issue a TAN that 'gives effect to' one of its warrants by requiring the DCP doing an act or thing specified in the warrant is not explicitly limited to warrants that are in force at the time the TAN was issued (and not subsequently). *(This observation also applies to TARs and TANs issued by ASIO, TCNs issued for the benefit of ASIO, and TARs issued by ASIS and ASD, which request or require a DCP to provide assistance that gives effect to an authorisation obtained by the relevant agency.)*
- ✗ Ambiguity remains about whether TARs and TANs can cover the provision of repetitive assistance (doing the specified act multiple times) or whether a TAR or TAN is spent after a single instance of providing the specified assistance, and a new one would be needed.

- ***defences for IGIS officials; and***

Fully addressed in Government amendments

- ✓ Removal of evidential burden from IGIS officials in s 317ZF(5).
- ✓ Insertion of exception in s 63AC of the *TIA Act*.

- ***clear information sharing provisions.***

Fully addressed for IGIS in Government amendments

- ✓ Amendments to s 63AC of the *TIA Act*.

PJCIS recommendation 17

The Committee recommends that the Government:

- ***Amend clause 317ZG of Schedule 1 to explicitly prohibit an interception agency from asking a designated communications provider to voluntarily implement or build a systemic weakness or vulnerability under a technical assistance request;***

Fully implemented in Government amendments

✓ Section 317ZG applies to TARs (as well as TANs and TCNs).

- ***Amend clause 317ZH of Schedule 1 so that the 'general limits' on technical assistance notices and technical capability notices apply equally to technical assistance requests.***

Partially implemented in Government amendments (subject to one apparent technical issue)

✓ Subsection 317ZH(1) applies explicitly to TARs, in addition to TANs and TCNs.

× However, amendments to ss 317ZH(1) and (4) may be needed to account for the fact that ASD and ASIS can issue TARs. This appears to be a technical oversight. (Specifically, the *Intelligence Services Act* may need to be added to the list of Acts in paragraphs 317ZH(1)(a) and the exception in subsection 317ZH(4) may need to refer to giving help to ASD or ASIS under a TAR.)

Attachment C

Handling of IGIS concerns about Schedules 2 and 5 (ASIO Act)

The Committee's recommendations on the Bill, while inclusive, were directed to Schedule 1 (other than two discrete matters in recommendation 5 concerning disclosure provisions relevant to IGIS, which applied to provisions in Schedules 1, 2 and 5).

However, the Government moved some further amendments to address aspects of IGIS's concerns about Schedule 2 (ASIO warrants) and Schedule 5 (ASIO civil immunities for voluntary assistance, and compulsory assistance orders).

This attachment identifies those of IGIS's concerns that have been implemented in statute, and those that remain outstanding, as they have not been included in the Act or in the *ASIO Guidelines* at the time of writing. IGIS has not received advice from ASIO or the Department of Home Affairs about whether there is an intention to amend the Guidelines to include some or all of these matters.

IGIS concerns addressed in the Government amendments

Schedule 2 (extended powers under ASIO computer access warrants)

- ✓ **Reporting on post-warrant concealment:** Specific reporting requirements to the Attorney-General on post-warrant concealment activities (activities to conceal acts done under a warrant, and further concealment of those activities).
- ✓ **Equivalent safeguards for concealment activities as for computer access activities:** Concealment activities are subject to equivalent limitations on causing material interference, loss or damage to lawful computer users as those currently applying to computer access.

Schedule 5 (s 21A(1) civil immunities for voluntary assistance and s 34AAA assistance orders)

Civil immunities for voluntary assistance: s 21A(1)

- ✓ **Notification requirement:** Notification of IGIS of issuing s 21A(1) requests (civil immunities for voluntary assistance).
- ✓ **Form requirement:** Requirement that s 21A(1) requests must be made in writing, unless there are circumstances of urgency, or a risk of prejudice to security or operational security.

Compulsory assistance orders: s 34AAA

- ✓ **Previous requests:** ASIO's requests to the Attorney-General for the issuing of s 34AAA assistance orders must specify any previous requests made in relation to the person (and outcomes of those requests).
- ✓ **Integration with warrant reporting:** ASIO's warrant reports must include information about related s 34AAA assistance orders in relation to data obtained under the warrant.
- ✓ **Annual reporting:** ASIO's classified annual reports must include statistical information on 34AAA orders and s 21A(1) assistance requests.
- ✓ **Duty to advise Attorney-General if grounds for order have ceased to exist:** The Director-General of Security must inform the Attorney-General if satisfied the grounds for issuing an s 34AAA order have ceased to exist. The Attorney-General must revoke the order if satisfied that the issuing grounds have ceased to exist.

IGIS concerns not addressed

Schedule 2 (extended powers under ASIO computer access warrants)

- **Limitation on warrant reporting—temporary removals:** Warrant reports under s 34 are not required to specifically identify whether a computer or other thing has been removed from premises in all instances. (Reporting will only be required under existing provisions of section 34, if ASIO has assessed the removal to have caused material interference with the lawful use of the computer. This will make it difficult to oversee the exercise by ASIO of the new temporary removal powers, and its decision-making about whether a temporary removal caused a material interference.)

Schedule 5 (s 21A(1) civil immunities for voluntary assistance and s 34AAA assistance orders)

Civil immunities for voluntary assistance: s 21A(1)

- **Proportionality:** No statutory issuing criteria requiring the Director-General of Security (or delegate) to be satisfied that the conferral of civil immunity is reasonable and proportionate.
- **Exclusion of certain conduct causing serious loss or harm:** No statutory exclusion of conduct causing significant financial loss, or serious physical or mental harm to another person.
- **Maximum period of effect:** No statutory maximum period of effect for s 21A(1) requests. (Noting there is doubt that a period of effect could, in some way, be implied from separate legal instruments such as warrants or contracts.)
- **Overlap with Technical Assistance Notices:** No exclusion of conduct that could be the subject of a TAR under Part 15 of the *Telecommunications Act 1997* (inserted by Schedule 1 to the Act), noting that TARs are subject to stronger limitations than s 21A(1) voluntary assistance requests.
- **Conduct for which ASIO would require a warrant / authorisation to undertake directly:** No exclusion of conduct for which ASIO would require a warrant or an authorisation to carry out itself (except in those cases in which ASIO had already obtained a warrant or authorisation, which was in force at the time, and the person who is subject to an s 21A(1) request was also authorised to exercise authority under that warrant or authorisation).
- **Notification of IGIS if conduct causes serious harm or damage:** There is no requirement for ASIO to notify IGIS if it becomes aware that a person engages in conduct in purported reliance on a civil immunity under s 21A(1), and the act or thing exceeds applicable limits on the immunity (including the additional limits IGIS has suggested). For example, if the conduct causes another person to suffer significant financial loss, property loss or damage, or physical or mental harm.
- **Powers of variation and revocation:** No specific statutory power of variation or revocation. (Noting that s 33(3) of the *Acts Interpretation Act 1901* would not be available, at least for oral requests; and there is legal uncertainty about the existence and scope of implied powers of variation or revocation.)
- **Repetitive provision of assistance:** Ambiguity as to whether requests can cover the repetitive provision of assistance, or are spent after the first performance of the specified conduct. (Proportionality requirements and a maximum period of effect will be even more important if requests are intended to cover, and therefore confer immunity for, the repetitive provision of assistance.)

Compulsory assistance orders: s 34AAA

- **Persons who may be subject to an order:** Assistance orders can be issued in relation to any person who is reasonably suspected of being involved in an activity that is prejudicial to security. This is not required to be an activity that is prejudicial to the security matter in respect of which the underlying warrant is issued, and could be any unrelated security matter. (IGIS is aware that the Department of Home Affairs gave evidence to the PJCIS that this broader application was not the intent.)
- **Not all orders are required to specify essential matters:** Assistance orders are only required to specify essential matters (including the compliance period, place of attendance and conditions on the order) if a computer has been removed from premises under a warrant. This means that, where a computer is accessed wholly remotely (for example, under ASIO's computer access warrants) there is no requirement for orders to include these conditions. This reduces transparency in the terms of an order that the Attorney-General is being asked to approve, and in the information given to persons who are subject to orders, because these matters are not required to be recorded explicitly on the face of the order itself.
- **Arbitrary deprivation of liberty:** No statutory safeguards against the risk of orders requiring a person to attend a place to provide assistance resulting in an arbitrary deprivation of liberty.
- **Retention / deletion of information obtained under an assistance order:** No requirement for the Director-General of Security to delete records or copies of information obtained under an assistance order, if the Director-General is satisfied that it is no longer required for the purpose of ASIO's functions and powers under the *ASIO Act*. (Such an obligation exists in section 31 in relation to information obtained under the underlying special powers warrant. Not all information obtained under an s 34AAA warrant will be covered by s 31 itself. For example, login credentials to a computer, potentially including biometric identification information.)
- **Cessation of action taken under an order where issuing grounds no longer exist:** No obligation on the Director-General of Security to take all necessary steps to cease executing an s 34AAA order if satisfied that the issuing grounds have ceased to exist, noting that such an obligation applies to ASIO's special powers warrants under s 30(1)(b).
- **Notification and service of orders:** No statutory requirements for the notification and service of assistance orders on persons.
- **Interaction with ASIO's questioning and detention warrants:** No statutory guidance on the execution of an assistance order in relation to a person who is the subject of an ASIO questioning warrant or a questioning and detention warrant (including a role for IGIS, where in attendance for the compulsory questioning of a person).