Australian Government
Attorney-General's Department

August 2023

Submission to the Review of the Intelligence Services Legislation Amendment Bill 2023

Parliamentary Joint Committee on Intelligence and Security

Contents

1. Introduction

The Attorney-General's Department (the department) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee) Review of the Intelligence Services Legislation Amendment Bill 2023 (the Bill).

Australia's national intelligence and law enforcement agencies provide a vital role in keeping Australians safe and protecting Australia's national interest. To support them in performing their functions, the Parliament has entrusted these agencies with significant powers. This trust is dependent on effective and appropriate statutory oversight to ensure that agencies act legally, with propriety and consistently with human rights.

With national security threats becoming more complex and interconnected, agencies in the National Intelligence Community (NIC) are more closely collaborating and sharing intelligence information.

The Bill

The Bill enhances parliamentary and statutory oversight mechanisms to ensure oversight of the NIC is holistic and commensurate with the powers and responsibilities of those agencies. The measures in the Bill will support the Inspector-General of Intelligence and Security (IGIS) and the Committee to oversee Australia's intelligence agencies. Robust oversight continues to be needed to ensure public confidence in and social license for Australia's intelligence agencies. Strengthening the parliamentary committee system and enhancing parliamentary and statutory oversight of the NIC agencies will provide greater assurance that they are operating with legality, propriety and consistently with human rights.

The measures in the Bill address recommendations from the *2017 Independent Intelligence Review* by Mr Michael L'Estrange AO and Mr Stephen Merchant PSM, the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Comprehensive Review) by Mr Dennis Richardson AC, and various reports of the Committee (referred to below).

The Bill would:

Expand IGIS's jurisdiction

- to include four additional NIC agencies, specifically the Australian Criminal Intelligence Commission (ACIC), and the intelligence functions of the Australian Federal Police (AFP), the Australian Transaction Reports and Analysis Centre (AUSTRAC), and the Department of Home Affairs (Home Affairs)
- make consequential amendments to other Commonwealth legislation as a result of the expanded jurisdiction, including amendments to minimise overlap between the jurisdictions of the IGIS and other oversight bodies (such as the Commonwealth Ombudsman (Ombudsman)), without creating gaps in current oversight arrangements

Expand the Committee's jurisdiction

- to the ACIC and the intelligence functions of the AFP, AUSTRAC and Home Affairs
- to enable it to review, on its own motion, counter-terrorism and national security legislation

Strengthen relationships between oversight bodies and support the Committee's oversight role

- strengthen the relationship between the Committee and the IGIS, including by providing that the Committee may request the IGIS undertake inquiries into certain matters and, if the IGIS undertakes an inquiry, requiring the IGIS to provide a response or notify the Committee of the reasons why a response was not provided
- clarifying that the Committee may request the Independent National Security Legislation Monitor (INSLM) provide briefings
- support the Committee's oversight role by requiring it to be briefed annually by the IGIS and the Director-General of National Intelligence (DGNI)

The Bill would also:

- make technical amendments to the Committee-related provisions in the *Intelligence Services Act 2001* (IS Act) to clarify provisions, and enhance the efficiency of the Committee
- enhance the efficiency of the IGIS's complaints jurisdiction
- make a number of consequential technical amendments to Commonwealth legislation to update provisions and terminology relating to the IGIS's performance of functions
- clarify that the IGIS may communicate with relevant Ministers about the ongoing and completed work of the IGIS
- require matters relating to ACIC criminal intelligence assessments arising under the *Archives Act 1983* (Archives Act) to be heard in the Security Division of the Administrative Appeals Tribunal (AAT), and
- amend the *Criminal Code Act 1995* (Criminal Code), to provide defence officials and others engaged in relevant conduct with an exemption from civil and criminal liability for computer-related conduct engaged in inside or outside Australia, on a similar basis as the existing immunity for conduct relating to the activities of the Australian Secret Intelligence Service (ASIS), Australian Signals Directorate (ASD), Australian Geospatial-Intelligence Organisation (AGO) and Australian Security Intelligence Organisation (ASIO) under section 476.6 of the Criminal Code.

The Bill was developed in consultation with the Offices of the IGIS, Commonwealth Ombudsman and INSLM, and the NIC. The Departments of the Prime Minister and Cabinet; Defence; Foreign Affairs and Trade; and Infrastructure, Transport, Regional Development, Communications and the Arts were also consulted on the Bill.

2. Background

2.1 Current oversight arrangements of the NIC

Australia's intelligence oversight framework features specialised bodies with distinct and interrelated roles. These bodies are independent of each other and of the agencies within their jurisdiction.

2.1.1 Parliamentary oversight

Parliamentary Joint Committee on Intelligence and Security

The Committee plays a critical role in overseeing NIC agencies and scrutinising national security legislation. It provides oversight of the agencies within its jurisdiction by reviewing their administration and expenditure, reviewing national security bills introduced into Parliament and ensuring national security legislation remains necessary, proportionate and effective by conducting statutory reviews. The Committee may also be referred an inquiry by a responsible Minister on a matter relating to the activities of certain agencies.

The Committee has jurisdiction over Australia's six traditional intelligence agencies – ASIS, AGO, ASD, ASIO, the Defence Intelligence Organisation (DIO) and the Office of National Intelligence (ONI). It is expressly prohibited from reviewing these agencies' operations and activities. The Committee has a more limited jurisdiction over the AFP, including through its functions to monitor and review the performance by the AFP of its terrorism related functions. The Committee does not currently have oversight of the ACIC, AUSTRAC or Home Affairs.

Parliamentary Joint Committee on Law Enforcement

The Parliamentary Joint Committee on Law Enforcement (PJCLE) monitors and reviews the performance of the ACIC and the AFP. The PJCLE may report to Parliament upon any matter connected with the performance of those agencies' functions or on any matter appearing in, or arising out of the annual reports of that agency. The PJCLE also examines trends and changes in criminal activities, practices and methods and reports to Parliament on any change it thinks desirable to the functions, structure, powers and procedures of the ACIC or the AFP.

2.1.2 Commonwealth oversight bodies

Inspector-General of Intelligence and Security

The IGIS plays a critical role in the oversight framework by assisting Ministers in the oversight and review of the activities of agencies within its jurisdiction for legality, propriety, and consistency with human rights. In fulfilling these functions, the IGIS also assists Ministers in assuring the Parliament and the public that agencies within its jurisdiction are open to scrutiny.

The IGIS may undertake formal inquiries into the activities of the agencies within its jurisdiction in response to a complaint, at the request of a minister, or of their own motion. The IGIS also conducts regular inspections of intelligence agency activities. The IGIS has significant powers to support its inquiry functions, including powers to require the attendance of witnesses, take sworn evidence, copy and retain documents and to enter an intelligence agency's premises.

The IGIS currently has oversight over ASIO, ASIS, AGO, ASD, DIO and ONI. The IGIS also oversees the AFP's and the ACIC's use of network activity warrants under the *Surveillance Devices Act 2004* (Surveillance Devices Act) and disclosures of intelligence information under the *Public Interest Disclosure Act 2013* (PID Act).

Ombudsman

The Ombudsman is an independent statutory officer established by the *Ombudsman Act 1976* (Ombudsman Act). The Ombudsman has broad jurisdiction over Commonwealth agencies, including AFP, ACIC, AUSTRAC and Home Affairs, to consider actions that relate to matters of administration. This includes powers to investigate complaints, conduct own motion investigations on administrative practices and perform such other functions as are conferred by other Acts or Regulations. Relevantly, the *Telecommunications (Interception and Access) Act 1979* (TIA Act), the Surveillance Devices Act, the *Crimes Act 1914* (Crimes Act) and the *Telecommunications Act 1997* (Telecommunications Act) provide specific oversight functions on the Ombudsman with respect to the exercise of covert and intrusive powers by law enforcement. This includes the use of these regimes by state and territory law enforcement. The *Australian Federal Police Act 1979* (AFP Act) also relevantly provides an oversight function with respect to the handling of complaints about AFP conduct and practices.

The Ombudsman previously had jurisdiction over all NIC agencies with the exception of ASIO. By convention, however, the Ombudsman did not investigate action taken by ASIS, AGO, ASD, DIO and ONI. The *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Act 2023* (NSLAB No.2) formalised this position by amending the Ombudsman Act to expressly exclude ASIO, ASIS, AGO, ASD, DIO and ONI from the Ombudsman's jurisdiction.

Other oversight bodies

The NIC agencies are also subject to varied oversight by a range of other Commonwealth oversight bodies including the National Anti-Corruption Commission (NACC), Australian Human Rights Commission (AHRC), Office of the Australian Information Commissioner (OAIC) and Australian National Audit Office (ANAO). These oversight bodies have complementary roles in the oversight of intelligence agencies.

2.2 Recent independent and parliamentary reviews

2.2.1 2017 Independent Intelligence Review

The 2017 Independent Intelligence Review terms of reference directed that it focus on the traditional intelligence agencies – ASIS, ASIO, ASD, DIO, AGO and the then Office of National Assessments – but that it also examine the relationship and engagement between those agencies and the members of the broader NIC, including the AFP, ACIC, AUSTRAC and the then Department of Immigration and Border Protection (now Home Affairs).

In their report, the reviewers concluded that Australia's intelligence agencies were performing well but that the intelligence community faced challenges that were likely to increase over time and that 'Australia's future security

environment will demand greater levels of collaboration' across the NIC.[1] The review made 23 recommendations, including regarding structural arrangements, resourcing, legislation and oversight.

2.2.2 Comprehensive Review of the Legal Framework of the National Intelligence Community

The Comprehensive Review commenced in June 2018 and was the most in-depth review of Australia's national security laws since the Royal Commissions conducted by Justice Robert Hope in the 1970s and 1980s.

The terms of reference of the Comprehensive Review directed the review to consider legislation relating to the ten NIC agencies, distinctions between foreign and security intelligence and onshore and offshore collection, the adoption of a common legislative framework, improvements pursuant to coordination, cooperation, support, accountability and oversight, and any other specific proposals for reform. In his report, handed to the then government in December 2019, Mr Richardson made 203 recommendations about this legal framework.

2.2.3 Recent Committee Reports

The department notes the Committee has made several recommendations regarding the jurisdiction of the IGIS and its own jurisdiction in recent reports. The Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 (IM Bill) would have expanded the jurisdiction of the IGIS to the intelligence functions of AUSTRAC and the ACIC; and the jurisdiction of the Committee to cover the intelligence functions of AUSTRAC. It would not have expanded the jurisdictions of the IGIS or the Committee to the intelligence functions of the AFP or Home Affairs. The IM Bill was introduced into the House in December 2020. It was then referred to the Committee and the Committee presented its report in February 2022.

The department notes that in the Committee's *Advisory Report on the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020*, the Committee's recommendations included expanding its jurisdiction and that of the IGIS to the intelligence functions of the AFP. It also recommended expanding the jurisdiction of the Committee to the intelligence functions of the ACIC (noting the IM Bill would have expanded IGIS's jurisdiction to the ACIC). The IM Bill lapsed with the dissolution of Parliament on 11 April 2022.

These recommendations were consistent with earlier recommendations. In August 2021, the Committee presented its *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (SLAID Bill). The department notes the Committee recommended in this report that it and the IGIS should have oversight of the intelligence functions of the AFP and the ACIC, including but not limited to network activity warrants. In its *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* the Committee similarly recommended that the IGIS's jurisdiction be expanded to oversee the intelligence functions of the AFP and that its jurisdiction be expanded to include the intelligence functions of the ACIC.

[1] 2017 Independent Intelligence Review, page 6.

3. Overview of the Intelligence Services Legislation Amendment Bill 2023

3.1 Expanding IGIS's jurisdiction

3.1.1 Summary

The Bill would expand the IGIS's jurisdiction to the whole of the ACIC, and the intelligence functions of AUSTRAC, AFP and Home Affairs, and make consequential amendments to facilitate the IGIS's expanded jurisdiction, particularly in relation to information sharing with the Ombudsman to ensure shared oversight of agencies is effective and efficient.

The Bill would also make consequential amendments to a number of integrity frameworks to reflect the new oversight arrangements and minimise overlapping jurisdiction without creating gaps.

Given the increasing collaboration between NIC agencies, these amendments will ensure that the IGIS has holistic oversight of the intelligence activities of the NIC and that all NIC agencies are subject to the same high standard of specialised intelligence oversight.

3.1.2 Australian Criminal Intelligence Commission

Recommendation 21 of the 2017 Independent Intelligence Review recommended that the IGIS's jurisdiction be expanded to the intelligence functions of the ACIC. This was supported by the Comprehensive Review.[2] The Committee's Report on the IM Bill did not raise concerns with expanding the IGIS's jurisdiction to the intelligence functions of the ACIC.

The Bill would expand the IGIS's jurisdiction to the whole of the ACIC as the ACIC's functions of collecting, correlating, analysing and disseminating intelligence, including intelligence that may be relevant to national security, is inseparable from its other functions.

Interaction with the Ombudsman

The Bill would remove ACIC from the Ombudsman's jurisdiction that is provided for currently under the Ombudsman Act.[3] The Ombudsman would also no longer have oversight of the ACIC's use of covert and coercive powers under specific parts of the Crimes Act,[4] Telecommunications Act,[5] Surveillance Devices Act[6] and TIA Act.[7] Oversight of these powers would be undertaken by the IGIS. Given the broad scope of the IGIS's jurisdiction and the centrality of the ACIC's intelligence functions to the functions of the agency, this

[2] Comprehensive Review of the Legal Framework of the National Intelligence Community, para 40.102.
[3] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 2, item 195.
[4] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 2, items 146 to 150 (account takeover warrants) and 170 to 172 (controlled operations).
[5] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 2, items 257 to 287.
[6] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 2, items 247, 249, 250 and 251.
[7] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 2, items 301 and 302 (interception), 314 to 317 (stored communications and telecommunications data), and 328 to 330 (international production orders).

approach would reduce overlap in oversight without creating gaps. This approach is also consistent with the oversight arrangements for agencies wholly within the IGIS's jurisdiction.

The department notes that the lapsed IM Bill would have excluded matters relating to 'Indigenous violence and child sexual abuse' from the IGIS's jurisdiction on the basis that these matters would require specialist subject-matter expertise and cultural competencies that are best provided by the Ombudsman.[8] While the ACIC does provide work in the intelligence space in support of partners, the work is not targeted to a specific cohort. Further, there would be little value in retaining oversight by the Ombudsman in relation to 'Indigenous violence and child abuse' as it would be difficult for the Ombudsman to retain and provide meaningful oversight of one specific ACIC function that is rarely, if ever, used.

Interaction with the Public Interest Disclosure framework

Currently, disclosures under the PID Act relating to the intelligence functions of the ACIC may be made to a supervisor or authorised officer of the ACIC, or the IGIS. Other non-intelligence related disclosures relating to the ACIC may be disclosed within the ACIC, or to the Ombudsman.

The Bill would amend the definition of 'intelligence agency' for the purposes of the PID Act to include the ACIC.[9] As a result, all conduct will be required to be disclosed to a discloser's supervisor or authorised officer of the ACIC, or to the IGIS if the discloser believes on reasonable grounds that it would be appropriate for the disclosure to be investigated by the IGIS. This amendment reflects the removal of the ACIC from the Ombudsman's jurisdiction, and ensures that the ACIC is treated consistently with other agencies wholly within the IGIS's jurisdiction. Noting the passage of the *Public Interest Disclosure Amendment (Review) Act 2023*, the contingent amendments in the Bill would also require:[10]

- an authorised officer of the ACIC to provide written notice of certain matters regarding a disclosure to the IGIS as soon as reasonably practicable and in any case within one business day if the discloser states the disclosure is 'urgent' or 14 days for non-urgent disclosures, and
- the principal officer of the ACIC, where a disclosure is allocated to the ACIC for investigation, to provide regular written notice to the IGIS of the progress of the investigation and potential outcome timelines, including possible extensions.

Notwithstanding the ACIC's proposed classification as an 'intelligence agency' under the PID Act, the Bill would preserve the existing ability for public officials to make external disclosures of non-intelligence ACIC-related information under the PID Act.[11] Currently, external disclosures cannot be made in relation to the ACIC if the disclosure consists of, or includes, intelligence information as defined in section 41 of the PID Act, which includes 'sensitive law enforcement information'. These limitations will continue to provide appropriate safeguards for external disclosures relating to the ACIC.

[8] Explanatory Memorandum to the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020, para 605.
[9] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 2, item 220.
[10] Intelligence Services Legislation Amendment Bill 2023, schedule 1, parts 4 and 5.
[11] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 2, items 222 and 224 to 227.

The retention of this ability acknowledges that the same sensitivities do not arise for the ACIC in the same manner as other prescribed intelligence agencies, and it remains appropriate to subject disclosure of non-intelligence ACIC-related information to the additional oversight provided through the external disclosure mechanism.

Interaction with the Australian Human Rights Commission

The Bill would also exclude the ACIC from the jurisdiction of the AHRC under the AHRC Act.[12] This would minimise overlap without creating gaps in oversight, on the basis that the ACIC's intelligence functions are inseparable from their other functions. Additionally, the IGIS has the appropriate clearances, ability to access sensitive information and information protection arrangements in place required to deal with sensitive or classified ACIC information that may be required to receive complaints or provide a full picture of allegations relating to ACIC. The IGIS would also be best placed to identify matters relating to human rights through its program of inspections, complaints handling and inquiry functions. This approach is also consistent with the other agencies wholly within the IGIS's jurisdiction, noting that the IGIS has exclusive human rights jurisdiction in relation those agencies.

Interaction with the National Anti-Corruption Commission

The Bill would amend the definition of 'intelligence agency' under the NACC Act to include the ACIC.[13] Consistent with the approach for other agencies that are wholly within the IGIS's jurisdiction, this amendment will mean that the head of the ACIC, and other prescribed officials, will be required to refer suspected serious or systemic corruption issues that they become aware of to either the Commissioner or the IGIS. If the IGIS is satisfied that the issue is likely to involve corrupt conduct that is serious or systemic, the IGIS must refer the issue to the Commissioner. Providing the head, and prescribed officials, of the ACIC with a discretion to refer a matter to either the Commissioner or to the IGIS will enable the head of the ACIC to determine which is the most appropriate body to refer the corruption issue to on a case-by-case basis.

3.1.3 AFP

Recommendation 21 of the 2017 Independent Intelligence Review recommended that the IGIS's jurisdiction be expanded to the intelligence functions of the AFP. Recommendation 168 of the Comprehensive Review recommended against expanding IGIS's jurisdiction to the intelligence functions of the AFP**.** Recommendation 1 of the Committee's Report on the IM Bill, recommendation 3 of the Committee's Report on the SLAID Bill and recommendation 18 of the Committee's Report on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* recommended that the IGIS's jurisdiction be expanded to the intelligence functions of the AFP.

The Bill would expand the jurisdiction of the IGIS to the intelligence functions of the AFP, in addition to its existing jurisdiction under the PID Act and over the AFP's use of network activity warrants under the Surveillance Devices Act, to provide holistic oversight of the intelligence activities across the NIC. It would also ensure that all agencies within the NIC are subject to the same high standard of oversight. Since the

[12] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 2, items 125 and 127.
[13] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 3.

inception of the NIC as a single enterprise, the AFP has become increasingly interconnected with the other NIC agencies, including through enhanced coordination and information sharing. The introduction of network activity warrant powers under the Surveillance Devices Act in 2021, which are currently overseen by IGIS, also represents a shift in AFP's capabilities since the time of the 2017 Independent Intelligence Review and Comprehensive Review. Network activity warrants provided the AFP with a specific intelligence power to complement existing law enforcement powers.

While the AFP is already subject to a range of oversight mechanisms, IGIS oversight would provide dedicated intelligence oversight of their intelligence activities with the functions, powers, expertise, capabilities and appropriate security clearances required to do so.

The Bill would define the AFP's intelligence function as:[14]

- the collection, correlation, analysis, production and dissemination of intelligence by AFP to support the performance of its functions under paragraphs 8(1)(b), (baa), (bd), (be), (bf), (bg) and (bh) of the AFP Act
- the collection, correlation, analysis, production and dissemination of intelligence by AFP to support the performance of its functions under paragraph 8(1)(c) of the AFP Act in relation to a function under any of the paragraphs of that Act mentioned in paragraph (a) of this subsection
- the collection, correlation, analysis, production and dissemination of intelligence obtained by AFP from the execution of a network activity warrant under Division 6 of Part 2 or Divisions 1 or 2 of Part 6 of the Surveillance Devices Act, or
- a function or power conferred on a law enforcement officer of AFP by a Division referred to in paragraph (c).

For the avoidance of doubt, the Bill specifies that AFP's intelligence function excludes:

- the arrest, charging or detention of suspected offenders, or
- the gathering of evidence, or any activity undertaken to directly support the gathering of evidence.

The definition of AFP's intelligence function also excludes the following AFP functions:

- the provision of police services in relation to the Australian Capital Territory (ACT) under paragraph 8(1)(a) of the AFP Act as these are more equivalent to a State or Territory police force which would not fall within IGIS oversight
- the provision of police services in relation to the Jervis Bay Territory under paragraph 8(1)(aa) of the AFP Act as these are managed through ACT policing and are more equivalent to a State or Territory police force which would not fall within IGIS oversight
- the provision of police services in Australia's external territories under paragraph 8(1)(ba) of the AFP Act in accordance with arrangements entered into under subsection 8(1C) and doing anything else included in the arrangements that is incidental or conducive to the provision of the services, as these are more equivalent to a State or Territory police force which would not fall within IGIS oversight, and

[14] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 6.

- functions conferred by the *Witness Protection Act 1994* (Witness Protection Act) or by a law of a State or Territory that is a complementary witness protection law for the purposes of the Witness Protection Act under paragraphs 8(1)(bb) and 8(1)(bc) of the AFP Act as these are not investigatory in nature and are tied to the administration and management of the National Witness Protection Program under which participation is voluntary on the part of the participants.

This definition aims to capture AFP's key intelligence activities without extending IGIS oversight to operational matters involving AFP's direct and traditional criminal investigative activities and evidence gathering, and those activities which directly support evidence gathering. Those matters are appropriately dealt with by existing oversight and review mechanisms, including by the courts in relation to any prosecutions, noting the courts have the power to determine that evidence collected by the AFP was done so unlawfully and so is inadmissible. The Ombudsman would therefore retain oversight of AFP's administrative actions, the handling of conduct issues falling within the scope of Part V of the AFP Act and ensuring the AFP's compliance with relevant parts of the TIA Act*,* Surveillance Devices Act, Crimes Act and Telecommunications Act.

Interaction with the Ombudsman

The Bill does not propose amending the Ombudsman's jurisdiction over the AFP with respect to administrative actions, Part V of the AFP Act and relevant parts of the TIA Act*,* Surveillance Devices Act (excluding the use of network activity warrants), Crimes Act and Telecommunications Act that confer covert and coercive powers on the AFP. Extending the jurisdiction of the IGIS to cover 'intelligence functions' without a corresponding carve out of the Ombudsman's jurisdiction will require the two oversight entities to develop arrangements and policies to minimise overlap and gaps in oversight in practice. This approach was taken as the intelligence function of AFP is intrinsically linked to the AFP's policing functions such that carving out the Ombudsman's jurisdiction over the AFP's intelligence function could create unintended gaps in the Ombudsman's oversight of AFP's non-intelligence functions. In this circumstance, the overlapping jurisdiction with respect to the AFP's intelligence function is preferable to avoid the risk of gaps in oversight.

Amendments relating to information sharing contained in the Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Bill 2022 and this Bill will support the IGIS and Ombudsman to manage the overlapping jurisdiction, consistent with current arrangements for dealing with overlapping jurisdiction.

Interaction with the Public Interest Disclosure framework

Currently, disclosures relating to the intelligence functions of the AFP may be disclosed to a supervisor or authorised officer of the AFP, or the IGIS under the PID Act. Other non-intelligence disclosures relating to the AFP may be disclosed within the AFP, or to the Commonwealth Ombudsman. The Bill would preserve how disclosures relating to the AFP are currently dealt with under the PID Act.

Interaction with the Australian Human Rights Commission

Currently under subsection 20(4C) of the AHRC Act, if a complaint has been made in relation to the AFP and the AHRC Commissioner is of the opinion that the subject matter of the complaint could be more effectively or conveniently dealt with by the IGIS, the AHRC must transfer the complaint to the IGIS (subject to the IGIS's

agreement). The Bill would preserve this arrangement for the AFP as it effectively supports the AHRC and the IGIS to manage overlapping jurisdiction with respect to the AFP.

Interaction with the National Anti-Corruption Commission

The Bill would make no changes to how issues relating to the AFP are currently dealt with under the NACC Act. The head of AFP, and other prescribed officials, will continue to be required to refer issues to the Commissioner of the NACC, and it would be open to the NACC Commissioner to consult with the IGIS if they receive a corruption allegation that raised sensitive intelligence issues. The existing framework would effectively support the NACC and the IGIS to manage overlapping jurisdiction with respect to AFP.

3.1.4 AUSTRAC

Recommendation 21 of the 2017 Independent Intelligence Review recommended that IGIS's jurisdiction be expanded to all of AUSTRAC. The Comprehensive Review supported expanding IGIS's jurisdiction to the intelligence functions of AUSTRAC.[15] The Committee's Report on the IM Bill did not make any recommendations with respect to the proposed expansion of the IGIS's jurisdiction to the intelligence functions of AUSTRAC.

The Bill would extend the jurisdiction of the IGIS to the intelligence functions of AUSTRAC to ensure IGIS has holistic oversight of the intelligence activities of the NIC.

AUSTRAC's intelligence functions would be defined as the collection, correlation, analysis, production and dissemination of intelligence by AUSTRAC for the purposes of:

- the AUSTRAC CEO performing the CEO's financial intelligence functions under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act); or
- AUSTRAC, the AUSTRAC CEO or any other official of AUSTRAC referred to in paragraph 209(4)(c) of the AML/CTF Act performing functions incidental to that function.

This definition would not capture AUSTRAC's regulatory functions. Examples of activities that may fall within the definition of AUSTRAC's intelligence functions include:

- accessing and collecting information while assessing potential instances of criminal activity, including information obtained under the AML/CTF Act, information from government partners (both domestic and international) and information that is publicly available;
- correlation of information to detect transactions and patterns of behaviour that may be indicative of criminal activity, including money laundering, terrorism financing, and organised crime;
- analysis of information to identify specific targets (including persons, assets, criminal networks and associations), determine links between those targets and possible criminal activity or risks to national security, and derive actionable intelligence; and
- the production of intelligence reports and dissemination to relevant law enforcement, regulatory and national security partners (both domestic and international).

[15] Comprehensive Review of the Legal Framework of the National Intelligence Community, para 40.102.

The department notes that this definition was included in the lapsed IM Bill. The Committee Report on the IM Bill did not make any recommendations in relation to this definition.

Interaction with the Ombudsman

The Bill would maintain the Ombudsman's existing jurisdiction with respect to the intelligence functions of AUSTRAC. As the intelligence functions of AUSTRAC are linked to its regulatory functions, oversight gaps may be created if the intelligence functions are carved out from the Ombudsman's jurisdiction.

The Bill would not amend the Ombudsman's existing jurisdiction over AUSTRAC with respect to administrative actions as AUSTRAC's intelligence functions are linked to its non-intelligence functions. An explicit carve out of the intelligence functions from the Ombudsman's jurisdiction would increase the risk of creating gaps in oversight. However, extending the jurisdiction of the IGIS to cover 'intelligence functions' without a corresponding carve out of the Ombudsman's jurisdiction will require the two oversight entities to develop arrangements and policies to minimise overlap and gaps in oversight in practice.

Amendments relating to information sharing contained in the Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Bill 2022 and this Bill will support the IGIS and Ombudsman to manage the overlapping jurisdiction, consistent with current arrangements for dealing with overlapping jurisdiction.

Interaction with the Public Interest Disclosure framework

The Bill would extend the IGIS's oversight role to public interest disclosures relating to the intelligence functions of AUSTRAC which would enable disclosures relating to the intelligence functions of AUSTRAC to be disclosed to the IGIS under the PID Act, where appropriate. Other non-intelligence disclosures relating to AUSTRAC may be disclosed within AUSTRAC, or to the Commonwealth Ombudsman.

Interaction with the Australian Human Rights Commission

The AHRC currently has jurisdiction over AUSTRAC. Under subsection 20(4C) of the AHRC Act, if a complaint has been made in relation to the ACIC or AFP and the AHRC Commissioner is of the opinion that the subject matter of the complaint could be more effectively or conveniently dealt with by the IGIS, the AHRC must transfer the complaint to the IGIS (subject to the IGIS's agreement). The Bill would extend the complaint transfer mechanism under section 20(4C) of the AHRC Act to AUSTRAC. This would mean that the AHRC would have to consider if a complaint relating to AUSTRAC is more effectively or conveniently dealt with by the IGIS, and if so transfer the complaint to the IGIS (subject to the agreement of the IGIS). This would be consistent with the current approach for agencies that are partially overseen by IGIS, and support the AHRC and the IGIS to manage overlapping jurisdiction.

Interaction with the National Anti-Corruption Commission

The Bill would not change how issues relating to AUSTRAC are currently dealt with under the NACC Act. The head of AUSTRAC, and other prescribed officials, will continue to be required to refer issues to the NACC Commissioner, and it would be open to the NACC Commissioner to consult with the IGIS if they receive a corruption allegation that raised sensitive intelligence issues. The existing framework would effectively support the NACC and the IGIS to manage overlapping jurisdiction with respect to AUSTRAC.

3.1.5 Home Affairs

Recommendation 21 of the 2017 Independent Intelligence Review recommended that IGIS's jurisdiction be expanded to the intelligence functions of Home Affairs. Recommendation 168 of the Comprehensive Review, however, recommended against expanding the IGIS's jurisdiction to the intelligence functions of Home Affairs.

The Bill would expand the IGIS's jurisdiction to the intelligence functions of Home Affairs to provide the IGIS with holistic oversight of the intelligence activities of the NIC which will minimise the risk of gaps in oversight and foster more consistent and targeted oversight. This amendment will ensure that the intelligence activities of NIC agencies are subject to the same standard of oversight, and enhance the assurance provided to the public about the performance of Home Affairs' intelligence functions.

The Bill would define Home Affairs' 'intelligence functions' under regulations made under the IGIS Act.[16] Unlike the other agencies coming within the IGIS's jurisdiction, as a department of state, the matters dealt with by Home Affairs are defined in administrative arrangement orders. Defining Home Affairs' intelligence functions in regulations will ensure that updates can be made in a timelier manner in the event of any administrative changes that effect the scope of Home Affairs' intelligence functions.

The Bill would also allow the regulations to prescribe consultation requirements, and require the Minister for Home Affairs' agreement to be obtained before any regulations prescribing the intelligence functions or consultation requirements are made or amended.[17]

Proposed approach to regulations

The Government's intent is to progress regulations which define Home Affairs' intelligence functions by reference to the 'Intelligence Division' within Home Affairs as the intelligence activities of the department are currently confined to that division.

The Intelligence Division within Home Affairs undertakes intelligence analysis in support of policy and operational decision making in the Department of Home Affairs and the Australian Border Force, and to inform a number of other whole-of-government priorities, including threats to Australia's national security and resilience. At the strategic level, the Intelligence Division is integrated within the NIC and actively participates in NIC mission governance forums through the Australian Intelligence Mission framework. The Intelligence Division works with the NIC to provide dedicated intelligence support to operations and policy decision-making with a border nexus, including threats beyond, at and post Australia's border.

The department notes that recommendation 169 of the Comprehensive Review recommended that legislation establishing oversight responsibilities for the NIC should take a functional approach and that oversight should follow intelligence function, regardless of the structures used to support performance of the function for the following reasons. The Comprehensive Review noted that the risks of a structural approach include agencies being able to move activities out of the area being overseen, and arrangements becoming quickly outdated as internal and broader restructures may occur more frequently than the updating of

[16] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 6.
[17] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 6.

legislation.[18] However, defining the Home Affairs' intelligence legislation in regulations mitigates the risks of a structural approach as it will allow regulations to be updated in a timely manner as required to reflect changes to structure. The Bill also mitigates the risks of a structural approach by enabling the regulations to prescribe consultation requirements, including those necessary to ensure that changes in structure that may impact on oversight arrangements are able to be identified promptly and reflected in the regulations.

Interaction with the Ombudsman

The Bill would amend the Ombudsman Act and TIA Act to allow regulations to be made excluding parts of Home Affairs from the Ombudsman's jurisdiction, if required.

Home Affairs' intelligence functions can be clearly delineated from its non-intelligence functions. The intended regulations would exclude the 'Intelligence Division' from the Ombudsman's general jurisdiction that is provided for under the Ombudsman Act and from the Ombudsman's jurisdiction in relation to specific powers under the TIA Act.

However, in the event that there is a change to the intelligence functions of Home Affairs or to the scope of the IGIS's jurisdiction, prescribing the Ombudsman's jurisdiction with respect to Home Affairs in regulations will ensure that the scope of the Ombudsman's oversight can be updated in a timely manner to ensure there are no gaps in oversight.

Interaction with the Public Interest Disclosure framework

The Bill would extend the IGIS's oversight role to public interest disclosures relating to the intelligence functions of Home Affairs which would enable disclosures relating to the intelligence functions of Home Affairs to be disclosed to the IGIS under the PID Act, where appropriate. Other non-intelligence disclosures relating to Home Affairs may be disclosed within Home Affairs, or to the Commonwealth Ombudsman.

Interaction with the Australian Human Rights Commission

The AHRC currently has jurisdiction over Home Affairs. Under subsection 20(4C) of the AHRC Act, if a complaint has been made in relation to the ACIC or AFP and the AHRC Commissioner is of the opinion that the subject matter of the complaint could be more effectively or conveniently dealt with by the IGIS, the AHRC must transfer the complaint to the IGIS (subject to the IGIS's agreement). The Bill would extend the complaint transfer mechanism under section 20(4C) of the AHRC Act to Home Affairs. This would mean that the AHRC would have to consider if a complaint relating to Home Affairs is more effectively or conveniently dealt with by the IGIS, and if so transfer the complaint to the IGIS (subject to the agreement of the IGIS). This would be consistent with the current approach for agencies that are partially overseen by IGIS, and support the AHRC and the IGIS to manage overlapping jurisdiction.

Interaction with the National Anti-Corruption Commission

The Bill would make no changes to how issues relating to Home Affairs are currently dealt with under the NACC Act. The head of Home Affairs, and other prescribed officials, will continue to be required to refer

[18] Comprehensive Review of the Legal Framework of the National Intelligence Community, para 40.107.

issues to the NACC Commissioner, and it would be open to the NACC Commissioner to consult with the IGIS if they receive a corruption allegation that raised sensitive intelligence issues. The existing framework would effectively support the NACC and the IGIS to manage overlapping jurisdiction with respect to Home Affairs.

3.2 Expanding the Committee's jurisdiction

3.2.1 Summary

The Bill would expand the Committee's jurisdiction to the whole of the ACIC, and the intelligence functions of AUSTRAC, AFP and Home Affairs to provide holistic parliamentary oversight of the intelligence activities of the NIC. The Bill would also allow the Committee to review, on its own motion, proposed reforms to counter-terrorism and national security legislation, and all such expiring legislation.

These amendments would ensure the Committee has holistic oversight of the agencies within the NIC, and the counter-terrorism and national security legislation that supports the NIC.

3.2.2 Additional NIC agencies

Recommendation 21 of the 2017 Independent Intelligence Review recommended that the jurisdiction of the Committee be expanded to all of AUSTRAC, and the intelligence functions of the AFP, ACIC and Home Affairs. Recommendation 23(c) recommended allowing the Committee to initiate its own inquiries into the administration and expenditure of the ten intelligence agencies of the NIC. The Comprehensive Review did not make a recommendation in relation to the Committee's jurisdiction over AUSTRAC, AFP, ACIC or Home Affairs.

Recommendations 1 and 2 of the Committee's Report on the IM Bill and the Committee's Report on the SLAID Bill recommended that the jurisdiction of the Committee be expanded to the intelligence functions of the AFP and the intelligence functions of the ACIC. Recommendation 19 of the Committee Report on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* also recommended that the Committee's jurisdiction be expanded to the intelligence functions of the ACIC.

Consistent with the agencies wholly within the Committee's jurisdiction, the Bill would amend the functions of the Committee to add reviewing the administration and expenditure of the ACIC, including the annual financial statements of the ACIC, and reviewing any matter in relation to the ACIC that is referred to the Committee by the responsible Minister, the Attorney-General or a resolution of either House of the Parliament.[19] This approach reflects the inseparable nature of the ACIC's intelligence functions with the rest of the ACIC's functions.

In relation to AFP, AUSTRAC and Home Affairs, the Bill would amend the functions of the Committee to add:[20]

- reviewing the administration and expenditure, including the annual financial statements, of the AFP, AUSTRAC and Home Affairs in relation to the performance of those agencies' intelligence functions
- monitoring and reviewing the performance by the AFP, AUSTRAC or Home Affairs of those agency's

[19] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, items 50 and 51.
[20] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, items 50 and 53.

intelligence functions, that is referred to the Committee by the responsible Minister, the Attorney-General or a resolution of either House of the Parliament,[21] and

- reporting to both Houses of the Parliament on any matter appertaining to AFP, AUSTRAC or Home Affairs that is connected with the performance of those agency's intelligence functions, that are referred to the Committee by the responsible Minister, the Attorney-General or a resolution of either House of the Parliament.

The Bill would also amend the functions of the Committee to provide that the Committee may, by resolution, request the responsible Minister or the Attorney-General to refer a matter in relation to the activities of the ACIC; or the activities of AFP, AUSTRAC or Home Affairs in relation to the performance of those agencies' intelligence functions.[22]

The intelligence functions of AFP, AUSTRAC and Home Affairs would be defined by reference to the definitions of those terms in the IGIS Act.[23]

The expansion of the Committee's jurisdiction to all NIC agencies would provide holistic parliamentary oversight of the intelligence activities of the NIC, and ensure that all NIC agencies are subject to the same high standard of specialised-intelligence oversight that is commensurate with their powers and responsibilities.

Exclusions

Consistent with the current limitations on the Committee's jurisdiction, the Bill does not provide the Committee with direct operational oversight over the ACIC, or the intelligence functions of AFP, AUSTRAC and Home Affairs.

To ensure that operational information is not reviewed by the Committee and to provide exclusions consistent with the other agencies either wholly or partly within the Committee's jurisdiction, the Bill excludes from the Committee's functions:[24]

- the intelligence gathering and assessment priorities of the ACIC
- the sources of information, other operational assistance or operational methods available to the ACIC
- reviewing special ACC operations (within the meaning of the ACC Act) or special ACC investigations (within the meaning of the ACC Act) that have been, are being or are proposed to be undertaken by the ACIC
- reviewing an aspect of the activities of the ACIC that does not affect an Australian person
- conducting inquiries into individual complaints about the activities of AUSTRAC and ACIC (noting this exclusion already applies to AFP and Home Affairs)
- reviewing sensitive operational information or operational methods available to AUSTRAC and Home Affairs (noting this exclusion already applies to AFP), and

[21] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 6.
[22] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 55 and 56.
[23] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 47.
[24] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, items 58 to 64.

- reviewing particular operations or investigations that have been, are being or are proposed to be undertaken by AUSTRAC and Home Affairs (noting this exclusion already applies to the AFP).

The Bill also amends the definition of 'operationally sensitive information' to include information about:

- sources of information, other operational assistance or operational methods available to the ACIC
- particular operations that have been, are being or are proposed to be undertaken by the ACIC
- sources of information, other operational assistance or operational methods available to AFP AUSTRAC or Home Affairs in exercising those agencies' intelligence functions, and
- particular operations that have been, are being or are proposed to be undertaken by AFP, AUSTRAC or Home Affairs in exercising those agencies' intelligence functions.

Information protection

The Bill would include new categories of information to the list of information that must not be disclosed to Parliament, to ensure appropriate limitations on the disclosure of sensitive information, including to the public-at-large through a report to Parliament.

Proposed paragraphs 7(1)(d) to (i) are based on the disclosure restrictions in the *Parliamentary Joint Committee on Law Enforcement Act 2010*.[25] These categories reflect that ACIC, AUSTRAC, AFP, and Home Affairs may deal with information that does not constitute national security information, but is sufficiently sensitive to warrant appropriately limited disclosure.

Interaction with the Parliamentary Joint Committee on Law Enforcement

The Bill does not make any changes to the jurisdiction of the PJCLE. It is appropriate to retain the PJCLE's existing jurisdiction to ensure comprehensive oversight from a law enforcement perspective. Further, given the different focuses of the Committees, overlap in inquiry topics is likely to be minimised and can be dealt with administratively.

3.2.3 Counter-terrorism and national security legislation

Recommendations 23(b) and (c) of the 2017 Independent Intelligence Review recommended that the Committee's functions be expanded to enable the Committee to review on its own motion proposed reforms to counter-terrorism and national security legislation, and all such expiring legislation. The Comprehensive Review agreed with these recommendations.[26]

The Committee is responsible for reviewing the operation, effectiveness and implications of a range of counter-terrorism and national security legislation. As a matter of practice, the Committee also reviews proposed counter-terrorism and national security legislation. The Committee provides an important accountability mechanism in ensuring that proposed legislation is, or existing legislation continue to be, appropriate and fit for purpose.

[25] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 77.
[26] Comprehensive Review of the Legal Framework of the National Intelligence Community, para 42.12.

The Bill would amend the functions of the Committee to enable it to review, on its own motion, proposed amendments to counter-terrorism and national security legislation, and all such expiring legislation.[27] This would explicitly recognise the Committee's role in relation to counter-terrorism and national security legislation in the statutory functions of the committee.

3.3 Strengthening the relationship between intelligence oversight bodies and supporting the Committee's oversight role

3.3.1 Summary

The Bill would strengthen the relationship between the Committee, IGIS and INSLM to enhance coordination and cooperation between Australia's intelligence oversight bodies.

3.3.2 Briefings by the Committee

Recommendation 23(d) of the 2017 Independent Intelligence Review recommended amendments to enable the Committee to request a briefing from the INSLM, ask the INSLM to provide the Committee with a report on matters referred by the Committee, and for the INSLM to provide the Committee with the outcome of the INSLM's inquiries into existing legislation at the same time as the INSLM provides such reports to the responsible Minister.

Although the IS Act does not prevent the Committee from requesting the INSLM to provide a briefing, the Bill would add the INSLM to the list of persons from whom the Committee may request a briefing to clarify this position.[28] The INSLM would continue to have the discretion to not provide a briefing where it would be inappropriate to do so.

The Bill does not make amendments to enable the Committee to ask the INSLM to provide it with reports on matters referred by the Committee. The Committee may request the INSLM to provide it with reports on matters referred by the Committee.

The Bill does not require the INSLM to provide the Committee with the outcome of the INSLM's inquiries into existing legislation at the same time as the INSLM provide such reports to the responsible Minister. This is consistent with the fact that the INSLM is a statutory independent executive oversight body, established with the object of assisting Ministers to ensure that counter-terrorism and national security legislation is effective, consistent with international obligations and contains appropriate safeguards. Maintaining the INSLM's current discretion with regards to reports provided to the Committee appropriately reflects the INSLM's independence, and role to assist Ministers.

3.3.3 Referrals from the Committee to the IGIS

Recommendation 23(a) of the 2017 Independent Intelligence Review recommended that amendments be made to enable the Committee to request the IGIS conduct an inquiry into the legality and propriety of particular operational activities of NIC agencies, and to provide a report to the Committee, Prime Minister

[27] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 52.
[28] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 67.

and responsible Minister. Recommendation 181 of the Comprehensive Review recommended that recommendation 23(a) of the 2017 Independent Intelligence Review be implemented, provided that the Committee maintain its current restriction that prevents the Committee from requiring the disclosure of operationally sensitive information or information that would or might prejudice Australia's national security or the conduct of Australia's foreign relations.

Requests to inquire

The Bill amends the functions of the Committee to enable it to request the IGIS conduct an inquiry into a matter that relates to the legality and propriety of the operational activities of an agency, is within the functions of the IGIS, and does not relate to an individual complaint about the activities of an agency.[29] The Committee is not limited to requesting the IGIS inquire into matters that are within the Committee's own jurisdiction, and may request the IGIS to inquire into matters that are outside of the Committee's jurisdiction, such as operational matters.

This amendment will enhance oversight of the NIC by providing an avenue for matters of concern identified by the Committee, that cannot be reviewed by the Committee, to be brought to the IGIS's attention.

Responses to requests

The Bill also amends the functions of the IGIS to provide the IGIS with the discretion to undertake an inquiry at the request of the Committee.[30] If the IGIS does undertake an inquiry at the request of the Committee, the Bill requires that the IGIS must take reasonable steps to give a written response to the Committee, unless the Inspector-General is satisfied on reasonable grounds that doing so would prejudice security, the defence of Australia or Australia's relations with other countries.[31] The Bill also makes it clear that the Committee must not require the Inspector-General to disclose operationally sensitive information or information that would or might prejudice Australia's national security or the conduct of Australia's foreign relations, which reflects the current prohibition set out in clause 1 of Schedule 1 to the IS Act.

The IGIS and the head/s of the relevant intelligence agencies to which the inquiry relates must also agree that the terms of the proposed response would not prejudice:

- security, the defence of Australia or Australia's relations with other countries – consistent with Schedule 1 of the IS Act which restricts the Committee from requesting such information
- law enforcement operations, including methodologies and investigative techniques – reflecting that such information may not prejudice security or operationally sensitive information, but is still sufficiently sensitive to warrant appropriately limited disclosure.
- confidential commercial information held by AUSTRAC – to support confidence between AUSTRAC and the entities it regulates noting that as an agency with both intelligence and regulatory functions, AUSTRAC holds information collected from entities it regulates that may include confidential commercial information, or

[29] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 57.
[30] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 17.
[31] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 30.

- operationally sensitive information (within the meaning of Schedule 1 of the IS Act) – consistent with Schedule 1 of the IS Act which restricts the Committee from requesting such information.

For a response to be able to be provided to the Committee, the Inspector-General and head/s of the relevant intelligence agency/agencies must agree that there is no risk that the terms of the response would prejudice the above listed factors if provided to the Committee. For example, a response would be prejudicial to security if it causes, or could reasonably be expected to cause, harm to security.

These provisions as drafted are subject to a range of essential safeguards that reflect the sensitive nature of intelligence information.

Requiring the IGIS and agency heads to reach agreement in relation to the above categories reflects the important principle that agency heads are uniquely positioned to assess the sensitivity of information which originates from their agency, and the potential harm to national security the disclosure of that information may cause. Potential harm might include significant adverse consequences for Australia's intelligence agencies and foreign partner agencies, potentially compromising both current and future intelligence operations.

The Bill also requires the IGIS to consult with the head of the relevant intelligence agency as to whether the terms of the proposed response would prejudice the privacy of individuals, the fair trial of a person, or the impartial adjudication of a matter.[32] The IGIS then has the discretion to decide whether to exclude the information from the terms of the response. This reflects the more generalised nature of the risks, and that the IGIS is well-placed to assess these categories of information in order to assess whether the risks of disclosure outweigh the benefits to oversight.

If a report cannot be provided to the Committee, the IGIS must advise the Committee the reasons that a response could not be provided.

The department notes that the IGIS would still be required to provide reports on the inquiry to relevant Ministers in accordance with Division 4 of Part 2 of the IGIS Act.

3.3.4 Briefing by DGNI and IGIS

Recommendation 23(e) of the 2017 Independent Intelligence Review recommended that the Director-General of ONI and the IGIS be required to provide regular briefings to the Committee. The Comprehensive Review did not recommend against this amendment.[33]

The Bill would provide a requirement for the Committee to be briefed at least once each calendar year by the Director-General of ONI,[34] and separately by the IGIS.[35]

[32] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 30.
[33] Comprehensive Review of the Legal Framework of the National Intelligence Community, para 42.12
[34] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 85.
[35] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 44.

Given the ONI's significant coordination and evaluation role in relation to NIC agencies, briefings at least annually by the Director-General of ONI would support the Committee's oversight of those agencies. In practice, DGNI already briefs PJCIS several times a year, but this Bill would solidify this practice in legislation.

Annual briefings by the IGIS would also provide Committee members with a broader view on the role of the IGIS, and matters relevant to the Committee's functions.

3.4 Amendments to modernise, clarify and enhance the efficiency of the Committee

The Bill would amend the IS Act to modernise and clarify provisions related to the Committee and to enhance the efficiency of the Committee.

The Bill would:

- repeal redundant provisions (including those relating to reviews which have been completed)[36]
- include in the list of persons from whom the Committee may request a briefing to include any other agency head related to a Bill or matter under review by the Committee,[37] and clarify that the list is non-exhaustive[38]
- update the obligations of the committee to ensure they are adapted for contemporary circumstances[39]
- modernise clearance requirements, including to reflect existing practices,[40] and
- clarify the powers and procedures of sub-committees.[41]

The Bill would also make amendments that would ensure that classified information remains subject to appropriate protections. The amendments would provide that the Committee is unable to disclose evidence carrying a national security classification, or that the Committee believes should carry a national security classification without the approval of the relevant agency head or person (as applicable).[42] The written authority of the relevant agency head or person is not required for disclosure of unclassified information unless the PJCIS believes that the information should have a national security classification (for example where classified information is received from a former staff member of an intelligence agency but the document itself does not carry a classification).

These measures will ensure that the legislation governing the Committee is adapted to contemporary circumstances.

[36] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 54.
[37] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 67.
[38] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 66.
[39] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, items 78 and 79.
[40] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 80.
[41] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, items 73 and 81 to 84.
[42] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 77.

3.5 Enhancing the efficiency of the IGIS's complaints jurisdiction

The Bill would clarify the IGIS's complaints jurisdiction to provide that the Inspector-General is not required to commence an inquiry into any matters raised in a complaint if the Inspector-General is not satisfied that the action complained of is the kind of action that is reasonably likely to have been taken by an intelligence agency.[43] This measure will improve the efficiency of the IGIS's complaint handling functions in circumstances where activity alleged in a complaint is considered to be highly implausible or otherwise not credible.

Subsection 11(1) of the IGIS Act provides that the Inspector-General must commence an inquiry into actions raised in a complaint if inquiring into that action is within the functions of the Inspector-General unless subsection 11(2)-(6) apply. Item 22 of the Bill would insert a new subsection 11(1)(aa). This would enable the Inspector-General to exercise their discretion not to inquire into action that is alleged in a complaint that is highly implausible or otherwise not credible. This discretion could only be exercised in circumstances where the Inspector-General is not satisfied that the action complained of is the kind of action that is reasonably likely to have been taken by an intelligence agency.

The IGIS Act was enacted in 1986. Since that time, the IGIS's workload, including the number of contacts the IGIS receives from members of the public, has steadily increased. In the 2021-2022 financial year, the IGIS received 431 contacts from members of the public. Given the expansion of the IGIS's jurisdiction to additional intelligence agencies provided for in this Bill, as well as the proposed expansion to IGIS's complaints jurisdiction in relation to ONI and DIO contained in the Modernisation Bill, it is likely that the IGIS will experience a further increase in the volume of contacts received. This measure will assist the IGIS to more effectively and efficiently manage its complaints handling function in light of an increased jurisdiction by allowing it to more easily deal with contacts where the IGIS is not satisfied that the action complained of is the kind of action that is reasonably likely to have been taken by an intelligence agency.

3.6 ACIC Criminal Intelligence Assessments

Schedule 3 of the Bill will amend the *Administrative Appeals Tribunal Act 1975* (AAT Act) to enable matters relating to ACIC criminal intelligence assessments arising under the Archives Act to be heard in the Security Division of the AAT. The amendments would provide that, for the purposes of a proceeding relating to an application under the Archives Act to review a decision in respect of access to a record of the ACIC relating to a criminal intelligence assessment, the record is an exempt security record as defined in the AAT Act (as amended by NSLAB No. 2).

Criminal intelligence assessments (as defined in section 36A the ACC Act) are written statements prepared by the ACIC expressing any recommendations, opinions or advice on whether it is necessary or desirable for prescribed administrative actions to be taken in respect of a person, having regard to whether there is intelligence or information that suggests that the person may commit or assist another person to commit a serious or organised crime or may assist another person to do so. Criminal intelligence assessments are likely

[43] Intelligence Services Legislation Amendment Bill 2023, schedule 1, part 1, item 22.

to contain information of a sensitive nature such as the identities of criminal informants as well as undercover and covert operations conducted by the ACIC or other police agencies.

In recognition of these sensitivities, section 36J of the ACC Act appropriately provides that reviews of decisions by the ACIC to make an adverse criminal intelligence assessment must be heard by the Security Division of the AAT.

Records relating to ACIC criminal intelligence assessments are also likely to contain classified or sensitive information. These amendments will ensure the sensitive information contained in such records is subject to appropriate safeguards within the AAT. The amendments in this Bill are intended to ensure consistency in the way the AAT treats both reviews of a decision by the ACIC to make an adverse criminal intelligence assessment and reviews of decisions relating to access of ACIC records related to criminal intelligence assessments. These amendments would also make the treatment of records relating to ACIC criminal intelligence assessments consistent with that of exempt security records (as amended by NSLAB No.2).

The Bill would also insert new subsection 19F(3A) into the AAT Act which would provide that if a proceeding relates to an ACIC record related to criminal intelligence assessments, a presidential member of the AAT must not participate in the proceeding if the presidential member is or has been a member of the staff of the ACIC (within the meaning of the ACC Act).[44] This will mitigate the risk of an actual or perceived conflict of interest whereby a presidential member who was previously a member of the staff of the ACIC is participating in a proceeding regarding a decision by the Archives in respect of access to an ACIC record relating to a criminal intelligence assessment.

3.7 Exemptions from liability for defence officials

Recommendation 72 of the Comprehensive Review recommended that the Criminal Code be amended to give Australian Defence Force members immunity under Part 10.7 for computer-related acts done outside Australia in the course of properly declared operations under legally approved rules of engagement.

The Bill addresses recommendation 72 of the Comprehensive Review. Schedule 4 of the Bill will amend the Criminal Code to provide defence officials with an exemption from civil and criminal liability for computer-related conduct engaged inside or outside Australia, if they engage in conduct on the reasonable belief that it is likely to cause a computer related act, event, circumstance or result to take place outside of Australia, and the conduct was done in the proper performance of authorised activities of the Australian Defence Force.

Proposed subsections 476.7(1) and 476.7(2) largely mirror the immunities conferred on staff members of ASD, AGO and ASIS, as recommended by the Comprehensive Review (see paragraph 24.194). Unlike ASD, AGO and ASIS, which have statutory functions, the immunity for Defence officials will be for conduct which is undertaken in accordance with the 'proper performance of authorised ADF activities'. This means activities done in accordance with operational orders, rules of engagement and target directives, as issued by the Chief of the Defence Force (CDF). This aligns with the Comprehensive Review's finding that the immunity should be for conduct done under legally approved rules of engagement.

[44] Intelligence Services Legislation Amendment Bill 2023, schedule 3, item 3.

The Bill takes an approach that is consistent with that for ASD, AGO and ASIS under section 476.6 of the Criminal Code. It provides a specific immunity from the conduct covered by Part 10.7, and reflects that there may be conduct that could cause a 'computer-related act, event, circumstance or result' that may attract civil or criminal liability under other laws. The activity that is covered is limited by several aspects, notably the scope of the definition of computer-related act, event, circumstance or result. This is consistent with the Comprehensive Review, which stated that the new immunity should be similar to existing immunities provided for offshore computer-related activities undertaken by ASD, ASIS, and AGO (see paragraph 24.194 of the Review).

Changing operating environment for the Australian Defence Force

Offensive and defensive cyber operations, including those conducted as a precursor to military operations, are integral to supporting the ADF. Cyber-attacks have increasingly become a part of modern warfare. For example, hacking enemy computer systems that operate air defences to facilitate an air attack. During the Comprehensive Review, the Department of Defence submitted that current legal uncertainty requires the ADF to engage with an unacceptable level of risk, refrain from employing the full extent of its capabilities, or rely on indirect mechanisms that unnecessarily divert agency resources or that inappropriately subject it to the direction and control of other agencies (see paragraph 24.191 of the Comprehensive Review).

The ability to engage in conduct both inside and outside Australia that causes a computer-related act outside Australia is necessary to ensure that Defence officials can perform routine activities such as computer intelligence gathering and exploitation, and generate offensive and defensive effects through cyber capabilities where necessary. Defence officials must have a strong legal basis to perform routine activities such as computer intelligence gathering and exploitation and, where necessary, employ the full extent of their offensive and defensive cyber capabilities.

Defence has effective, disciplined, well-rehearsed targeting processes and procedures in place which enhance operational success while minimising unintended outcomes and the potential for incidental damage. These processes and procedures are set out in targeting doctrine, targeting directives and rules of engagement. Importantly, legal officers and their advice are integrated into the decision-making process to ensure that legal considerations are identified and addressed appropriately, as early as possible, and for residual legal risks to be clearly articulated to, and understood by decision-makers. A key method through which decision-makers receive context-specific legal advice is through the provision of a Legal Target Analysis. A Legal Target Analysis covers compliance with domestic and international law targeting directives, and rules of engagement.

The below example demonstrates how ASD's reliance on its immunity resulted in a successful military operation (where an overseas computer-related effect was generated from within Australia).

Case example: Tigris River Valley

In 2016, ASD was able to support safe passage to Iraqi and partner troops as they advanced north up the Tigris River Valley, by providing offensive cyber capabilities to inhibit Islamic State fighters. Canberra based ASD employees used unique capabilities to integrate cyber effects with real-time military operations, and disable ISIS battlefield communication channels. The operation helped the Iraqis liberate the Tigris River

Valley south of Mosul, reclaim Qayyarah Airfield, and isolate and subsequently clear eastern Mosul by early 2017. Whilst the computer-related act was generated inside Australia, the intended effect was to occur outside Australia in support of military operations.

Although this example used the ASD workforce, and could therefore rely on the immunities available to ASD, similar activities will increasingly need to be conducted by ADF personnel, Australian Public Service employees, and other persons engaged by Defence. The Comprehensive Review acknowledged that there will be situations where ASD will not be able to meet Defence's operational requirements in theatre and time critical situations (see paragraph 24.188). The Review also noted the impact of reliance on indirect mechanisms that unnecessarily divert agency resources or inappropriately subject it to the direction and control of other agencies (see paragraph 24.191).

Defence officials

While the Comprehensive Review only contemplated the ADF undertaking these computer-related activities, Defence's outcomes are not only achieved by uniformed ADF personnel. The Defence Strategic Review reflects the need to enable a genuine integrated force. All parts of Defence's workforce, including defence industry partners, may participate in activities to achieve Defence's mission, including for cyber activities. Ensuring that the immunity can apply across all parts of the workforce provides the necessary flexibility to cater for future requirements in an increasingly complex environment.

The term 'defence officials' is defined to include the various members of the integrated defence workforce, who ensure the security and defence of Australia. This includes:

- members of the ADF
- defence civilians within the meaning of the *Defence Force Discipline Act 1982*
- APS employees, contractors and consultants and the Secretary of the Department of Defence
- a person who is made available by another Commonwealth, state or territory government, or other person to perform services for the Department of Defence, and
- any person included in a class of persons specified in a declaration made by the Secretary of the Department of Defence, CDF, or a delegate[45] under the Bill.

Preparatory conduct

Cyber operations can also be complex tools in a military environment, requiring varying levels of preparatory or supporting conduct before the actual conduct occurs. The Bill also provides an exemption for persons who engage in activities, inside or outside Australia, that are preparatory to, in support of, or otherwise directly connected with Australian Defence Force activities outside Australia.

The Comprehensive Review states that the 'ADF may be required to undertake computer-related activities when pre-positioning in theatre under properly authorised operations, but because armed conflict is yet to occur combat immunity does not apply to its activities' (paragraph 24.190). The example set out above

[45] This delegation is limited to SES employees.

(where ASD supported ADF and coalition forces in the Tigris River Valley) illustrates why it is necessary for immunities to apply to those who are undertaking conduct 'in support of, or otherwise directly connected with, authorised ADF activities outside Australia'.

The proposed immunity is appropriately limited to preparatory, supporting or directly connected acts that together with the act, event, circumstance or result that took place, or was intended to take place overseas, would amount to an offence. The immunity also only applies to conduct undertaken in the proper performance of authorised ADF activities.

Location of activity

The immunity is necessary to allow Defence to continue to operate effectively in an increasingly complex online environment, where it is not always possible to reliably determine the geographic location of a device, data or a computer. This challenge is exacerbated where both state and non-state adversaries take active steps to obfuscate their physical location or the assets being used. For Defence to be able to effectively perform military activities in such an environment, it is critical to protect Defence officials from liability if they inadvertently affect a computer or device located inside Australia.

The immunity is appropriately limited by the requirement for reasonable belief that the activity is occurring outside Australia. The amendments will not provide Defence officials with immunity from civil or criminal liability in circumstances where they know or believe a target computer or device to be located inside Australia. Nor will it provide such persons with immunity where their belief that a target computer or device is likely located outside Australia is not reasonable. The immunity will also no longer apply once it is known to the Defence official that the target is not outside Australia.

For example, where the location of a device is unknown, but the Defence official subsequently becomes aware that its location is inside Australia. Any continued targeting in Australia by a Defence official, once the relevant official is aware that it is within Australia, would constitute an offence. This approach aligns with Recommendation 74 of the Comprehensive Review, to confer immunity where there is reasonable belief conduct is likely to take place outside Australia, whether or not it in fact takes place outside Australia.

Notification requirements

The amendment also requires that a person must provide written notification if they engage in conduct that causes material damage, material interference or material obstruction to a computer in Australia. This notification will go to the CDF for persons who fall under the CDF's command and to the Secretary of the Department of Defence in other cases. The notification process will facilitate consideration at the most senior levels within Defence of any necessary or appropriate internal review processes, to ensure accountability. Such review could include consideration of the legal basis for the original conduct, or operational review to ensure computer capabilities were used appropriately and in line with Defence standard operating procedures. The CDF and Secretary of the Department of Defence would also be able to take steps to remedy any issues identified in such an internal review, such as updating procedures and guidelines, and take any disciplinary action if that is necessary.

4. Conclusion

The department thanks the Committee for the opportunity to make a submission to its review of the Intelligence Services Legislation Amendment Bill 2023. Strong and effective oversight mechanisms are an essential part of advancing Australia's national security interests. The Bill would enhance existing parliamentary and statutory oversight mechanisms to ensure oversight of the NIC is holistic, and commensurate with those agencies' responsibilities and powers.