Senate Finance and Public Administration Legislation Committee

PO Box 6100

Parliament House

Canberra ACT 2600

21 October 2020

Re: Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020

To the Committee,

We are grateful for the opportunity to make a submission to this inquiry. We do so as members of the Griffith Criminology Institute (Dr Hardy) and the Gilbert + Tobin Centre of Public Law (Professor Williams). We are solely responsible for the views and content in this submission.

We welcome the introduction of Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020 (Cth) ('the Bill') and support its enactment. The changes will make an important contribution to the accountability of Australia's intelligence agencies, beyond the six agencies that comprise the Australian Intelligence Community. We respond briefly below to two issues raised in the government's submission to this inquiry, but otherwise support the Bill in its entirety. We also attach, as an Appendix, a chapter we contributed to a book on global oversight of intelligence agencies, edited by members of the NYU Center on Law and Security. In that chapter, we explore why enhancing oversight of Australia's intelligence agencies remains an important task.

The Bill proposes three main changes. First, it will expand the list of agencies that fall under the mandate of the Inspector-General of Intelligence and Security (IGIS). In addition to the six agencies in the Australian Intelligence Community (AIC), the IGIS would have oversight of the Australian Criminal Intelligence Commission (ACIC) and four agencies 'with an intelligence role or function'. Currently, this phrase is defined to include AUSTRAC, the Australian Federal Police, the Department of Home Affairs and the Department of Defence.[1]

Second, the Bill will expand the mandate of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to cover the same list of agencies. The PJCIS would continue to examine the administration and expenditure (but not the operations or activities) of those agencies.[2] Third, the Bill will allow the PJCIS to initiate its own inquiries and refer matters to the IGIS and the Independent National Security Legislation Monitor (INSLM).

We concur with the findings of the 2017 Independent Intelligence Review ('Independent Review'), which recommended these changes to enhance accountability and oversight of the National Intelligence Community. In particular, we support this statement offered by the Independent Review, which is repeated in the Explanatory Memorandum:

> It is critical in a democracy that intelligence agencies are subject to strong oversight and accountability mechanisms. Indeed, oversight of intelligence services is a central tenet of the 'state of trust' between intelligence services and the community of which they are part.[3]

We therefore support the passage of the Bill. These changes are needed because Australia lacks the same levels of oversight as other members of the Five Eyes network. For example:

---

[1] *Office of National Intelligence Act 2018* (Cth) s 4.
[2] *Intelligence Services Act 2018* (Cth) s 29.
[3] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review* (Department of the Prime Minister and Cabinet, 2017) 111.

- In the UK, the Intelligence and Security Committee of Parliament can examine the 'expenditure, administration, policy and operations' of MI5, MI6 and GCHQ.[4]
- In the US, the Senate Select Committee on Intelligence provides 'vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States'.[5]
- In Canada, the newly established National Security and Intelligence Review Agency (NSIRA) is a body of appointed experts that reports to Parliament. The NSIRA has access to all classified information held by Canada's intelligence agencies, with the only exception being documents that are marked as Cabinet-in-confidence.[6] The agency was established in 2019 to replace the Security Intelligence Review Committee, which was Canada's equivalent to the PJCIS.

In the context of these strong oversight measures overseas, the proposed changes in the current Bill are comparatively minor and should be supported.

We note that several federal government agencies have previously made a submission to this inquiry. Below, we address two issues raised in that submission. The first is whether the Department of Defence (beyond AGO and DIO) should be included in the list of proposed agencies, and the second is whether the additional mandate for IGIS and the PJCIS would create overlap and duplication across different accountability bodies. The government submission suggests that oversight by IGIS of these additional agencies is not needed, as they are already scrutinised by bodies including the Inspector-General ADF (IGADF), the Commonwealth Ombudsman and the Auditor-General.

[4] *Justice and Security Act 2013* (UK) c 18, s 2.
[5] US Senate Select Committee on Intelligence, *About the Committee* (last accessed 20 October 2020) <https://www.intelligence.senate.gov/about>.
[6] *National Security and Intelligence Review Agency Act*, SC 2019, c 13, s 9(1).

By referring to agencies 'with an intelligence role or function',[7] the Bill would include the Department of Defence within the remit of the IGIS and PJCIS. As the government submission correctly points out, Defence was not included in the list of 10 recommended agencies by the Independent Review. However, the review did not exclude it either. The authors stated that there was a 'compelling case for a consistent oversight regime to apply to all the intelligence capabilities that support national security'.[8] They added that it was inappropriate and unnecessary to expand the remit of the IGIS or PJCIS beyond intelligence capabilities,[9] but they did not exclude any particular agencies for other reasons, such as security concerns or existing oversight measures. Their concern was to increase oversight of intelligence functions performed by any other agencies, provided that the additional oversight did not include their other, non-intelligence activities. The Bill addresses this issue by allowing the IGIS and PJCIS to oversee the activities of the agencies only to the extent they relate to intelligence.

The Bill is therefore consistent with the recommendations of the Independent Review, even though the changes would include Defence in the list of additional agencies. Defence is clearly a department, to use the words of the Independent Review, which has 'intelligence capabilities that support national security'.[10] The fact that Defence was previously included in the *Office of National Intelligence Act 2018* (Cth) as an 'agency with an intelligence role or function' provides further support for this position. There is no clear justification for the IGIS and PJCIS to oversee the intelligence activities of the AFP and Home Affairs, but not the Department of Defence, only because the Independent Review did not specifically refer to it.

[7] *Office of National Intelligence Act 2018* (Cth) s 4.
[8] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review* (Department of the Prime Minister and Cabinet, 2017) 116.
[9] Ibid.
[10] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review* (Department of the Prime Minister and Cabinet, 2017) 116.

The government's concerns about the proposed changes creating overlap and duplication are also overstated. The government submission is correct in pointing out that other integrity bodies – including the IGADF and Commonwealth Ombudsman – oversee the agencies to be added. However, these offices have different statutory functions and powers to the IGIS. The functions of the Commonwealth Ombudsman, for example, are to investigate complaints relating to administration of federal agencies.[11] The functions of the IGADF include inquiring into matters concerning the military justice system and promoting military justice values across the Defence Force.[12] The functions of the IGIS, by contrast, are to investigate the propriety of intelligence activities, whether intelligence activities comply with laws and regulations, and whether intelligence activities are contrary to human rights or constitute discrimination.[13] The IGIS also has extensive inquiry powers that are not available to other statutory offices. The Commonwealth Ombudsman can compel the production of information and documents, but the Attorney-General can issue a certificate preventing disclosure for national security reasons.[14] By contrast, no similar process applies in IGIS inquiries,[15] meaning the level of access to classified information granted to that office is secured to a higher degree.

As the purpose of the proposed changes is to enhance oversight of intelligence activities, these specific inquiry functions and powers of the IGIS – beyond those currently available to other integrity bodies – are essential. To the extent that any overlap across different inquiries may occur, the legislation already deals with this possibility by requiring the IGIS to consult with the Auditor-General and Ombudsman to avoid duplication.[16] The Bill could provide additional clarity by extending this obligation to other integrity bodies, but the statutory functions of these agencies remain sufficiently distinct to justify additional IGIS oversight.

---

[11] *Ombudsman Act 1976* (Cth) s 5.
[12] *Defence Act 1903* (Cth) s 110C.
[13] *Inspector-General of Intelligence and Security Act 1986* (Cth) s 8.
[14] *Ombudsman Act 1976* (Cth) s 9.
[15] *Inspector-General of Intelligence and Security Act 1986* (Cth) s 18.
[16] *Inspector-General of Intelligence and Security Act 1986* (Cth) s 16.

Finally, in light of the additional responsibilities to be taken on by IGIS, we would support the Independent Review's recommendation to allocate additional resources to that office.[17]

Yours sincerely,

Dr Keiran Hardy and Professor George Williams

[17] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review* (Department of the Prime Minister and Cabinet, 2017) 118.

Global Intelligence Oversight

GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY

Edited by Zachary K. Goldman

and Samuel J. Rascoff

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide. Oxford is a registered trademark of Oxford University Press in the UK and certain other countries.

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America.

Library of Congress Cataloging in Publication Data

Names: Goldman, Zachary K., editor. | Rascoff, Samuel James, editor.
Title: Global intelligence oversight : governing security in the twenty-first century / Edited by Zachary K. Goldman and Samuel J. Rascoff.
Description: New York : Oxford University Press, 2016. | Includes bibliographical references and index.
Identifiers: LCCN 2015051038 | ISBN 9780190458072 ((hardback) : alk. paper)
Subjects: LCSH: Intelligence service—Law and legislation. | National security—Law and legislation. | Internal security. | Legislative oversight.
Classification: LCC K3278 .G56 2016 | DDC 343/.01—dc23 LC record available at http://lccn.loc.gov/2015051038

9 8 7 6 5 4 3 2 1

Printed by Edwards Brothers Malloy, United States of America

Note to Readers

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is based upon sources believed to be accurate and reliable and is intended to be current as of the time it was written. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. Also, to confirm that the information has not been affected or changed by recent developments, traditional legal research techniques should be used, including checking primary sources where appropriate.

(Based on the Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.)

Contents

12

Executive Oversight of Intelligence Agencies in Australia

Keiran Hardy and George Williams***

I. INTRODUCTION

When it comes to government accountability, intelligence agencies present a special case. Ordinarily, government departments are subject to robust scrutiny from a variety of sources. The media constantly inspects, evaluates, and critiques the conduct of government and its policies. This fuels further discussion by the general public through print, radio, and social media. Courts assess whether government officials have used their statutory powers in accordance with the law and whether the legislation that provides those powers is constitutional. Parliament examines the expenditure, administration, and operation of government agencies through estimates hearings and committee inquiries and by inspecting their annual reports. Tribunals assess whether government officials made their decisions correctly,[1] and ombudsmen investigate whether those decisions were unjust, oppressive, or discriminatory.[2] This combination of public, judicial, legislative, and executive scrutiny is a comprehensive system for maintaining the accountability of government.

Many of these avenues are ineffective or problematic when applied to intelligence agencies due to the inherent secrecy of their work. The classification of national security information and exemptions from freedom of information (FOI) legislation mean that media and public

* Lecturer, School of Criminology and Criminal Justice, Griffith University.

** Anthony Mason Professor, Scientia Professor and Foundation Director, Gilbert + Tobin Centre of Public Law, Faculty of Law, University of New South Wales; Australian Research Council Laureate Fellow; Barrister, New South Wales Bar.

[1] *Drake v. Minister for Immigration and Ethnic Affairs* (1979) 24 ALR 577, 591.

[2] *Ombudsman Act 1976* (Cth) § 15(1)(a)(ii).

scrutiny of intelligence agencies can be superficial at best.[3] Indeed, some laws are specifically designed to outlaw public discussion of intelligence operations. For example, in October 2014, the conservative Liberal-National Coalition government led by Australian prime minister Tony Abbott enacted a Special Intelligence Operations (SIO) regime.[4] This regime grants officers of the Australian Security Intelligence Organisation (ASIO) immunity for unlawful acts done in the course of specially approved undercover operations.[5] Attached to this regime is a criminal offense punishable by five years imprisonment that applies to anyone who discloses information relating to an SIO.[6] This offense prohibits any public discussion of SIOs—even if, for example, a journalist revealed that ASIO officers had mishandled an operation, caused death or serious injury to a suspect, or been involved in an illegal activity.

The possibilities for holding intelligence agencies accountable in the courts are also limited. Judges may defer to the executive branch when a case involves national security concerns,[7] and the use of secret evidence can make it difficult for individuals to challenge the conduct of intelligence officers or decisions by intelligence officials.[8] In Australia, the possibilities for judicial review are further limited because intelligence agencies are exempt from the Administrative Decisions (Judicial Review) Act 1977 (Cth), which provides for statutory judicial review of administrative action.[9] Australia also lacks a national, judicially enforceable Bill of Rights, which further limits opportunities for individuals to challenge the lawfulness of statutory powers granted to intelligence agencies. Individuals cannot, for example, challenge such legislation on the grounds that it infringes a general right to freedom of speech or association. To give rise to constitutional concerns, the legislation must, for example, infringe the separation of powers or one of a few implied rights in the Australian Constitution.[10] No such constitutional limits have ever proven to be of use in challenging the statutory powers of Australian intelligence agencies.

---

[3] *Freedom of Information Act 1982* sch 3.

[4] *Australian Security Intelligence Organisation Act 1979* (Cth) pt III div 4, which was enacted pursuant to *National Security Legislation Amendment Act (No. 1) 2014* (Cth) sch 3.

[5] *Australian Security Intelligence Organisation Act 1979* (Cth) § 35K.

[6] *Id.* § 35P.

[7] *See generally*, Ashley S. Deeks, *The Observer Effect: National Security Litigation, Executive Policy Changes, and Judicial Deference*, 82 Fordham L. Rev. 827 (2013); Robert M. Chesney, *National Security Fact Deference,* 95 Va. L. Rev. 1361 (2009); Kim Lane Scheppele, *The New Judicial Deference*, 92 B.U. L. Rev 89 (2012). In Australia, judicial deference to the executive branch is particularly apparent when policy or administrative decisions combine immigration and national security concerns. *See* Brian Galligan & Emma Larking, School of Political Sciences, Criminology & Sociology, The University of Melbourne, Paper presented at Australasian Political Science Association Conference, University of Queensland: *The Separation of Judicial and Executive Powers in Australia: Detention Decisions and the Haneef Case* (July 9, 2008), at 15–16. For example, in *Leghaei v. Director-General of Security* [2005] FCA 1576, the Federal Court held (at ¶ 88) that procedural fairness requirements applied to adverse security assessments issued by ASIO, but due to national security considerations these requirements were, in practical terms, reduced to "nothingness." On ASIO's power to issue adverse security assessments, see discussion below in Section III(B).

[8] *See, e.g.*, Nicola McGarrity & Edward Santow, "Anti-Terrorism Laws; Balancing National Security and a Fair Hearing" *in* Global Anti-Terrorism Law and Policy (Victor V Ramraj et al. eds., 2d ed, 2012); Keiran Hardy, *ASIO, Adverse Security Assessments and a Denial of Procedural Fairness*, 17 Austl. J. Admin. L. 39, 44–45 (2009); Rebecca Scott Bray & Greg Martin, *Closing Down Open Justice in the United Kingdom,* 37 Alternative L.J. 126 (2012).

[9] *Administrative Decisions (Judicial Review) Act 1977* (Cth) sch 1 § 3 item 3.

[10] For example, the Australian High Court has read into the Constitution an implied freedom of political communication and an implied right to vote. *Lange v. Australian Broadcasting Corporation* (1997) 189 CLR 520;

Parliamentary scrutiny of intelligence agencies is also limited. Only one of the six intelligence agencies in Australia is required to produce an annual report to Parliament,[11] and any operationally sensitive parts of that report are redacted.[12] Even if the intelligence agencies were required to provide more information to Parliament, parliamentarians do not typically have the knowledge and experience required to assess the appropriateness of intelligence-gathering priorities or operations.[13]

Specialized parliamentary committees are playing an increasingly important role to fill this gap,[14] but their effectiveness can also be limited due to political interests, tightly defined statutory powers, and the protection of classified information. Australia's Parliamentary Joint Committee on Intelligence and Security (PJCIS) examines new counterterrorism laws introduced by the government,[15] but is required to have a majority of government members,[16] and so its findings usually align with the political and policy priorities of the government of the day. As a result, the Committee may not recommend substantive changes to otherwise extraordinary counterterrorism measures.[17] The PJCIS also reviews the expenditure and administration of Australia's six intelligence agencies,[18] but it is not permitted to review intelligence-gathering priorities or operations, and it has no power to launch inquiries of its own choosing.[19] Much of the Committee's work is also conducted behind closed

---

Roach v Electoral Commission (2007) 233 CLR 162. *See generally* David Hume & George Williams, Human Rights under the Australian Constitution (2d ed. 2013).

[11] *Australian Security Intelligence Organisation Act 1979* (Cth) § 94. The Director-General of the Australian Secret Intelligence Service is also required to produce an annual report, but this is given only to the Minister for Foreign Affairs, and is not required to be submitted to Parliament. *Intelligence Services Act 2001* (Cth) § 42.

[12] *Australian Security Intelligence Organisation Act 1979* (Cth) § 94(5).

[13] Hugh Bochel et al., Watching the Watchers: Parliament and the Intelligence Services 5–6 (2014).

[14] *See id*. at 75–102; Andrew Defty, *Educating Parliamentarians about Intelligence: The Role of the British Intelligence and Security Committee*, 61(4) Parliamentary Affairs 621 (2008); Peter Gill, *Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the "War on Terror,"* 22(1) Intelligence & Nat'l Security 14 (2007); Jennifer Kibbe, *Congressional Oversight of Intelligence: Is the Solution Part of the Problem?*, 25(1) Intelligence & Nat'l Security 24 (2010).

[15] *See. e.g.*, Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014 (2014) [hereinafter PJCIS Report]; Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014 (2014).

[16] *Intelligence Services Act 2001* (Cth) § 28(3).

[17] For example, in September 2014 the Abbott government introduced a range of controversial new measures in response to the threat of foreign fighters returning from Syria and Iraq. These new laws included an offense punishable by 10 years imprisonment for entering or remaining in a "declared area." An area of a foreign country may be designated as a "declared area" where the Minister for Foreign Affairs is satisfied that a terrorist organization is engaged in hostile activity in that area. The person need only travel to the area, and need not have any malicious intent. The PJCIS recommended some improvements to the legislation, such as removing the power to declare a whole country as a "declared area" and providing for Committee oversight of the minister's declarations, but it recommended no substantive changes to this otherwise extraordinary offense. *See Criminal Code Act 1995* (Cth) § 119.2; PJCIS Report, *supra* note 15, at 103–08.

[18] *Intelligence Services Act 2001* (Cth) § 29(1)(a).

[19] *Id.* at § 29(3). Inquiries must be referred to the PJCIS either by the responsible minister or by a resolution of either House of Parliament: *Intelligence Services Act 2001* (Cth) § 29(1)(b). The Committee may, by resolution,

doors, as it frequently relies on classified submissions, and its reports may be redacted by the responsible minister on the advice of the intelligence agencies.[20] This means that the public must often trust that the PJCIS is using its limited powers to hold the intelligence agencies to account, rather than knowing this to be the case.

The fact that public, judicial, and parliamentary scrutiny of Australia's intelligence agencies is severely constrained means that the executive branch takes on a particularly important role in holding these agencies to account. Specially appointed office holders and inquiries are trusted, where others are not, to access classified information and assess the appropriateness of intelligence agencies' powers and operations. This is not to suggest that the other mechanisms considered above are not also important or complementary, where they are available. However, it is clear that these other mechanisms are less robust and effective when applied to intelligence agencies as compared to other aspects of government.

The key conceptual and practical problem with executive oversight of intelligence agencies is that the relevant accountability mechanisms—including statutory officeholders, royal commissions, and administrative tribunals—are part of the same arm of government to which the intelligence agencies belong. This undermines the notion of "horizontal" accountability, being that the different arms of government—legislature, judiciary, executive—should keep each other in check.[21] There is an increasing amount of scholarship on executive oversight mechanisms as an "integrity branch" of government,[22] but these integrity mechanisms are not yet sufficiently independent from the rest of government to compare their accountability function to the traditional separation of powers.

Executive oversight mechanisms therefore play an important but also potentially problematic role in keeping intelligence agencies accountable. Given this, the aim of this chapter is to assess whether executive oversight of the Australian intelligence agencies is robust, stringent, and effective. It considers whether there are any gaps or vulnerabilities in this system of executive accountability, and whether stronger powers or other improvements are needed to further counterbalance the limited public, judicial, and parliamentary scrutiny of intelligence agencies.

In Section II, we set out the six Australian intelligence agencies and their functions. In Section III, we set out the executive bodies that oversee those agencies, including their responsible ministers, the Inspector-General of Intelligence and Security, the Independent National Security Legislation Monitor, and other various forms of oversight and inquiry. We categorize these mechanisms according to the function they perform (such as authorizing the use of covert powers, or reviewing legislation) and explain their jurisdiction and investigative powers. In line with the other contributions to this collection,[23] we also consider a range of *governance* mechanisms: those that oversee the intelligence agencies by developing intelligence policy and setting their collection priorities—rather than simply ensuring their compliance with the law.

---

ask the minister to refer something for its consideration, but a referral is not guaranteed. *See Intelligence Services Act 2001* (Cth) § 29(2).

[20] *Intelligence Services Act 2001* (Cth) sch 1 cl 7.

[21] Bochel et al., *supra* note 13, at 4.

[22] *See, e.g.*, Lisa Burton & George Williams, *The Integrity Function and ASIO's Extraordinary Questioning and Detention Powers*, 38(3) Monash U. L. Rev. 1 (2012).

[23] *See, e.g.*, the contributions of Zachary Goldman, Jane Harman, Jon Moran and Clive Walker, and Kent Roach to this volume.

In Section IV, we evaluate the strengths and weaknesses of this executive accountability system. To this end, we consider a range of important questions. Do executive oversight bodies sufficiently cover the activities and administration of Australia's intelligence agencies, or are there significant gaps in jurisdiction? Are the investigative powers of these bodies sufficiently strong to undertake robust inquiries? Do these bodies have appropriate powers to remedy instances of misconduct or wrongdoing? Have executive oversight mechanisms proved effective in keeping the Australian intelligence agencies accountable? The conclusion returns to these questions and draws some broader lessons about the role that the executive branch plays in holding secret intelligence organizations to account. In particular, our analysis suggests that executive accountability mechanisms are weak to the extent that they possess only recommendatory powers, and their effectiveness depends on whether the government of the day is willing to accept recommendations for change. Our analysis also suggests there are limits to what executive oversight can achieve when the government of the day grants intelligence agencies statutory powers of extraordinary reach. These conclusions emerge from the Australian experience, but they are also of more general application in identifying broader themes and concerns that relate to the operation of intelligence organizations in a range of nations.

II. AUSTRALIAN INTELLIGENCE AGENCIES

Australia has six intelligence agencies, which are collectively known as the Australian Intelligence Community (AIC). Two of these agencies are responsible for collecting intelligence from human sources (HUMINT): a foreign intelligence collection agency and a domestic security service, the latter being also responsible for intelligence assessment. There are three intelligence agencies situated within the Department of Defence, one of which is an assessment (as opposed to collection) agency. Finally, another assessment agency is responsible to the Prime Minister.

A. Human Intelligence

1. Australian Secret Intelligence Service

The Australian Secret Intelligence Service (ASIS) is Australia's foreign intelligence collection agency. Like the other foreign intelligence collection agencies set out below, ASIS is governed by the Intelligence Services Act 2001 (Cth) (ISA 2001). Its main functions under the ISA 2001 are "to obtain . . . intelligence about the capabilities, intentions or activities of people or organizations outside Australia,"[24] and to communicate that intelligence to government as required.[25] ASIS also conducts counterintelligence activities and provides assistance to the Australian Defence Force (ADF) in its overseas military operations.[26] In these respects, ASIS is the Australian equivalent of MI6, the British Secret Intelligence Service.[27]

[24] *Intelligence Services Act 2001* (Cth) § 6(1)(a).
[25] *Id.* § 6(1)(b).
[26] *Id.* § 6(1)(ba)–(c).
[27] *Intelligence Services Act 1994* (UK) c 13, § 1.

In contrast to the U.S. Central Intelligence Agency (CIA), ASIS officers are not permitted to undertake paramilitary activities, nor to proactively engage in the use of violence.[28] Like all the other Australian intelligence agencies, ASIS is also prohibited from carrying out police functions (such as arresting and charging individuals for criminal offenses) or enforcing the law in any other way.[29] ASIS officers employed overseas are, however, trained in the use of some weapons—including handguns, batons, and capsicum spray—for the purposes of self-defense.[30]

2. Australian Security Intelligence Organisation

The Australian Security Intelligence Organisation is Australia's domestic security service. Its main role is to "gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's national security."[31] In the post-9/11 era, this means that much of ASIO's work involves collecting and assessing intelligence on potential terrorist threats within Australia's borders. In this respect, ASIO is the Australian equivalent of MI5, the British security service. ASIO also undertakes security assessments of foreign nationals applying for refugee status in Australia.[32]

ASIO is governed by the Australian Security Intelligence Organisation Act 1979 (Cth) (ASIO Act).[33] The organization's main function under the ASIO Act is to "obtain, correlate and evaluate intelligence relevant to security."[34] Under section 4 of the ASIO Act, "security" is defined broadly as the protection of the Australian government and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defense system, acts of foreign interference, and serious threats to border security.[35] Like ASIS, ASIO is not permitted to perform police functions such as arrest.[36] However, ASIO officers exercise a range of clandestine powers similar to those used by law enforcement, such as searching private premises and installing telephone intercept devices.[37]

B. Defense Intelligence Agencies

1. Australian Signals Directorate

The Australian Signals Directorate (ASD), formerly the Defence Signals Directorate (DSD), is Australia's signals intelligence agency. It is the equivalent of Britain's Government

---

[28] *Intelligence Services Act 2001* (Cth) § 6(4).

[29] *Id.* § 11(2). It may however communicate that intelligence to law enforcement where necessary. *See Intelligence Services Act 2001* (Cth) § 11(2)(c).

[30] *See id.* at sch 2.

[31] Australian Security Intelligence Organisation, *available at* http://www.asio.gov.au (last visited June 15, 2015).

[32] *Australian Security Intelligence Organisation Act 1979* (Cth) pt 4.

[33] Prior to this Act, the relevant legislation was the *Australian Security Intelligence Organisation Act 1956* (Cth).

[34] *Id.* § 17(1)(a).

[35] *Id.* § 4.

[36] *Id.* § 17(2).

[37] *See id.* at pts 2, 3.

Communication Headquarters (GCHQ) or the U.S. National Security Agency, although ASD is more specifically focused on military activities than its American and British counterparts. Like ASIS, ASD is governed by the ISA 2001. Under the ISA 2001, ASD's primary functions are to collect foreign signals intelligence and communicate that intelligence to the Australian government and the ADF in support of its military operations.[38] ASD also plays an important role in information and cyber security—such as advising government departments how to protect their computer networks, coordinating responses to cyber attacks, and providing services in codebreaking and encryption.[39]

2. Australian Geospatial-Intelligence Organisation

The Australian Geospatial-Intelligence Organisation (AGO) is Australia's geospatial intelligence agency. Geospatial intelligence is intelligence gained from imagery and geospatial data—such as topographical maps and images from aircraft and satellites. Like ASIS and ASD, AGO is a foreign intelligence collection agency governed by the ISA 2001; its main function is to collection intelligence "about the capabilities, intentions or activities of people or organisations outside Australia."[40] AGO communicates that intelligence to the Australian government and the ADF, and assists Commonwealth and state bodies in responding to security threats and natural disasters.[41]

3. Defence Intelligence Organisation

The Defence Intelligence Organisation (DIO) is a strategic, all-source assessment agency. This means that DIO does not collect intelligence, but rather relies on intelligence collected by the foreign collection agencies (i.e., ASIS, ASD, and AGO), as well as open source material such as media and policy documents, to produce strategic policy advice to the Australian government and the ADF. DIO assessments are used to support ADF operations as well as government planning on defense and national security issues.[42] For example, an assessment produced by DIO might include information about the military capabilities, weapons systems, and cyber-warfare capabilities of countries relevant to Australia's security environment.[43] Whereas the functions of ASIS, ASD, and AGO are each set out in the ISA 2001,[44] DIO has no explicit statutory function.[45]

---

[38] *Intelligence Services Act 2001* (Cth) § 7.

[39] *See* Australian Signals Directorate, Information Security, *available at* http://www.asd.gov.au/infosec/index.htm (last visited July 9, 2015).

[40] *Intelligence Services Act 2001* (Cth) § 6B(a).

[41] *Id.* §§ 6B(d), (e)(iii).

[42] Defence Intelligence Organisation, About Us, *available at* http://www.defence.gov.au/dio/about-us.shtml (last visited July 9, 2015).

[43] *Id*.

[44] *Intelligence Services Act 2001* (Cth) §§ 6, 6B, 7.

[45] *See* Australian Government, The Australian Intelligence Community: Agencies, Functions, Accountability and Oversight 5 (2006). However, the ISA 2001 does include some relevant provisions, including offenses where a DIO employee discloses or unlawfully records classified information. *Intelligence Services Act 2001* (Cth), §§ 40B, 40M.

C. Intelligence Assessment

1. Office of National Assessments

The Office of National Assessments (ONA) is an all-source assessment agency that produces reports for the prime minister and the Australian government on international matters of political, strategic, and economic importance.[46] Like DIO, ONA relies on intelligence collected by the other intelligence agencies and open source material, as well as information from other government departments. ONA also helps to coordinate and evaluate Australia's foreign intelligence activities, such as by providing advice to the government as to whether the intelligence agencies have sufficient resources.[47] ONA is an independent body established under section 4(1) of the Office of National Assessments Act 1977 (Cth).

III. EXECUTIVE OVERSIGHT

In this section, we set out the key executive bodies that oversee Australia's six intelligence agencies. We categorize these bodies according to the function they perform, such as authorizing clandestine powers and reviewing intelligence operations. These oversight bodies supplement the role of the PJCIS, which reviews new counterterrorism laws and oversees the administration and expenditure of the intelligence agencies.[48] However, as explained in the introduction, the PJCIS has a tendency to align with government policy, and its statutory powers are tightly defined.[49] Many of the mechanisms outlined below have a wider remit, such as by being able to launch their own inquiries and review intelligence operations.

A. Ministerial Authorization of Powers

Each of Australia's intelligence agencies is responsible to a cabinet minister in the federal government. ASIS is responsible to the Minister for Foreign Affairs, ASIO to the Attorney-General, the three defense intelligence agencies to the Minister for Defence, and ONA to the prime minister. Unlike in the United States, these senior members of the executive branch are required to sit in Parliament.[50] In theory, this means that the responsible ministers are accountable via Parliament to the Australian people for any misconduct or maladministration by the intelligence agencies. This is one of the core characteristics of the system of responsible government adopted as part of the Westminster system by Australia, the U.K., and other like nations.

Responsible government in this case is undermined by the inherent secrecy of intelligence operations. As explained above, only one of the six intelligence agencies (ASIO) is required to table an annual report in Parliament,[51] and any operationally sensitive information in that report is redacted.[52] This makes it virtually impossible to identify from the report whether

---

[46] *Office of National Assessments Act 1977* (Cth) § 5(1)(a).
[47] *Id.* § 5(1B)(b).
[48] *Intelligence Services Act 2001* (Cth) § 29.
[49] *Id.*
[50] Australian Constitution § 64.
[51] *Australian Security Intelligence Organisation Act 1979* (Cth) § 94.
[52] *Id.* § 94(5).

ASIO has misused its powers, or to make that determination unless such information is forthcoming from other sources.[53]

The more significant accountability function performed by the responsible ministers is to authorize the use of clandestine powers by intelligence officers. For example, the Director-General of Security (the head of ASIO) may request the Attorney-General to issue a warrant allowing ASIO officers to search private premises.[54] The Attorney-General may do so where he or she is satisfied on reasonable grounds that ASIO officers accessing records or things on those premises would "substantially assist the collection of intelligence . . . that is important in relation to security."[55] Similar examples include ministerial warrants that allow ASIO officers to intercept telephone calls, install surveillance devices, inspect postal articles, and access data held on computers.[56]

Ministerial authorization is also required before the foreign intelligence collection agencies are able to collect any intelligence on Australian citizens.[57] These agencies are prohibited from collecting intelligence on Australian citizens unless the relevant minister is satisfied that the person is likely to be involved in one of a range of serious activities—including those that pose a significant risk to safety, are likely to be a threat to security, or are related to the proliferation of weapons of mass destruction.[58] These ministerial authorizations may also be issued in relation to a "class of Australian persons" where one of the intelligence agencies is assisting the ADF in its overseas military operations.[59] What constitutes a "class of Australian persons" is not defined or otherwise set out in the Act.

Stronger protections apply to ASIO's questioning and detention warrants.[60] These are one of the most controversial counterterrorism powers available to ASIO. They allow, pursuant to a warrant, any person to be questioned for up to 24 hours, and detained for up to one week for that purpose, without being suspected of any involvement in terrorism.[61] A person must

---

[53] For example, ASIO's most recent annual report includes the findings of the Independent Reviewer of Adverse Security Assessments, who concluded that one adverse security assessment issued by ASIO was not appropriate, and that ASIO had updated that assessment as a result. *See* Australian Security Intelligence Organisation, ASIO Report to Parliament: 2013–2014, at 48 (2014) [hereinafter ASIO Annual Report 2014].

[54] *Australian Security Intelligence Organisation Act 1979* (Cth) § 25(1).

[55] *Id.* § 25(2).

[56] *Id.* §§ 25A, 26, 27; *Telecommunications (Interception and Access) Act 1979* (Cth) § 9.

[57] By contrast, ASIO is charged with collecting and analyzing intelligence relevant to "security," which is defined as a range of threats to Australia's national interests, including espionage, sabotage, and politically motivated violence. *See Australian Security Intelligence Organisation Act 1979* (Cth) §§ 4, 17. This ensures a division of responsibilities, similar to that between the FBI and CIA, by which ASIO is responsible for collecting intelligence on Australian citizens and foreign nationals within Australia's borders, and the foreign collection agencies are responsible for collecting intelligence overseas, including intelligence on Australian citizens. The agencies can, however, cooperate in the performance of their functions, provided that they do so subject to any arrangements or directions by the responsible minister. *See Australian Security Intelligence Organisation Act 1979* (Cth) §§ 17(1)(f), 19A; *Intelligence Services Act 2001* (Cth) § 13A.

[58] *Intelligence Services Act 2001* (Cth) § 9(1A).

[59] *Id.* § 8(1)(a)(ia)–(ib).

[60] *Australian Security Intelligence Organisation Act 1979* (Cth) pt 3 div 3.

[61] *Id.* §§ 34G, 34R, 34S.

answer a question put to him or her by ASIO, or face imprisonment for up to five years.[62] To apply for one of these warrants, the Director-General of Security must first obtain the Attorney-General's consent to apply to an "issuing authority" (who must be a serving judge, and has the same protection and immunity as a Justice of the High Court of Australia).[63] The Attorney-General may grant consent only where he or she is satisfied about a range of conditions, including that the warrant would substantially assist in the collection of intelligence and that other means of collecting the intelligence would be ineffective.[64] The issuing authority provides an added layer of executive oversight,[65] and is permitted to issue the warrant only if he or she agrees that the person's detention would substantially assist in the collection of intelligence that is relevant to security.[66] The Director-General of Security must also provide details on the use of questioning and detention warrants in ASIO's annual report, including the number of requests made, the number of warrants issued, and the number of hours each person spent under questioning and in detention.[67]

B. Review of Operations

When an intelligence agency seeks to rely upon special powers such as clandestine searches and surveillance, it is important not only that those powers are independently authorized before their use, but that they are also subject to rigorous post-hoc review to assess whether they have been misused or used unlawfully. In Australia, primary responsibility for this lies with the Inspector-General of Intelligence and Security (IGIS), an independent statutory office established by the Inspector-General of Intelligence and Security Act 1986 (Cth). The office was created in response to concerns that Australia's intelligence agencies "were not sufficiently under ministerial control, nor subject to enough scrutiny."[68] The position is currently held by Dr. Vivienne Thom, a former Deputy Ombudsman.

The IGIS supervises the six intelligence agencies by assessing whether they have acted in accordance with laws, directions, and guidelines, and whether their activities are consistent with human rights.[69] The IGIS also assesses the "propriety" of their activities, although the precise meaning of this term remains unclear.[70] To assess the intelligence agencies' activities against these criteria, the IGIS conducts two forms of review: inquiries and formal inspections.[71] Inspections involve regular scrutiny of intelligence agencies' records and oversight of

[62] *Id.* § 34L(2).

[63] *Id.* §§ 34AB, 34F, 34ZM.

[64] *Id.* § 34F(4).

[65] In Australia, judges can perform executive or administrative functions such as issuing warrants if Parliament confers a function on the judge in his or her personal capacity, the judge consents to performing that function, and the function is not incompatible with the holding of judicial office. *See Hilton v. Wells* (1985) 157 CLR 57; *Grollo v. Palmer* (1995) 184 CLR 348; *Wilson and Ors v. Minister for Aboriginal and Torres Strait Islander Affairs and Anor* (1996) 189 CLR 1.

[66] *Australian Security Intelligence Organisation Act 1979* (Cth) § 34G(1)(b).

[67] *Id.* § 94(1).

[68] Vivienne Thom, Inspector-General of Intelligence and Security, Speech at the Supreme and Federal Court Judges' Conference: Address to Supreme and Federal Court Judges' Conference (Jan. 26, 2009), at 2.

[69] *Inspector-General of Intelligence and Security Act 1986* (Cth) §§ 8(1)(a)(i)–(ii), (v).

[70] *Id.* § 8(1)(a)(iii). *See* Burton & Williams, *supra* note 22, at 12.

[71] *Inspector-General of Intelligence and Security Act 1986* (Cth) §§ 8, 9A.

some statutory powers.[72] For example, when the head of ASIO requests a questioning and detention warrant, the IGIS must be informed and may be present during the questioning or enter any place of detention.[73]

The IGIS has conducted several inquiries into alleged misconduct by the Australian intelligence agencies, including one relating to the detention and torture overseas of Mamdouh Habib, a dual Australian-Egyptian citizen.[74] These inquiries may be conducted at the request of a responsible minister, at the request of the prime minister, after a complaint to the IGIS, or on the IGIS's own motion.[75] To conduct these inquiries, the IGIS is bestowed with strong investigative powers akin to those held by royal commissions—including powers to summon witnesses, compel documents, and enter the intelligence agencies' premises at any reasonable time.[76]

The IGIS also conducts an inquiry if an intelligence employee seeks protection for disclosing information under the Public Interest Disclosure Act 2013 (Cth) (PID Act).[77] The PID Act is a new federal whistle-blower scheme; it provides immunity from civil, criminal, and administrative liability for public officials who according to a specified procedure disclose wrongdoing by government departments.[78] Generally, the opportunities for intelligence officers to seek protection under the scheme are very limited.[79] However, they may disclose information to the IGIS where they believe on reasonable grounds that it would be appropriate for one or more instances of misconduct to be investigated by the office.[80]

The other major post-hoc review of ASIO's activities is undertaken by the Security Appeals Division of the Administrative Appeals Tribunal (AAT). Merits review of decisions by intelligence agencies is generally prohibited, although the Security Appeals Division has jurisdiction to review adverse security assessments issued by ASIO.[81] An adverse security assessment is a security assessment made by ASIO that recommends that certain administrative action

---

[72] *Id*. § 9A. *See* Thom, *supra* note 68, at 1–2.

[73] *Australian Security Intelligence Organisation Act 1979* (Cth) §§ 34ZI, 34P, 34Q; *Inspector-General of Intelligence and Security Act 1986* (Cth) §§ 9B, 19A. Most recently, the inspection functions of the IGIS were expanded to include oversight of ASIO's Special Intelligence Operations (SIO) regime: *Australian Security Intelligence Organisation Act 1979* (Cth) s 35PA.

[74] Inspector-General of Intelligence and Security, Inquiry into the Actions of Australian Government Agencies in relation to the Arrest and Detention Overseas of Mr Mamdouh Habib from 2001 to 2005 (2011). Habib was suspected of having prior knowledge of the September 11 attacks; he was arrested in Pakistan, then sent to Egypt under the CIA's rendition program, and then detained as an enemy combatant for approximately three years in Guantanamo Bay.

[75] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 8.

[76] In line with royal commission powers, the IGIS can compel a person to answer a question or produce a document that would incriminate him- or herself. *See Inspector-General of Intelligence and Security Act 1986* (Cth) § 18(6). However, the information or document cannot be used in evidence except in a prosecution for refusing to provide information or documents to the IGIS, or for providing false or misleading information: *id*.

[77] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 8A.

[78] *Public Interest Disclosure Act 2013* (Cth) §§ 10(1), 26.

[79] Due to exemptions for intelligence information. *Public Interest Disclosure Act 2013* (Cth) §§ 26(1)(c). *See* Keiran Hardy & George Williams, *Terrorist, Traitor or Whistleblower? Offences and Protections in Australia for Disclosing National Security Information*, 37(2) U. New South Wales L.J. 784, 814–15 (2014).

[80] *See id.* at 814; *Public Interest Disclosure Act 2013* (Cth) § 34(1).

[81] *Australian Security Intelligence Organisation Act 1979* (Cth) § 54.

be taken against the interests of an individual (such as cancelling a passport or denying employment at an airport).[82] Australian citizens can apply to the Security Appeals Division to have these decisions reviewed on their merits.[83]

A significant number of adverse security assessments are issued in relation to noncitizens applying for refugee status in Australia.[84] A noncitizen who is denied refugee status due to an adverse security assessment cannot seek merits review of that decision in the AAT.[85] However, the person can apply to the Independent Reviewer of Adverse Security Assessments (Independent Reviewer of ASAs), an office that was established in December 2012 and extended in 2014 for a further two-year term.[86] The Independent Reviewer of ASAs conducts independent advisory reviews and 12-month periodic reviews of adverse security assessments issued in relation to noncitizens seeking refugee status.[87] The position is currently held by the Honorable Margaret Stone, a former federal court judge.

Occasionally, review of the intelligence agencies' activities is conducted by royal commissions and other ad hoc inquiries. Early in ASIO's history, the Menzies government appointed a royal commission into Soviet espionage in Australia after a KGB agent posing as a senior member of the Soviet Embassy defected.[88] Two further royal commissions in the 1970s and 1980s, led by New South Wales Supreme Court Judge Robert Hope, examined the structure, functions, and accountability of the intelligence agencies.[89] The Hope Royal Commissions resulted in significant changes to the administrative structure and accountability mechanisms applying to Australia's intelligence agencies, including the division of intelligence-gathering functions between ASIO and the foreign collection agencies, the creation of ONA as an independent statutory agency, and the creation of the IGIS and PJCIS.[90]

---

[82] *Id.* § 35.

[83] *Id.* § 54.

[84] In 2013/14, ASIO issued 27,149 security assessments in relation to visa applications by noncitizens. *See ASIO Annual Report 2014, supra* note 53, at xiii.

[85] *Australian Security Intelligence Organisation Act 1979* (Cth) § 36.

[86] Attorney-General, Continuation of the Office of the Independent Reviewer of Adverse Security Assessments (Dec. 11, 2014), *available at* http://www.attorneygeneral.gov.au/Mediareleases/Pages/2014/FourthQuarter/11December2014-ContinuationoftheOfficeoftheIndependentReviewerofAdverseSecurityAssessments.aspx.

[87] Nicola Roxon, Independent Reviewer of Adverse Security Assessments: Independent Review Function—Terms of Reference (Oct. 16, 2012), *available at* http://www.cla.asn.au/Submissions/2012/Independent%20Reviewer%20for%20Adverse%20Security%20Assessments.pdf.

[88] *See* John Faulkner, *Surveillance, Intelligence and Accountability: An Australian Story*, Australian Fin. Rev., Oct. 24, 2014, at 21 (full essay *available at* http://www.afr.com/rw/2009-2014/AFR/2014/10/23/Photos/cad23366-5a65-11e4-a5ea-c145dc509150_Surveillance,%20Intelligence%20and%20Accountability%20by%20senator%20John%20Faulkner.pdf); Museum of Australian Democracy, *The Petrov Affair: Royal Commission, available at* http://moadoph.gov.au/exhibitions/online/petrov/royal-commission.html (last visited, Jan. 7, 2016)).

[89] *See* Faulkner, *supra* note 88, at 21–22.

[90] *See* Office of National Assessments, History of the Australian Intelligence Community (2010), *available at* http://www.ona.gov.au/history/australian-intelligence-community.html (last visited June 15, 2015). *See also* Faulkner, *supra* note 88, at 14–18. Although Justice Hope recommended against creating a parliamentary oversight committee, the Labor government nonetheless created the Parliamentary Joint Committee on the Australian Security Intelligence Organisation (later expanded into the PJCIS). Parliamentary Debates, House of Representatives, 22 May 1985 (Robert Hawke, Prime Minister) (Austl.), *available at*

More recent inquiries have investigated specific instances of wrongdoing. For example, in 2008, the then Attorney-General Robert McClelland appointed the Honorable John Clarke QC to report on the arrest and detention of Mohamed Haneef.[91] Haneef was an Indian doctor working in Australia who was mistakenly linked to the bombing attempt on Glasgow airport.

Ordinarily, the Commonwealth Ombudsman would play a key role in reviewing the administrative decisions of government departments,[92] but that office does not have jurisdiction over the intelligence agencies.[93] The Commonwealth Ombudsman does play a limited role in overseeing ASIO's questioning and detention warrant regime, as a person being detained must be informed of his or her right to make a complaint to the office.[94] However, such complaints may only be made in relation to the conduct of Australian Federal Police (AFP) officers in taking the person into custody.[95]

C. Law Reform

In addition to the authorization and post-hoc review of intelligence agencies' powers, it is important to assess whether the legislation that provides those powers is appropriate and does not unduly infringe rights. In Australia, the key executive body responsible for this is the Independent National Security Legislation Monitor (INSLM).[96] Although many individuals and organizations contribute to law reform debates, such as by making submissions to parliamentary inquiries, the INSLM plays a unique role as the office has access to classified information and strong investigative powers.

The INSLM is an independent statutory office, which is loosely modeled on the U.K.'s Independent Reviewer of Terrorism Legislation.[97] The position was held from 2011 to 2014 by Bret Walker SC, a prominent Sydney barrister. After Walker had completed his three-year term, the Abbott government introduced legislation to abolish the office,[98] but then decided against this and appointed former judge Roger Gyles AO QC to the position.[99] In March 2015, the new INSLM began an inquiry into section 35P of the ASIO Act, mentioned in the introduction, which prohibits the disclosure of any information relating to specially approved undercover operations.[100]

---

http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=%28Dataset%3Aweblastweek,hansardr,noticer,webthisweek,dailyp,votes,journals,orderofbusiness,hansards,notices,websds%29%20ParliamentNumber%3A%2234%22%20Government_Phrase%3A%22yes%22%20Context_Phrase%3A%22ministerial%20statement%22%20Speaker_Phrase%3A%22mr%20hawke%22;rec=13.

[91] John Clarke QC, Report of the Clarke Inquiry into the Case of Dr Mohamed Haneef (2008).

[92] *Ombudsman Act 1976* (Cth) §§ 5, 15.

[93] *Ombudsman Regulations 1977* (Cth) sch 1 reg 4.

[94] *Australian Security Intelligence Organisation Act 1979* (Cth) §§ 34J, 34K.

[95] *Id*. § 34J(1)(e)(ii).

[96] *Independent National Security Legislation Monitor Act 2010* (Cth).

[97] *See* Independent Reviewer of Terrorism Legislation, The Reviewer's Role (2015), *available at* https://terrorismlegislationreviewer.independent.gov.uk/about-me/ (last visited July 9, 2015).

[98] *Independent National Security Legislation Monitor Repeal Bill 2014* (Cth).

[99] Prime Minister of Australia, Appointment of Independent National Security Legislation Monitor (Dec. 7, 2014), *available at* https://www.pm.gov.au/media/2014-12-07/appointment-independent-national-security-legislation-monitor (last visited July 9, 2015).

[100] *Australian Security Intelligence Organisation Act 1979* (Cth), § 35P. *See* Department of the Prime Minister and Cabinet, Independent National Security Legislation Monitor (2015),

The INSLM has two main functions. The first is to review the operation and effectiveness of Australia's counterterrorism laws.[101] The second is to assess whether Australia's counterterrorism laws remain proportionate and necessary, and contain appropriate safeguards to protect the rights of individuals.[102] These reviews can be undertaken on the INSLM's own motion or a matter may be referred to the INSLM by the prime minister or the PJCIS.[103] To conduct these reviews, the INSLM has strong investigative powers similar to those of the IGIS and royal commissions—including the power to hold hearings, summon witnesses, and compel documents.[104]

Ad hoc and statutory inquiries also play an important role in reviewing and reporting on the legislation that grants intelligence agencies their powers. The Security Legislation Review Committee (Sheller Committee), for example, was established in accordance with section 4 of the Security Legislation Amendment (Terrorism) Act 2002 (Cth) (SLAT Act).[105] Its members included the IGIS, the Commonwealth Ombudsman, and the Human Rights and Privacy Commissioners. In 2006, the Sheller Committee published a detailed report on the operation and effectiveness of Australia's counterterrorism laws, including their impact on human rights and Muslim communities.[106]

Beginning in August 2012, another comprehensive review of Australia's counterterrorism laws was undertaken by the Council of Australian Governments Review of Counter-Terrorism Legislation (COAG Review).[107] The COAG Review received a wide range of submissions from individuals and organizations, and it held public hearings in major cities around Australia.[108] It had a similar mandate to the INSLM in that its role was to assess the operation and effectiveness of Australia's counterterrorism laws and whether those laws contained appropriate safeguards.[109]

A more limited ongoing role is played by the Australian Law Reform Commission (ALRC). The ALRC is an independent statutory body established under section 5 of the Australian Law Reform Commission Act 1996 (Cth). It reviews Commonwealth (federal) laws for the purpose of "removing defects" in those laws and "providing improved access to justice."[110] It has conducted some important reviews into Australia's counterterrorism and

---

available at http://www.dpmc.gov.au/pmc/about-pmc/core-priorities/independent-national-security-legislation-monitor (last visited July 9, 2015).

[101] *Independent National Security Legislation Monitor Act 2010* (Cth) § 6(1)(a).

[102] *Id.* § 6(1)(b).

[103] *Id.* §§ 6(1), 7, 7A.

[104] *See id.* pt 3. In contrast to the IGIS, the INSLM does not have the power to compel answers that would incriminate a person. *See Independent National Security Legislation Monitor Act 2010* (Cth) § 25(6). The INSLM may also conduct public hearings, whereas IGIS inquiries are conducted in private: *Independent National Security Legislation Monitor Act 2010* (Cth) § 21(1); *Inspector-General of Intelligence and Security Act 1986* (Cth) § 17(1).

[105] *Security Legislation Amendment (Terrorism) Act 2002* (Cth) § 4, as amended by the *Criminal Code Amendment (Terrorism) Act 2003* (Cth).

[106] Security Legislation Review Committee, Report of the Security Legislation Review Committee (2006) [hereinafter *Sheller Committee Report*].

[107] Australian Government, Council of Australian Governments Review of Counter-Terrorism Legislation (2013) [hereinafter COAG Review].

[108] *See id.* at 2–3.

[109] *See id.* at 3.

[110] *Australian Law Reform Commission Act 1996* (Cth) § 21.

national security legislation, including sedition offenses and secrecy laws.[111] However, these reports have covered only a limited range of topics as the ALRC cannot initiate investigations on its own; it can only inquire into matters that are referred by the Attorney-General.[112]

The role of the Australian Human Rights Commission (AHRC) is also limited in relation to national security matters. Ordinarily, the AHRC plays a key role in investigating breaches of human rights by government departments,[113] but its mandate does not extend to examining the conduct of the intelligence agencies.[114] Its role in this context is therefore limited to advocacy and law reform, such as contributing to PJCIS inquiries on counterterrorism laws.[115] Where the AHRC receives a complaint about the intelligence agencies, this must be referred to the IGIS for investigation.[116]

D. Review of Finances and Administration

One of the few accountability measures that applies equally to intelligence agencies as other government departments is the independent auditing of their finances and expenditure. The Commonwealth Auditor-General is an independent office that conducts annual performance and financial statement audits of all Commonwealth entities.[117] Agencies must submit financial reports to the office,[118] and the audits are conducted with the support of the Australian National Audit Office (ANAO).

Australia's intelligence agencies also have a range of internal mechanisms for ensuring compliance with financial obligations—including employee guidelines, training programs, and software to monitor compliance.[119] For example, ASIO has an Internal Audit directorate, and it has developed Fraud Management Guidelines that provide staff with specific guidance on the fraud control framework.[120] ASIO also conducts fraud awareness training for all new employees and contractors.[121]

E. Governance

A key theme across the chapters in this book is that intelligence agencies are subject not only to accountability mechanisms that ensure their compliance with the law, but also governance mechanisms that set their policy and intelligence collection priorities. In Australia,

---

[111] Australian Law Reform Commission, Fighting Words: A Review of Sedition Laws in Australia (2006); Australian Law Reform Commission, Secrecy Laws and Open Government in Australia (Report No. 112, 2009).

[112] *Australian Law Reform Commission Act 1996* (Cth) § 21(1).

[113] *Australian Human Rights Commission Act 1986* (Cth) § 11(1)(f).

[114] *Id.* § 11(3).

[115] *See, e.g.*, Australian Human Rights Commission, Submission No 7 to Parliamentary Joint Committee on Intelligence and Security: Inquiry into Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014, Oct. 2, 2014.

[116] *Australian Human Rights Commission Act 1986* (Cth) § 11(3).

[117] *Auditor-General Act 1997* (Cth) pt 4.

[118] *Public Governance, Performance and Accountability Act 2013* (Cth) § 42.

[119] *See* Faulkner, *supra* note 88, at 25.

[120] *ASIO Annual Report 2014*, *supra* note 53, at 56.

[121] *Id.*

a range of executive bodies perform this function. The key example is the National Security Committee of Cabinet (NSC), which comprises the prime minister and senior cabinet ministers (the Deputy Prime Minister, Attorney-General, Foreign Minister, Defence Minister, Immigration Minister, and Treasurer). The NSC is the "primary decision-making body on national security, including intelligence matters."[122] It sets the priorities of the intelligence agencies (generally once per year), and it supports the Attorney-General in coordinating responses to national security matters.[123] For example, when a gunman held 17 hostages in a central Sydney café in December 2014, the NSC was immediately convened to discuss responses to the crisis.[124]

The National Security Adviser (NSA), a position established by the Rudd government in 2008, supplements the NSC in developing national security policy and crisis responses.[125] In the event of a terrorist act, the NSA or Deputy NSA would chair the National Crisis Committee (NCC) to coordinate the exchange of information between the Commonwealth and state governments.[126] Formally, the Deputy NSA also co-chairs the National Counter-Terrorism Committee (NCTC), which includes senior representatives from the intelligence agencies and law enforcement, and further seeks to "coordinate an effective nation-wide counter-terrorism capability."[127] Reports from government insiders, however, suggest that the Abbott government has sidelined the NSA and Deputy NSA with a view to abolishing those offices.[128]

The Council of Australian Governments (COAG), Australia's peak intergovernmental forum, also helps to develop government policy and strategy on counterterrorism matters, particularly with regard to cooperation between the federal and state governments.[129]

Finally, the ministers responsible for the intelligence agencies govern the conduct of those agencies by developing and introducing new legislation that defines the scope of their powers,[130] and by making regulations under that legislation. For example, under section 8A of the ASIO Act, the Attorney-General is empowered to make guidelines to be observed by ASIO

---

[122] Australian Government, The Australian Intelligence Community, *supra* note 45, at 13–14. *See also* National Counter-Terrorism Committee, Plan 6 (3d ed. 2012) [hereinafter *National Counter-Terrorism Plan*].

[123] *See* Faulkner, *supra* note 88, at 23; *National Counter-Terrorism Plan, supra* note 122, at 6.

[124] *See* David Wroe & Lisa Cox, *Martin Place Siege: Tony Abbott Convenes National Security Committee*, Sydney Morning Herald (Dec. 15, 2014), *available at* http://www.smh.com.au/federal-politics/political-news/martin-place-siege-tony-abbott-convenes-national-security-committee-20141215-127brq.html.

[125] *National Counter-Terrorism Plan, supra* note 122, at 6.

[126] *Id.*

[127] *Id.* at 5.

[128] *See* Jason Koutsoukis, *Tony Abbott Dismantles Role of National Security Adviser by Stealth, Insiders Say*, Sydney Morning Herald (Oct. 25, 2013), *available at* http://www.smh.com.au/federal-politics/political-news/tony-abbott-dismantles-role-of-national-security-adviser-by-stealth-insiders-say-20131024-2w4do.html.

[129] *See, e.g.*, Australian Government, Council of Australian Governments' Communiqué, Special Meeting on Counter-Terrorism (Sept. 27, 2005), *available at* http://archive.coag.gov.au/coag_meeting_outcomes/2005-09-27/docs/coag270905.pdf.

[130] For example, Attorney-General George Brandis recently played the lead role in introducing legislation to expand ASIO's powers in response to the threat of returning foreign fighters. *See* Attorney-General, New Counter-Terrorism Measures for a Safer Australia (Aug. 5, 2014).

officers in the performance of their functions.[131] Those guidelines set out advice on a range of matters, such as how ASIO should collect and use personal information, and when it should investigate politically motivated violence.[132]

IV. IS EXECUTIVE OVERSIGHT OF INTELLIGENCE AGENCIES ROBUST AND EFFECTIVE?

In this section, we evaluate the strengths and weaknesses of the executive accountability measures outlined above. Do these accountability measures provide sufficient jurisdiction to cover the range of activities undertaken by Australia's intelligence agencies? Are their investigative powers sufficiently strong to allow robust inquiries to be undertaken? Do they have the capacity to allow instances of misconduct and wrongdoing to be remedied? Have they proved effective in keeping the intelligence agencies accountable? And what about vulnerabilities and weaknesses in the system? Below we answer these questions by identifying a range of themes, including the difficulties in holding governments to account with recommendatory powers, and in holding intelligence agencies accountable for the use of broadly defined statutory powers.

A. Strengths

The first thing that becomes apparent from the previous section is that a wide range of executive accountability measures are used to oversee Australia's six intelligence agencies. The intelligence agencies are each responsible to senior government ministers, who authorize the use of their clandestine powers. Their activities are subject to inspections and inquiries by the IGIS. ASIO's security assessments in regard to Australian citizens are subject to merits review by the Security Appeals Division of the AAT, and this process is supplemented by the Independent Reviewer of ASAs for assessments in regard to noncitizens. The INSLM reviews the legislation that provides intelligence agencies with their powers. The Auditor-General reviews each intelligence agency's resources and finances. Ad hoc and statutory inquiries supplement these forms of accountability, and advisory panels and senior ministers oversee intelligence policy and collection priorities.

The quantity and broad jurisdiction of these accountability measures is crucial given the difficulties posed by public, judicial, and parliamentary scrutiny of the intelligence agencies. These accountability measures allow oversight not only of the use of clandestine powers by the intelligence agencies, but also their finances, legislation, and policy direction. This lends support to the views of the previous IGIS, who believed that the intelligence agencies were subject to a "multi-faceted set of accountability arrangements," and that those arrangements should provide "considerable reassurance to the community that the day-to-day activities of the agencies are subject to substantial scrutiny."[133]

---

[131] *Australian Security Intelligence Organisation Act 1979* (Cth) § 8A.

[132] Australian Security Intelligence Organisation, The Attorney-General's Guidelines (2015) *available at* http://www.asio.gov.au/About-ASIO/Oversight-and-Accountability/Attorney-General-Guidelines.html.

[133] Ian Carnell, Accountable Intelligence Agencies: Not an Oxymoron. Address at the National Security and Counter-Terrorism Summit (Oct. 24, 2006), at 3, 6.

Another obvious strength of the system is that the independent officeholders possess strong investigative powers. Both the IGIS and the INSLM are empowered to compel witnesses for questioning,[134] to examine those witnesses on oath or affirmation,[135] and to compel the production of documents.[136] These powers are backed by the force of the criminal law, as it is an offense punishable by six months imprisonment to fail to comply with any of these demands.[137] The IGIS may also enter an intelligence agency's premises, or any place where a person is being detained by ASIO, at any reasonable time.[138] Importantly, the IGIS and INSLM, as well as the Auditor-General and Independent Reviewer of ASAs, all have access to classified information held by the intelligence agencies.[139] This puts the offices in a unique position to assess the appropriateness of intelligence agencies' powers and conduct and, where relevant, to uncover instances of misconduct and maladministration.

The independence of these officeholders is ensured by their statutory tenure and protection from liability. The IGIS is appointed for a period of five years, and the INSLM for a period of three years.[140] These appointments may only be terminated by reason of misbehaviour, or physical or mental incapacity,[141] which is equivalent to judicial tenure.[142] Both offices are protected from civil liability for any act or omission done in good faith in the performance of the office's functions or the exercise of its powers.[143]

The inquiries undertaken by the INSLM in particular have been detailed and rigorous. In his three years in office, Walker produced four reports, which examined a range of controversial powers held by the intelligence agencies and law enforcement.[144] He was highly

---

[134] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 18(3); *Independent National Security Legislation Monitor Act 2010* (Cth) § 22.

[135] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 18(4); *Independent National Security Legislation Monitor Act 2010* (Cth) § 23.

[136] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 18; *Independent National Security Legislation Monitor Act 2010* (Cth) § 24.

[137] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 18(7); *Independent National Security Legislation Monitor Act 2010* (Cth) § 25. It is also an offense to fail to attend a public hearing when served with a notice by the INSLM to do so. *See Independent National Security Legislation Monitor Act 2010* (Cth) § 25(2). Similar powers are held by the Auditor-General, although failure to comply with the orders of that office will amount to a fine and not a criminal offense. *See Auditor-General Act 1997* (Cth) § 32.

[138] *Inspector-General of Intelligence and Security Act 1986* (Cth) §§ 9B, 19, 19A. The Auditor-General also has a power to enter a government department's premises at any reasonable time. *See Auditor-General Act 1997* (Cth) § 33.

[139] *See Inspector-General of Intelligence and Security Act 1986* (Cth) § 20; *Independent National Security Legislation Monitor Act 2010* (Cth) § 28; *Auditor-General Act 1997* (Cth) § 26; Roxon, *supra* note 87.

[140] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 26; *Independent National Security Legislation Monitor Act 2010* (Cth) § 12. The Auditor-General is appointed for a period of 10 years. *See Auditor-General Act 1997* (Cth) sch 1 item 1(1).

[141] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 30; *Independent National Security Legislation Monitor Act 2010* (Cth) § 19.

[142] *Australian Constitution* § 72(ii).

[143] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 33; *Independent National Security Legislation Monitor Act 2010* (Cth) § 31.

[144] Bret Walker SC, Annual Report: 16 December 2011 (2012) [hereinafter *INSLM 2011 Report*]; Bret Walker SC, Declassified Annual Report: 20th December 2012 (2013) [hereinafter *INSLM 2012*

critical of some of these laws,[145] but supportive of others,[146] which suggests that he was sufficiently independent from government and adopted a fair and balanced approach rather than simply criticizing the government or echoing its policies. On this basis Walker has been praised in comparison to Lord Carlile, the U.K.'s former Independent Reviewer of Terrorism Legislation, as Carlile repeatedly advocated the U.K. government's position and failed to recommend changes to problematic laws.[147] This distinction was partly the result of how the two offices were designed, as the INSLM is tasked with assessing both the operation of the laws and whether they include sufficient protections for rights, whereas the U.K.'s Independent Reviewer only assesses the operation of the laws.[148]

Other inquiries into Australia's counterterrorism laws, including those by the Sheller Committee and the COAG Review,[149] have been conducted in a similarly thorough fashion. They have involved submission processes, public hearings, and detailed analysis of complex legislation. As discussed below, government responses to these reports have frequently been inadequate, but there is no question that the inquiries have been thorough, balanced, and conducted in a professional manner.

The Clarke Inquiry into the Haneef affair is a good example of how executive branch oversight of the intelligence agencies can lead to substantive change. Haneef was detained and questioned without charge for 12 days in 2007 after being mistakenly linked to the bombing attempt on Glasgow airport. After examining the roles of ASIO, the AFP, and other authorities in detaining Haneef, Clarke made a number of recommendations, including that the office of the INSLM should be created and that limits should be placed on the time allowed for pre-charge detention of terrorist suspects.[150] Both of these recommendations were put into law in 2010.[151] This demonstrates that executive branch oversight mechanisms can be taken seriously by government and act as a catalyst for substantive change in how the intelligence and law enforcement agencies operate.

The reports produced by the IGIS have also been rigorous, and there is no doubt that those appointed to the position have taken their job seriously in inspecting the activities of the intelligence agencies and investigating allegations of misconduct. However, the

---

Report]; Bret Walker SC, Annual Report: 7th November 2013 (2013); Bret Walker SC, Annual Report: 28th March 2014 (2014) [hereinafter *INSLM 2014 Report*].

[145] For example, Walker recommended the repeal of control orders, preventative detention orders, and ASIO's power to detain people for the purposes of questioning. *See INSLM 2012 Report, supra* note 144, at 44, 67, 106.

[146] For example, Walker recommended that ASIO retain its coercive questioning powers, and that it be granted a power to temporarily suspend passports while further security checks are conducted. *See INSLM 2012 Report, supra* note 144, at 70; *INSLM 2014 Report, supra* note 144, at 48–49.

[147] *See* Jessie Blackbourn, *Who's Watching Counter-Terrorism Laws in Australia*, The Conversation, Apr. 3, 2012; Jessie Blackbourn and Nicola McGarrity, *National Security Monitor: Off to a Good Start*, The Drum (ABC) (Mar. 30, 2012), *available at* http://www.abc.net.au/news/2012-03-30/blackbournmcgarrity-national-security-monitor-good-start/3920962.

[148] *Independent National Security Legislation Monitor Act 2010* (Cth) § 6(1); *Terrorism Act 2006* (UK) c 11, § 36(1).

[149] *Sheller Committee Report, supra* note 106; *COAG Review, supra* note 107.

[150] Clarke, *supra* note 91, at xii, 246, 255–56.

[151] *Independent National Security Legislation Monitor Act 2010* (Cth); *National Security Legislation Amendment Act 2010* (Cth) sch 3.

effectiveness of the office and its independence from the intelligence agencies is difficult to gauge due to protections for classified information. Many IGIS reports contain valuable recommendations, such as how the intelligence agencies can improve their procedures in line with legislative requirements,[152] and most of these seem to have been adopted by the relevant agencies.[153] However, many other recommendations are classified,[154] so it is often difficult to know the extent to which the office is holding the agencies to account.

B. Weaknesses

Although there are clearly a number of strengths to this system of executive accountability, there are also a number of key weaknesses and vulnerabilities. An initial point is that breadth should not be mistaken for depth. Although the number and broad coverage of the executive branch oversight mechanisms outlined above is commendable, this does not mean that the framework operates effectively or is sufficient to hold the intelligence agencies to account, even where the exercise of one power might be subject to multiple forms of oversight. The INSLM, for example, described the safeguards applying to ASIO's questioning and detention powers as having "a degree of commendable redundancy."[155] However, having several bodies overseeing the same agencies or powers does not lead to greater accountability if the functions of those bodies overlap, or if they do not delve any deeper into an agency's activities.

One major weakness is that ministerial accountability of the intelligence agencies is not—or at least is not perceived to be—as robust as it might be. Today, ministers tend to have a close relationship with Australia's intelligence agencies, and indeed tend to highlight this for political benefit. Since the events of 9/11, Australian ministers have frequently championed the expansion of the powers of intelligence agencies, without at the same time emphasizing the need for those powers to be tightly constrained to their purpose, or subjected to stringent oversight.

In 2014, for example, Attorney-General George Brandis played the lead role in developing and introducing legislation to dramatically expand ASIO's powers. This included the enactment of a Special Intelligence Operations (SIO) regime, mentioned in the introduction, which provides immunity from civil and criminal liability for ASIO officers involved in specially approved undercover operations.[156] Attached to this regime is a criminal offense that prohibits the public discussion of any information relating to SIOs.[157] The Attorney-General must authorize SIOs in advance and consent to any prosecutions under that offense,[158] but

---

[152] *See, e.g.*, Inspector-General of Intelligence and Security, Inquiry into the Attendance of Legal Representatives at ASIO Interviews, and Related Matters 4 (2014).

[153] *See id.*; *ASIO Annual Report 2014, supra* note 53.

[154] Inspector-General of Intelligence and Security, Inquiry into the Attendance of Legal Representatives at ASIO Interviews, *supra* note 152, at 4.

[155] *INSLM 2011 Report, supra* note 144, at 30.

[156] *Australian Security Intelligence Organisation Act 1979* (Cth) pt 3 div 4.

[157] *Id.* § 35P.

[158] *Id.* § 35B, 35C; Attorney-General, Press Conference Announcing the Introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Oct. 30, 2014), *available at* http://www. attorneygeneral.gov.au/transcripts/Pages/2014/

when Brandis was the key advocate arguing that ASIO needed those powers,[159] it must be questioned whether he, or his successors, will bring a skeptical critical approach to the exercise of those powers. Certainly it does not reflect the same level of independent accountability as if those powers were authorized by a judge or independent statutory office.

This close relationship between the Attorney-General and ASIO differs from that of some previous eras. In 1973, the then Attorney-General Lionel Murphy famously "raided" ASIO's headquarters after he accused the organization of withholding information on a terrorist group.[160] It is difficult to imagine an Attorney-General in the contemporary security environment taking such a radical step in holding the intelligence agencies to account. This may simply reflect the individual approaches of different Attorneys-General, but it also suggests a shift in how the role of the Attorney-General is perceived. The more traditional view, inherited from the U.K., is that the Attorney-General is the first law officer who provides legal advice to the government, oversees the drafting of legislation, and represents the public interest by protecting public rights and upholding the rule of law.[161] In contemporary Australia, the Attorney-General is more frequently viewed as a politician who is more likely to advocate the expansion of executive power than to protect individual rights.

Another key weakness in the system is that independent officeholders such as the IGIS and INSLM have strong investigative powers but no remedial powers. The role of the IGIS, INSLM and Independent Reviewer of ASAs is limited to providing recommendations, and whether these recommendations are adopted depends on whether the government of the day is willing to accept and implement them. Certainly, the record to date demonstrates that Australian governments (on both sides of politics) are very reluctant to accept recommendations for change from executive bodies, and particularly from the INSLM. The government has employed obvious political tactics (such as introducing the INSLM's reports into Parliament on budget day) so that valuable recommendations have been overshadowed by other events.[162] Indeed, the government has not only ignored the INSLM's recommendations to reduce the scope of Australia's counterterrorism laws, but also to expand them. As the INSLM repeated in his final report:

> When there is no apparent response to recommendations that would increase powers and authority to counter terrorism, some skepticism may start to take root about the political imperative to have the most effective and appropriate counter-terrorism laws.[163]

It was significant that this was not the first but the second time he had made this criticism. On neither occasion did even this very pointed observation elicit a government response.

FourthQuarter2014/30October2014-PressConferenceAnnouncingIntroduction OfTelecommunicationsInterceptionAndAccessAmendmentDataRetentionBill.aspx.

[159] *See* Attorney-General, New Counter-Terrorism Measures for a Safer Australia, *supra* note 130.

[160] *See generally* Jenny Hocking, Lionel Murphy: A Political Biography 163–66 (1997).

[161] *See* Ross Ray, The Role of the Attorney-General: An Australian Perspective. Address at the International Bar Association Conference (Oct. 13, 2008), at 3–5.

[162] Jessie Blackbourn, *Non-response Reduces Security Monitor's Role to Window Dressing*, The Conversation, Dec. 19, 2013.

[163] *INSLM 2014 Report, supra* note 144, at 2.

Indeed, the current prime minister Tony Abbott recognized that "the former government ignored all the Monitor's recommendations,"[164] but then used this as a reason to try to abolish the office rather than to change that record.[165]

The government's reluctance to accept the advice of executive oversight bodies can be seen over time in the lack of response to reviews of Australia's counterterrorism laws. This is especially the case where different committees and inquiries reach different conclusions, as the government can adopt a "lowest common denominator" approach or choose to do nothing by claiming that there is no consensus for change.[166] As one of us has written:

> [W]here effective reviews have been conducted, the level of political commitment to implementing their recommendations has been low. Findings even of high-level, expert panels have been ignored or only implemented some years after a change of government. The common thread of Australia's anti-terror laws is thus that such laws have often been enacted in undue haste and reviewed and repaired sometimes at leisure, or often not at all.[167]

One positive counterexample, as detailed above, is the Clarke inquiry into the Haneef affair.[168] That inquiry led to some substantive improvements in the laws relating to pre-charge detention for terrorist suspects.[169] However, those changes were accompanied by an expansion of police power (to conduct warrantless searches of private premises),[170] so the impact of that inquiry in promoting appropriate limits to counterterrorism operations should not be overstated.

Intelligence agencies appear to have accepted the majority of recommendations from the IGIS,[171] although there are some anomalies in the IGIS reports that raise questions about the effectiveness of the office. For example, in 2013, the IGIS began an inquiry into weapons training by ASIS officers. One of the concerns raised by the inquiry related to the requirement that ASIS officers must not handle firearms if their blood alcohol content is above 0.00.[172] In her 2013 report, the IGIS noted that there was "some misconception by staff in relation to this matter," and that "ASIS did not have adequate controls in place," but she

---

[164] Prime Minister, Ministerial Statement on Deregulation (Mar. 19, 2014).

[165] *Independent National Security Legislation Monitor Repeal Bill 2014* (Cth).

[166] Andrew Lynch, *The Impact of Post-Enactment Review on Anti-Terrorism Laws: Four Jurisdictions Compared*, 18(1) J. Leg. Stud. 63, 66 (2012).

[167] George Williams, *A Decade of Australian Anti-Terror Laws*, 35 Melbourne U. L. Rev.1136, 1168 (2011).

[168] Clarke, *supra* note 91.

[169] *National Security Legislation Amendment Act 2010* (Cth) sch 3.

[170] *Id.* at sch 4.

[171] *See, e.g.*, Inspector-General of Intelligence and Security, Inquiry into the Attendance of Legal Representatives at ASIO Interviews, *supra* note 152, at 4; *ASIO Annual Report, supra* note 53, at 44.

[172] Inspector-General of Intelligence and Security, Executive Summary to the Inquiry into the Provision of Weapons and the Training in and Use of Weapons and Self-Defence Techniques in the Australian Secret Intelligence Service 2 (Nov. 2013).

otherwise concluded that there was "no direct evidence that any ASIS staff member had retrieved a weapon with a blood alcohol level greater than 0.00."[173]

In her 2014 annual report, however, the IGIS revealed that an incident involving alcohol and a firearm occurred overseas that "had the potential to cause serious injury."[174] She also revealed that there were "substantial discrepancies" in the information provided to her by ASIS officers in the original inquiry.[175] This admission raises questions about just how effective IGIS is in its oversight in this area, in part because of an apparent lack of willingness on behalf of the intelligence agencies to comply with its inquiries. It is an offense to fail to swear an oath or to refuse to answer a question asked by the IGIS,[176] but in this case the intelligence officers did not face any formal consequences for misleading the IGIS in her inquiries.[177]

The inquiry into the questioning of Izhar Ul-Haque also raises questions about the role of the IGIS, and its independence from the intelligence agencies. Ul-Haque was a young medical student who was suspected of involvement in terrorism and associating with other known terrorists. He was confronted by ASIO officers at a train station and then taken in their car to a nearby park, where he was told there would be serious consequences if he did not cooperate and answer the officers' questions.[178] The IGIS found no evidence to make out a case of trespass, false imprisonment, or unlawful detention.[179] In reaching this conclusion, she seemed to place significant weight on the views of the intelligence agencies as to the threat of terrorism at that time,[180] as well as the testimony of the ASIO officers involved, who "denied that their tone . . . had been threatening or coercive."[181]

By contrast, Justice Adams in the New South Wales Supreme Court delivered a scathing judgment that led the Crown to abandon its case against Ul-Haque. Justice Adams found that the ASIO officers were guilty of trespass, false imprisonment, kidnapping, and unlawful detention.[182] He concluded that their conduct was "grossly improper and constituted an unjustified and unlawful interference with the personal liberty of the accused."[183] On one view, it would be possible to conclude that the IGIS reached a different and more accurate conclusion because she was privy to classified information that the court was not. At the same time, the serious discrepancy between the IGIS report and Supreme Court judgment gives rise to questions about the degree of closeness and common ground between the IGIS and the intelligence agencies, and whether this may hamper the ability of the office to act as a strong accountability mechanism.

---

[173] *Id.*

[174] Inspector-General of Intelligence and Security, *Annual Report: 2013–2014* , at 11 (2014).

[175] *Id.*

[176] *Inspector-General of Intelligence and Security Act 1986* (Cth) § 18(7).

[177] It is however an offense to provide false or misleading information to a person exercising powers or performing functions under a law of the Commonwealth: *Criminal Code Act 1995* (Cth), § 137.1.

[178] *See R v Ul-Haque* [2007] NSWSC 1251, ¶¶ 15–25.

[179] Inspector-General of Intelligence and Security, Report of Inquiry into the Actions Taken by ASIO in 2003 in Respect of Mr Izhar Ul-Haque and Related Matters 37, 39, 41 (2008).

[180] *Id.* at 7–8.

[181] *Id.* at 33, 35.

[182] *R v Ul-Haque* [2007] NSWSC 1251, ¶ 62, ¶ 95.

[183] *Id.* ¶ 62.

Oversight of the intelligence agencies by other executive bodies is also limited in key respects. The Commonwealth Ombudsman and the AHRC would both ordinarily play an important role in investigating the conduct of government departments, but neither has jurisdiction over the intelligence agencies.[184] The ALRC plays a limited role in the national security context given that it has no capacity to self-initiate investigations, and is restricted to assessing legislation on its face (rather than by accessing classified information to assess how that legislation has been used).[185] Even the INSLM, for all the strengths of that office, is only a part-time position with limited resources.[186]

Merits review of the intelligence agencies is particularly weak. It is only available in the Security Appeals Division of the AAT in relation to ASIO's adverse security assessments,[187] and then only to citizens affected by those assessments.[188] The more significant concern with adverse security assessments relates to their use in applications for refugee status,[189] but merits review in the Security Appeals Division is not available to noncitizens.[190] Even where citizens apply to the Security Appeals Division to challenge an assessment, this is incredibly difficult due to the issuing of public interest certificates by the Attorney-General.[191] Those certificates allow the tribunal to rely on classified information without revealing it to the applicant.

The difficulties that noncitizens face in challenging adverse security assessments were eased somewhat after the first Independent Reviewer of ASAs was appointed in 2012. However, that position only exists by virtue of terms of reference issued by the Attorney-General: in contrast to the IGIS and INSLM,[192] the office has no legislative backing and therefore no statutory tenure or questioning powers. This means that the Independent Reviewer of ASAs is less independent from government compared to the IGIS and INSLM, and also in a much weaker position to conduct robust inquiries. The terms of reference permit the Independent Reviewer of ASAs to access all information held by ASIO in issuing its adverse security assessments,[193] but the office cannot, for example, compel intelligence officers to appear for questioning.

The initial reports of the Independent Reviewer of ASAs largely confirm that ASIO has acted appropriately in declaring certain noncitizens to be a security risk,[194] but this is curious

---

[184] *Ombudsman Regulations 1977* (Cth) sch 1 reg 4; *Australian Human Rights Commission Act 1986* (Cth) § 11(3).

[185] *Australian Law Reform Commission Act 1996* (Cth) § 21(1).

[186] *Independent National Security Legislation Monitor Act 2010* (Cth) § 11(1).

[187] *Australian Security Intelligence Organisation Act 1979* (Cth) § 54.

[188] *Id*. § 36.

[189] *See generally* Ben Saul, *Dark Justice: Australia's Indefinite Detention of Refugees on Security Grounds under International Human Rights Law*, 13 Melbourne J. Int'l L. 685 (2012); Ben Saul, *"Fair Shake of the Sauce Bottle": Fairer ASIO Security Assessment of Refugees*, 37(4) Alternative L.J. 221 (2012); Ben Saul, *The Kafkaesque Case of Sheikh Mansour Leghaei: The Denial of the International Human Right to a Fair Hearing in National Security Assessments and Migration Proceedings in Australia*, 33(3) U. New South Wales L.J. 629 (2010).

[190] *Australian Security Intelligence Organisation Act 1979* (Cth) § 36.

[191] *Id*. § 38(2); *Administrative Appeals Tribunal Act 1975* (Cth), § 36. *See* Hardy, *supra* note 8, at 44–48.

[192] *Inspector-General of Intelligence and Security Act 1986* (Cth); *Independent National Security Legislation Monitor Act 2010* (Cth).

[193] *See* Roxon, *supra* note 87, at 1.

[194] *See ASIO Annual Report 2014, supra* note 53, at 47–49.

given the weight of other expert evidence suggesting that certain populations subject to adverse security assessments (particularly the Tamil community from Sri Lanka) pose no risk of terrorism.[195] This is not to suggest that the Independent Reviewer of ASAs does not take her review functions seriously, or is helping ASIO to cover up misconduct, but it does suggest a more general problem—which is that it is very difficult to gauge the effectiveness of an executive oversight body that relies on classified information. The IGIS, INSLM, and Independent Reviewer of ASAs, as well as other inquiries such as the COAG Review, all rely on classified submissions from the intelligence agencies and law enforcement to reach their conclusions and recommendations. The public must ultimately trust that these bodies are holding the intelligence agencies to account, rather than (for example) being able to access and inspect that information themselves through freedom of information requests.[196]

This degree of secrecy could be excused if there were greater confidence that serious misconduct would be uncovered if existing oversight mechanisms fail. This is where whistleblower protections play a crucial role, as they provide a "release valve" that allows employees of a government department to disclose wrongdoing that has not been uncovered by other means. However, in Australia, the broad exemptions for intelligence information in the PID Act mean that the scheme does not provide any greater accountability than the IGIS already provides.[197] If an intelligence officer sought to reveal one or more instances of misconduct by disclosing classified information, he or she would only receive whistle-blower protections if the information was disclosed internally to the officer's supervisors, to the IGIS, or to a lawyer.[198] It would be virtually impossible for the officer to receive protection for disclosing that information externally, such as to a respected journalist or member of Parliament.[199] Indeed, Parliament has recently enacted a range of stronger offenses to prevent whistle-blowing by intelligence officers.[200]

Perhaps the major vulnerability in executive oversight of the intelligence agencies is that it is extremely difficult to hold those agencies to account when the government has granted them such extraordinary statutory powers. For example, ASIO's questioning and detention warrant regime allows the organization to detain non-suspect citizens for up to a week for questioning.[201] When legislation empowers ASIO to do this, what can the IGIS or INSLM do if those powers are used correctly, other than suggest changes to the legislation, which the government is then free to ignore? Those powers may be exercised to the letter of the law, but they are still of concern for their impact on fundamental rights.

---

[195] *See* Andrew & Renata Kaldor Centre for International Refugee Law, *Factsheet: Refugees with an Adverse Security Assessment by ASIO* (Feb. 24, 2015), *available at* http://www.kaldorcentre.unsw.edu.au/sites/default/files/ASIO%20factsheet%20%2024%202%2015.pdf. For example, one Tamil refugee classified as a security risk was a mentally ill young man who was left brain-damaged after being beaten by the Sri Lankan military: Kerry Brewster, *Tamils Speak Out against ASIO Security Rulings*, Lateline (ABC TV) (Aug. 13, 2012), *available at* http://www.abc.net.au/lateline/content/2012/s3567008.htm.

[196] Due to numerous exemptions: *see, e.g. Freedom of Information Act 1982* (Cth) sch 3.

[197] *Public Interest Disclosure Act 2013* (Cth) §§ 26(1)(c). *See* Hardy & Williams, *supra* note 79, at 814–15.

[198] *See* Hardy & Williams, *supra* note 79, at 814–15.

[199] *See id*.

[200] *National Security Legislation Amendment Act (No 1) 2014* (Cth) sch 6; *Intelligence Services Act 2001* (Cth) pt 6; *Australian Security Intelligence Organisation Act 1979* (Cth) §§ 18–18B, 35P.

[201] *Australian Security Intelligence Organisation Act 1979* (Cth) pt III div 3.

This suggests that the larger problem is not necessarily how the current system of executive accountability has been designed, or whether statutory officeholders have sufficient investigative powers. Rather, it is how executive accountability mechanisms can counterbalance the vast expansion of counterterrorism laws over more than a decade, from those introduced in the wake of the 9/11 attacks to those introduced in 2014 and 2015 in response to the threat of foreign fighters returning from Syria and Iraq.[202] An intelligence agency will seldom be held to account for exercising statutory powers that are difficult to exceed.

V. CONCLUSION

Executive oversight mechanisms play a crucial role in keeping intelligence agencies accountable because it is difficult to scrutinize those agencies' activities in the media, courts, and Parliament. In Australia, a broad range of executive oversight mechanisms allow oversight of the six intelligence agencies. These overseeing bodies include the IGIS, a statutory office that inspects and inquires into the intelligence agencies' activities; the INSLM, an independent monitor of Australia's counterterrorism laws; the Security Appeals Division of the AAT and the Independent Reviewer of ASAs, both of which review the merits of adverse security assessments issued by ASIO; the Auditor-General and the Australian National Audit Office, which conduct performance and financial audits of the intelligence agencies; and several committees comprising senior members of the executive branch, which govern intelligence policy and collection priorities.

This system of executive accountability has several strengths. The number and broad coverage of oversight mechanisms is evidence of a commitment to maintaining the accountability of intelligence agencies, despite their secret activities. The IGIS and the INSLM in particular have statutory tenure and strong investigative powers,[203] which preserves their independence from government and allows the officeholders to conduct thorough inspections, inquiries, and reviews. Other statutory and ad hoc inquiry bodies, such as the COAG Review of Counter-Terrorism Legislation, have conducted rigorous inquiries involving written submissions and oral evidence from a wide range of interested individuals and organizations. These inquiries have produced detailed reports on complex areas of Australia's counterterrorism laws.[204]

At the same time, there are a number of weaknesses and vulnerabilities in the system that suggest room for improvement. The relationship between the intelligence agencies and their responsible ministers is perceived as being very close, rather than an effective check on the misuse of statutory powers. The most that executive oversight mechanisms can do to remedy wrongdoing or problematic legislation is to recommend change, which is rarely forthcoming from the government. Some bodies that play an important role in holding other government departments accountable—namely the Commonwealth Ombudsman, Australian Law

[202] *Security Legislation Amendment (Terrorism) Act 2002* (Cth); *National Security Legislation Amendment Act (No 1) 2014* (Cth); *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* (Cth).

[203] *Inspector-General of Intelligence and Security Act 1986* (Cth) §§ 18, 30; *Independent National Security Legislation Monitor Act 2010* (Cth) § 19, pt 3.

[204] *See, e.g., Sheller Committee Report, supra* note 106; *COAG Review, supra* note 107.

Reform Commission, and Australian Human Rights Commission—are limited to advocacy and law reform work with regard to national security matters. Merits review of the intelligence agencies is particularly weak, as the Security Appeals Division of the AAT only has jurisdiction to review adverse security assessments issued by ASIO in relation to Australian citizens.

Although the details of these accountability mechanisms are specific to the Australian context, they raise a number of themes or lessons relating to executive oversight of intelligence agencies generally and how this oversight might be improved. These may have some resonance beyond Australia. The first is that recommendatory powers can have only limited impact in holding intelligence agencies to account. This is because governments are free to accept or ignore the recommendations of executive bodies as they see fit. It is difficult to conceive of how independent officeholders or other inquiry bodies could have stronger remedial powers along the lines of those possessed by a court, and indeed this is a weakness inherent in any form of executive oversight. Nevertheless, small changes to strengthen their existing recommendatory powers could be a notable improvement. For example, the government and the intelligence agencies could be required to consider the recommendations of independent officeholders and to provide reasons (so far as possible while protecting classified information) within a set period of time as to why any recommendations have not been followed.[205] This would prevent government from ignoring important reports or burying them with political tactics.

A second point is that the success and effectiveness of executive oversight mechanisms is difficult to gauge as they rely heavily on classified information. The need to protect classified information is the reason special statutory offices and inquiries are needed to review the activities of the intelligence agencies. However, those offices and inquiries are, understandably, subject to the same protections as the agencies themselves,[206] so the public must often trust that they are holding the intelligence agencies to account rather than knowing this to be the case. Trust in this process can be maximized if governments appoint experienced and well-respected individuals to positions such as the IGIS and INSLM, if the independence and tenure of those offices is guaranteed by statute, and if the offices possess strong statutory powers to undertake their reviews and inquiries.

Third, given this need for secrecy, whistle-blower legislation will provide a crucial "release valve" in circumstances where misconduct or maladministration by the intelligence agencies is not uncovered by other means. Striking the right balance in whistle-blower legislation between protecting classified information and promoting accountability will be difficult, but it is an important task that requires ongoing attention. On the one hand, any information leaked by intelligence officers must be kept to the minimum necessary to reveal wrongdoing, and that information must not endanger lives or expose intelligence sources or methods. On the other hand, public confidence in the accountability of intelligence agencies is undermined by blanket exemptions to whistle-blower legislation and strong anti-whistle-blower

---

[205] The IGIS may produce a report when a government response is inadequate, but there is no obligation on the government or an agency to respond to a report or provide reasons as to why any recommendations have not been adopted. *See Inspector-General of Intelligence and Security Act 1986* (Cth) § 24A.

[206] *See Inspector-General of Intelligence and Security Act 1986* (Cth) § 20; *Independent National Security Legislation Monitor Act 2010* (Cth) § 28; *Auditor-General Act 1997* (Cth) § 26; Roxon, *supra* note 87.

offences.[207] The Australian government's recent crackdown on intelligence whistle-blowing gives the impression that it is unwilling for misconduct or maladministration by the intelligence agencies to see the light of day.

If the Australian intelligence agencies are to be held to a sufficient standard of accountability, intelligence officers should have some capacity to responsibly disclose serious wrongdoing by their employers where other avenues, including the IGIS, have been exhausted. This could be achieved by amending the PID Act to allow an intelligence officer to disclose serious wrongdoing or unlawful conduct to specified persons or bodies outside the agency and executive branch (such as a judge, another member of Parliament, or the PJCIS) where he or she believes on reasonable grounds that all other inquiries into that wrongdoing have been inadequate.

Fourth, executive oversight of the intelligence agencies could be improved if tribunals equipped to handle classified information were granted a wider jurisdiction. In Australia, the Security Appeals Division of the AAT assesses the merits of adverse security assessments issued by ASIO, but this is only a small portion of one intelligence agency's activities. Given the difficulties in holding the intelligence agencies to account through other means, specialist tribunals could take on a larger share of the burden by scrutinizing a wider range of intelligence agencies' activities. Improved procedures for handling classified information, such as a program whereby applicants could rely on special advocates with security clearances,[208] would help to improve the fairness of merits review proceedings.

Last, counterterrorism laws that define the intelligence agencies' powers require ongoing attention and scrutiny. It is these powers, and not necessarily weaknesses in executive oversight, which pose the greatest threat to the accountability of intelligence agencies. Whichever form it takes, such oversight should be rigorous and recurring, and it must be taken seriously by the government. This is crucial given the extraordinary breadth of clandestine powers granted to intelligence agencies in response to the ongoing threat of terrorism. Unless the powers granted to intelligence agencies are themselves properly constrained in the first place, no form of executive oversight is likely to be effective.

[207] Hardy & Williams, *supra* note 79, at 814–15; *National Security Legislation Amendment Act (No. 1) 2014* (Cth) sch 6.

[208] *See generally* McGarrity & Santow, *supra* note 8; Bray & Martin, *supra* note 8; Aileen Kavanagh, *Special Advocates, Control Orders and the Right to a Fair Trial*, 73(5) Modern L. Rev. 836 (2010); John Ip, *The Rise and Spread of the Special Advocate*, Public L. 717 (2008).