IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Dr Christopher Jessup QC
Inspector-General of Intelligence and Security

26 February 2021

TABLE OF CONTENTS

1. INTRODUCTION

1. The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill).

2. The Inspector-General is an independent statutory officer with oversight in relation to the activities of the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD), the Australian Geospatial-Intelligence Organisation (AGO), the Defence Intelligence Organisation (DIO) and the Office of National Intelligence (ONI). The overarching purpose of IGIS's activities is to provide assurance that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.

3. As at February 2021, IGIS had 35 staff employed under the *Public Service Act 1999*, in addition to the Inspector-General. The Hon Dr Christopher Jessup QC commenced as the Inspector-General on 8 February 2021 (having been acting Inspector-General since 18 January 2021).

4. Consistent with established practices, IGIS does not make any comment on the policy underlying the Bill, except to the extent that IGIS oversight is affected. IGIS notes that aspects of the Bill overlap with the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 (Integrity Measures Bill) and therefore, this submission should ideally be considered in the context of IGIS's submission to the Committee on the Integrity Measures Bill.

5. IGIS was consulted by the Department of Home Affairs during the development of this Bill. IGIS was also consulted by the Attorney-General's Department on the development of the Integrity Measures Bill. IGIS worked closely with the Attorney-General's Department and the Department of Home Affairs to ensure that the proposed amendments in the two Bills are consistent with one another.

2. BACKGROUND

6. The Bill makes amendments to the *Surveillance Devices Act 2004* (SD Act) and other legislation to give the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP) new powers to respond to online criminal activity. This submission will primarily focus on Schedule 2 of the Bill, which introduces a new 'network activity warrant' framework. The Bill proposes that IGIS will have responsibility for the oversight of this warrant framework.

7. This submission will also briefly discuss Schedules 1 and 3 of the Bill which provide for other new powers ('data disruption' and 'account takeover' warrant frameworks, respectively). The Bill proposes that the use of these powers by ACIC and AFP be overseen by the Commonwealth Ombudsman, but their exercise may also incidentally attract IGIS's oversight where an intelligence agency within IGIS's jurisdiction renders technical assistance to ACIC and AFP.

INTERACTION WITH INTEGRITY MEASURES BILL

8. Among other things, the Integrity Measures Bill will amend IGIS's powers, functions and duties in the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) and related legislation to expand IGIS's oversight jurisdiction to the intelligence functions of ACIC and AUSTRAC. The Integrity Measures Bill also makes amendments aimed at ensuring that the IGIS Act is properly adapted to contemporary circumstances.

9. IGIS notes that Schedule 2, Part 3 of the Integrity Measures Bill contains amendments contingent on the passage and commencement of this Bill. These contingent amendments are divided, subject to when, and whether, this Bill commences. As such, the amendments in this Bill that expand IGIS's oversight jurisdiction and amend the provisions of the IGIS Act should ideally be considered in conjunction with the equivalent provisions in these sections of the Integrity Measures Bill.

STRUCTURE OF THE BILL

10. Briefly, the Bill comprises:

Schedule 1 (Data disruption warrants) – a new Division 5 to Part 2 of the SD Act that will:

- enable law enforcement officers of ACIC and AFP to apply for data disruption warrants that will authorise the disruption of data held in a computer that is likely to assist substantially in frustrating the commission of relevant offences;
- allow an eligible Judge or nominated AAT member to issue data disruption warrants;
- provide for Commonwealth Ombudsman oversight of the data disruption framework, with the ability to share information with IGIS where relevant to the performance of IGIS's powers, functions or duties.

Schedule 2 (Network activity warrants)

- Part 1 – a new Division 6 to Part 2 of the SD Act that will:
    - enable the chief officers of ACIC and AFP to apply for warrants that authorise access to data held in computers which will substantially assist in the collection of intelligence relating to a criminal network of individuals;
    - allow an eligible Judge or nominated AAT member to issue network activity warrants;
- Part 2 – Consequential amendments to other Acts that, among other things, will:
    - expand IGIS's jurisdiction to include oversight of ACIC's and AFP's use of network activity warrants;

- enhance IGIS's ability to manage its concurrent jurisdiction with other integrity bodies and to provide oversight of ACIC's and AFP's use of network activity warrants.

Schedule 3 (Account takeover warrants) – a new Part IAAC of the *Crimes Act 1914* that will:

- enable law enforcement officers of ACIC and AFP to apply for account takeover warrants that authorise them to take control of one or more online accounts for investigatory purposes;
- allow a magistrate to issue an account takeover warrant;
- provide for Commonwealth Ombudsman oversight of the account takeover framework, with the ability to share information with IGIS where relevant to the performance of IGIS's powers, functions or duties.

3. SCHEDULES 1 & 3 – DATA DISRUPTION AND ACCOUNT TAKEOVER WARRANT FRAMEWORKS

11. Schedule 1 will introduce a new data disruption warrant framework into Division 5 to Part 2 of the SD Act. This framework will enable ACIC and AFP to apply for data disruption warrants to authorise access to and the disruption of certain data held in a computer, including by modifying, adding, copying or deleting the data. The purpose of such a warrant is to frustrate the commission of a 'relevant offence' that involves or is likely to involve data held in a target computer.[1] These powers will be used covertly by ACIC and AFP and will include the ability to conceal the execution of a warrant.[2] A data disruption warrant may only be sought for the purpose of disrupting the commission of an offence, not for evidence gathering purposes. However, any information collected in the course of executing a warrant may be submitted as evidence in criminal proceedings.[3]

12. Schedule 3 will introduce a new account takeover framework into Part IAAC of the *Crimes Act 1914*. This framework will enable law enforcement officers of ACIC and AFP to apply for account takeover warrants that authorise them to take control of one or more online accounts for investigatory purposes. These powers will be used covertly and information collected in the course of executing a warrant will be available to be used as evidence in criminal proceedings.[4]

13. The Bill proposes that the Commonwealth Ombudsman have oversight of ACIC's and AFP's use of these powers.[5] Relevantly to IGIS, the Ombudsman may communicate information obtained in the course of its oversight of these powers to IGIS officials for the purposes of IGIS officials exercising powers, or performing functions or duties as such.[6]

14. IGIS notes that, in practice, there may not always be a clear delineation between IGIS's oversight of the network activity warrant framework detailed in Schedule 2, and the Ombudsman's oversight of the data disruption warrant and account takeover warrant frameworks in Schedules 1 and 3. IGIS notes, however, that the information sharing provisions, and the other provisions in Schedule 2 of the Bill, aimed at addressing concurrent jurisdiction between IGIS and other integrity bodies, is intended to ensure that the risk of duplication of oversight between IGIS and the Ombudsman is appropriately managed and minimised.

15. Although only ACIC and AFP are permitted to seek data disruption warrants and account takeover warrants, ASD may have a role in providing technical assistance to ACIC and AFP under these frameworks.[7] IGIS understands that ASD's assistance to ACIC and AFP is intended to fall within its existing functions and will not involve expansion of its legislated powers. IGIS further understands that ASD assistance would not extend to the execution of the warrants on behalf of ACIC or AFP. Consistent with its existing jurisdiction, IGIS will oversee conduct undertaken by ASD in rendering technical assistance to ACIC and AFP in the execution of a warrant under the Bill.

---

[1] 'Relevant offence' retains its existing meaning in subsection 6(1) of the SD Act.
[2] Item 13 of Schedule 1, proposed subsection 27KE(9); Explanatory Memorandum, paragraph 8.
[3] Item 51 of Schedule 1, proposed section 65C of the SD Act; Explanatory Memorandum, paragraph 8.
[4] See existing Division 3 of Part 6 of the SD Act which provides for Ombudsman oversight of law enforcement agencies' use of SD Act powers and will, if the Bill is passed, extend to ACIC's and AFP's use of data disruption warrants; Item 4 of Schedule 3, proposed Division 7 of Part IAAC of the *Crimes Act 1914*.
[5] Items 35 and 56 of Schedule 1, proposed subsection 45(6A), and proposed section 63AD of the SD Act. These specific amendments will complement the oversight related provisions referred to in footnote 4.
[6] Item 35 of Schedule 1, proposed subsection 45(6A) of the SD Act; Item 4 of Schedule 3, proposed subsection 3ZZVH(5) of the *Crimes Act 1914*.
[7] Department of Home Affairs, *Home Affairs Portfolio submission to the review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, 12 February 2021, paragraph 37.

4. SCHEDULE 2 – NETWORK ACTIVITY WARRANT FRAMEWORK

OVERVIEW OF THE WARRANT FRAMEWORK

16. Schedule 2 of the Bill will introduce a network activity warrant framework into Division 6 of Part 2 of the SD Act. ACIC and AFP may apply for a network activity warrant to access data held in computers that will substantially assist in the collection of intelligence that relates to a criminal network of individuals. Under the Bill, applications for network activity warrants must be made to an eligible Judge or nominated member of the Administrative Appeals Tribunal (AAT). Applications may be sought by the chief officer of ACIC or AFP, or a delegated Senior Executive Service (SES) staff member of the agency, if they suspect, on reasonable grounds, that:
    - a group of individuals is a criminal network of individuals; and
    - access to data held in a computer being used, or likely to be used from time to time by individuals in the group, will substantially assist in the collection of intelligence that relates to the group or its members, and the data is relevant to the prevention, detection, or frustration of relevant offences.[8]
17. The Bill also allows for remote and unsworn applications.[9]
18. The Judge or AAT member may issue a network activity warrant if satisfied that there are reasonable grounds for the suspicion 'founding the application'.[10] In determining whether a network activity warrant should be issued, the Judge or AAT member must have regard to, among other things, the nature and gravity of the conduct and the likely intelligence value of any information obtained.[11] As it does with other intelligence warrants it oversights, IGIS would expect warrant applications to address each of the factors to which a Judge or AAT member would be required have regard to in determining an application.
19. The decisions of a Judge or AAT member in dealing with a warrant application would not fall within the ambit of IGIS's oversight jurisdiction (in the same way, Ministerial decisions are not within the current jurisdiction of IGIS).[12] The warrant application, however, along with information relied upon in support of the application, would be reviewable by IGIS. In reviewing an application, IGIS would give close consideration to whether the information relied upon is comprehensive and accurate.
20. A network activity warrant may be issued for a period of up to 90 days.[13] Proposed section 27KQ would allow for a warrant's duration to be extended an unlimited number of times in increments of up to 90 days (discussed below).[14] A network activity warrant may authorise the ACIC or AFP to do any of the specified things listed in proposed section 27KP in relation to a relevant target computer. These include, but are not limited to, adding to, copying, deleting or altering data to obtain access to data, intercepting communications passing over a telecommunications system and using a surveillance device for the purposes of doing any thing specified in the warrant.[15]
21. As with the data disruption warrant and account takeover warrant frameworks, ASD will have a role in in providing technical assistance to ACIC and AFP under the network activity warrant

[8] Item 9 of Schedule 2, proposed section 27KK.
[9] Item 9 of Schedule 2, proposed section 27KL and subsection 27KK(5), respectively.
[10] Item 9 of Schedule 2, proposed section 27KM.
[11] Item 9 of Schedule 2, proposed subsection 27KM(2).
[12] IGIS Act, paragraph 9AA(b).
[13] Item 9 of Schedule 2, proposed subsection 27KN(2).
[14] Item 9 of Schedule 2.
[15] Item 9 of Schedule 2.

framework.[16] As discussed in paragraph 15 above, IGIS understands that this will not represent an expansion of ASD's functions or powers. IGIS has jurisdiction to oversee conduct undertaken by ASD (or any other intelligence agency in its jurisdiction) in rendering technical assistance to ACIC and AFP in the execution of a warrant under the Bill.

IGIS OVERSIGHT

JURISDICTION AND REPORTING

22. The Bill provides for IGIS oversight of the network activity warrant framework. IGIS's oversight is supported by requirements for the chief officer to notify the Inspector-General when a network activity warrant is issued,[17] extended or varied,[18] revoked,[19] or when certain concealment activities are undertaken.[20]

23. The SD Act currently requires the chief officers of ACIC and AFP to make a report to the Minister as soon as practicable after a warrant issued under the Act ceases to be in force.[21] Section 50 of the Act also contains requirements for certain information to be included in ACIC's and AFP's annual reports, including the number of applications made for warrants under the Act, the number of warrants issued or refused and the number of extensions applied for and granted and refused. These existing reporting requirements would extend to network activity warrants.

24. In addition, the Bill proposes specific reporting requirements in relation to network activity warrants. Proposed subsection 49(2E) provides that reports to Ministers must contain specific information about a warrant including, but not limited to, the name (if known) of any person whose data was accessed, the extent to which the execution of the warrant assisted the agency in carrying out its functions and details of the compliance with the conditions (if any) stipulated in the warrant.

25. The Bill also contains record keeping requirements, including provisions governing the destruction of records obtained by accessing data under a network activity warrant. Proposed section 46AA specifies that the chief officers of ACIC and AFP must ensure that every record or report relating to network activity warrant information is kept in a secure place, and destroyed within specified timeframes.[22] Consistent with its current practice in reviewing other intelligence warrants, IGIS would inspect these records on a regular basis.

SCOPE AND DEFINITIONS

26. In IGIS's experience, effective oversight is more readily achieved where the scope and content of intelligence or law enforcement powers are articulated clearly and fully on the face of the legislation and where consistency is sought, where possible, across like regimes. This is especially so in respect of coercive or covert powers.

27. The scope of the network activity warrant framework is defined by reference to a number of cascading definitions in the Bill. Proposed paragraph 27KK(1)(a) specifies that one of the conditions for applying for a network activity warrant is that a group of individuals is a 'criminal network of individuals'. A 'criminal network of individuals' is defined in proposed section 7A as:

> 'an electronically linked group of individuals, where one or more individuals in the group have engaged, are engaging or are likely to engage, in conduct that constitutes a relevant offence;

[16] Explanatory Memorandum, paragraphs 574 to 576.
[17] Item 9 of Schedule 2, proposed subsection 27KM(3).
[18] Item 9 of Schedule 2, proposed subsection 27KQ(7).
[19] Item 9 of Schedule 2, proposed subsection 27KR(7).
[20] Item 23 of Schedule 2, proposed section 49D.
[21] SD Act, section 49.
[22] Item 20 of Schedule 2, proposed section 46AA.

or have facilitated, are facilitating, or are likely to facilitate the engagement by another person in conduct that constitutes a relevant offence'.[23]

28. 'Relevant offence' retains its existing definition in section 6 of the Act. This definition includes, among other things, Commonwealth offences that are punishable by a maximum term of imprisonment of 3 years or more, or for life.

29. An 'electronically linked group of individuals' is further defined as:

> 'a group of 2 or more individuals, where each individual in the group does, or is likely to do, either or both of the following things:
> - use the same electronic services as at least one other individual in the group;
> - communicate with at least one other individual in the group by electronic communication.'[24]

30. IGIS notes that the definition of an 'electronically linked group of individuals' commences with 'a group of 2 or more individuals' and the word 'group' is not itself defined. The Explanatory Memorandum suggests that passive engagement with the same electronic service would bring an individual within the definition of an electronically linked group of individuals. [25]

31. The Bill does not require the warrant to specify the target computer or the details, if known, of any relevant individuals who may be affected by the warrant.[26] For comparison, computer access warrants issued under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and SD Act must include the specific target computer, premises or person, if known.[27]

32. The details of the particular offences being investigated do not need to be specified in a warrant: only 'the *kinds* of relevant offences in respect of which the warrant is issued' need to be specified.[28] While the Explanatory Memorandum notes that the warrants are intended to 'target activity of the most serious nature including terrorism, child exploitation, drug trafficking and firearms trafficking'[29], the Bill does not require the 'kinds' of relevant offences being targeted to be specified in the warrant in detail.

33. These cascading definitions are complex and potentially unclear in scope. This could create challenges for IGIS oversight, including in determining the legality and propriety of particular action purportedly taken pursuant to a warrant.

CONSIDERATION OF PRIVACY

34. Proposed section 27KM outlines the factors that a Judge or AAT member must take into account in determining an application for a network activity warrant. These include:

> (a) the nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant; and

[23] Item 8 of Schedule 2, proposed section 7A.
[24] Item 3 of Schedule 2, amendments to subsection 6(1).
[25] Explanatory Memorandum, paragraph 304.
[26] While proposed paragraph 27KN(1)(b) states that a warrant must specify the criminal network of individuals to which the warrant relates, and subsections 27KP(1) and (2) state that a warrant must authorise the doing of specified things in relation to a target computer, subsection 27KK(2) expressly states that it is immaterial whether the identities of the individuals in the group can be ascertained or if the target computer in question can be identified.
[27] Paragraphs 25A(3A)(c)—(e) of the ASIO Act and subparagraphs 27D(1)(b)(vii)—(ix) of the SD Act.
[28] Proposed subparagraph 27KN(1)(b)(ii) Item 9 of Schedule 2.
[29] Explanatory Memorandum, paragraph 24.

(b) the extent to which access to data under the warrant will assist in the collection of intelligence that:

(i) relates to the group referred to in paragraph 27KK(1)(a) or to any of the individuals in the group; and

(ii) is relevant to the prevention, detection or frustration of one or more kinds of relevant offences; and

(c) the likely intelligence value of any information sought to be obtained; and

(d) whether the things authorised by the warrant are proportionate to the likely intelligence value of any information sought to be obtained; and

(e) the existence of any alternative, or less intrusive, means of obtaining the information sought to be obtained; and

(f) the extent to which the execution of the warrant is likely to result in access to data of persons who are lawfully using a computer; and

(g) any previous warrant sought or issued under this Division in relation to the group referred to in paragraph 27KK(1)(a). [30]

35. While proposed paragraph 27KM(2)(f) requires a decision-maker to consider the 'extent to which the execution of the warrant is likely to result in access to data of persons who are lawfully using a computer', it is unclear whether this is intended to be equivalent to a requirement to consider any privacy implications.[31] IGIS notes that its jurisdiction includes assisting Ministers in ensuring that the conduct of agencies is consistent with human rights (which includes the right to privacy).[32] Clarity on the extent to which the right to privacy is intended to guide the use of network activity warrants will assist IGIS in the exercise of its legality and human rights oversight functions.

ACTIVITIES AUTHORISED BY THE WARRANT: OVERSIGHT OF THE RETENTION OF COMPUTER OR 'THING'

36. Proposed section 27KP specifies the things that a network activity warrant may authorise. These include, but are not limited to, entering premises, using a target computer to access data and using surveillance devices for the purposes of doing any thing specified in the warrant. Network activity warrants also authorise the removal of a computer or other thing from premises for the purposes of doing any thing specified in the warrant. Proposed subsection 27KP(3) states that if a computer or thing is removed from premises in accordance with a network activity warrant, the computer or thing must be returned to the premises within a reasonable period.[33]

37. IGIS recognises that what might constitute a reasonable period would depend on the context and circumstances of a particular issue. As part of its oversight of these warrants, IGIS would review the period in which an item was retained and the time in which it was returned to ensure that this action is consistent with the legislation, and that the action taken was consistent with propriety. IGIS would expect that the reasons for any significant delay in returning an item to be well documented.

[30] Item 9 of Schedule 2, proposed subsection 27KM(2).
[31] Item 9 of Schedule 2, proposed paragraph 27KM(2)(f).
[32] IGIS Act, paragraph 4(b). 'Human rights' is defined in section 3 of the IGIS Act with reference to the definition in the *Australian Human Rights Commission Act 1986.* The relevant definition in section 3 of the *Australian Human Rights Commission Act 1986* expressly includes, among other things, the International Covenant on Civil and Political Rights which includes the right to privacy (article 17).
[33] Item 9 of Schedule 2.

REPORTING TIMEFRAMES

38. IGIS notes that the Bill does not currently set a maximum timeframe within which a report must be provided to the Minister, other than 'as soon as practicable'. As noted above, network activity warrants have effect for a maximum period of 90 days. However, under proposed section 27KQ, a network activity warrant may be extended by further increments of up to 90 days on an unlimited number of occasions, subject to review by the issuing authority on each occasion.[34] It is possible that certain warrants will be in force for significant periods of time, thereby delaying the time before a report to the Minister is produced.

39. This is in contrast to other warrant frameworks in which a maximum timeframe for reporting has been incorporated.[35] In addition to assisting IGIS to conduct its inspections and review the accuracy of records, clear statutory requirements to report on action taken under covert and coercive powers enhances accountability and transparency.

CONSEQUENTIAL AMENDMENTS TO EXPAND IGIS JURISDICTION

40. To facilitate IGIS oversight of the network activity warrant framework, the Bill makes consequential amendments to the IGIS Act and related legislation to expand IGIS's jurisdiction to cover matters related to the 'intelligence functions' of ACIC and AFP. These agencies' intelligence functions are defined narrowly in item 55 of Schedule 2 of the Bill (amendments to subsection 3(1) of the IGIS Act):

> ***intelligence function***:
>
> (a) for ACIC—means:
>
> (i) the collection, correlation, analysis, production and dissemination of intelligence obtained by ACIC from the execution of a network activity warrant; or
>
> (ii) the performance of a function, or the exercise of a power, conferred on a law enforcement officer of ACIC by the network activity warrant provisions of the *Surveillance Devices Act 2004*; or
>
> (b) for the Australian Federal Police—means:
>
> (i) the collection, correlation, analysis, production and dissemination of intelligence obtained by the Australian Federal Police from the execution of a network activity warrant; or
>
> (ii) the performance of a function, or the exercise of a power, conferred on a law enforcement officer of the Australian Federal Police by the network activity warrant provisions of the *Surveillance Devices Act 2004*.

41. This definition is only intended to cover ACIC's and AFP's activities in relation to network activity warrants, not any of their other functions or powers. These amendments expand IGIS's existing inspection and inquiry powers, functions and duties in the IGIS Act to apply to ACIC and AFP and will work in conjunction with the main amendments to the SD Act to ensure that IGIS's oversight jurisdiction over the six intelligence agencies within IGIS's existing remit will be replicated with respect to ACIC's and AFP's use of network activity warrants.

42. As foreshadowed above, these sections and definitions will be further amended by the passage of the Integrity Measures Bill, which expands IGIS's jurisdiction to the broader intelligence functions

[34] Item 9 of Schedule 2.

[35] See section 17 of the TIA Act and clause 129 of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (which is currently before the Parliament). In both of these examples, a report is required to be provided to the Attorney-General within 3 months.

of ACIC and AUSTRAC (see, for example, Items 60, 121 and 162 of Schedule 2 of the Integrity Measures Bill). The Integrity Measures Bill contains contingent amendments aimed at ensuring that, in the event that both Bills pass, the final construct of each provision is the same regardless of the order of their passage.

OTHER CONSEQUENTIAL AMENDMENTS

43. In addition to the amendments that directly expand IGIS's oversight jurisdiction over ACIC's and AFP's use of network activity warrants, the Bill also includes a range of other consequential amendments. These amendments, primarily contained in Schedule 2, Part 2 of the Bill, mirror some of the amendments in the Integrity Measures Bill.

44. Broadly, these amendments seek to:

- **insert exceptions to secrecy offences in legislation governing ACIC and AFP specifically to cover disclosures to IGIS officials** for the purpose of IGIS officials performing functions or duties or exercising powers as IGIS officials. For example, item 37 of Schedule 2 creates a new exception to section 40ZA of the *Australian Federal Police Act 1979* to ensure that it is not an offence for a person to divulge or communicate information that was given to, or obtained by, the person in the course of, or for the purposes of, the investigation or inquiry if the communication was to an IGIS official 'for the purpose of the IGIS official exercising a power, or performing a function or duty, as an IGIS official'.

  While there are existing immunities in the IGIS Act for people who give information to IGIS officials (either voluntarily or under compulsion),[36] these exceptions will make it explicit on the face of the legislation governing ACIC and AFP that it is lawful and proper to give information to IGIS. This will also avoid potential legal complexities about the interaction of offence provisions with the immunities in the IGIS Act. The approach to these exceptions replicates the approach taken in Part 5.6 of the *Criminal Code* and other legislation governing agencies within IGIS's existing jurisdiction.[37]

- **clarify the ability of IGIS to share certain information or documents with other integrity bodies** where it would be relevant to the receiving bodies' functions. Proposed section 32AC of the IGIS Act (inserted by item 71 of Schedule 2) should be read with reference to the secrecy offences in section 34 of the IGIS Act, which prohibit IGIS officials from disclosing any information or documents acquired under the IGIS Act (regardless of its classification) 'except in the performance of his or her functions or duties or in the exercise of his or her powers' under the IGIS Act or the *Public Interest Disclosure Act 2013* (PID Act). Although information sharing with other integrity bodies is arguably already implicitly permitted by the IGIS Act, proposed section 32AC provides clearer statutory authority for the Inspector-General to share information or documents with other integrity bodies in accordance with the requirements of the section. This makes clear that such sharing is not subject to the prohibition in section 34. Amendments located in item 68 of Schedule 2 (proposed subsection 11(4A) of the IGIS Act) will also clarify that IGIS may decide not to inquire into a complaint if it could have been made to another integrity body.

- **clarify the ability of integrity bodies to share information with, and transfer complaints concerning ACIC's or AFP's use of network activity warrants to, IGIS.** The Bill will achieve this through consequential amendments to a series of other Acts. For example, item 47 of Schedule 2 amends the *Australian Human Rights Commission Act 1986* (AHRC Act) to provide that the Commission may decide not to inquire, or continue to inquire, into an act or practice

[36] See existing subsections 18(6) and (9) and section 34B of the IGIS Act.

[37] For example, see paragraph 317ZF(3)(f) of the *Telecommunications Act 1997* and section 63AC of the *Telecommunications (Interception and Access) Act 1979*.

of ACIC or AFP following a complaint, if the Commission is of the opinion that the subject matter of the complaint could be more effectively or conveniently dealt with by IGIS. The provisions require the Commission to consult with the Inspector-General and, if the Inspector-General agrees, to transfer the complaint and any related information or documents to the Inspector-General as soon as is reasonably practicable. Items 46 and 47 of Schedule 2 create exceptions to the non-disclosure offence in section 49 of the AHRC Act to ensure that such information and documents can be disclosed to IGIS officials without penalty.

- **clarify the ability of IGIS staff to enter premises for the purposes of conducting an inspection** of ACIC or AFP (extended to cover all agencies within IGIS's existing jurisdiction in the Integrity Measures Bill). These amendments are located in item 65 of Schedule 2 in this Bill (proposed subsection 9A(2) of the IGIS Act), and items 68 and 171 of Schedule 2 of the Integrity Measures Bill.
- **amendments to the PID Act to support IGIS investigation of public interest disclosures concerning ACIC's and AFP's use of network activity warrants.** For example, item 97 of Schedule 2 amends the PID Act to provide that an authorised officer of IGIS is an 'authorised internal recipient' for a public interest disclosure, where the discloser believes on reasonable grounds that the disclosure relates to action taken by ACIC or AFP in relation to its intelligence functions, and it would be appropriate for the disclosure to be investigated by IGIS.
- **remove the evidential burden for IGIS officials in relation to defences to various secrecy provisions**. Under section 13.3 of the *Criminal Code*, the default position is that a person seeking to raise a defence or an exception to an offence will bear an evidential burden in relation to that defence, requiring them to lead evidence that points to the reasonable possibility that a matter exists. IGIS officials are subject to strict secrecy offences under section 34 of the IGIS Act and are prevented from disclosing information acquired in the course of their duties to any person, including to a court. Currently, provisions that exempt IGIS officials from the evidential burden are scattered throughout various pieces of legislation. This amendment would centralise and clarify these exemptions in proposed section 34C of the IGIS Act, covering the field for all secrecy offences that would apply to IGIS officials.