*Greg Carne**

GUIDING LIGHT OR OPAQUE FILTER?: THE MINISTER'S GUIDELINES FOR THE AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION IN PERFORMING ITS FUNCTIONS AND EXERCISING ITS POWERS AS RELEVANT TO SECURITY

Abstract

The issue in 2020 of new ministerial guidelines ('*2020 Guidelines*') for the performance by the Australian Security Intelligence Organisation ('ASIO') of its functions and the exercise of its powers as relevant to security, after a 13-year interval, is significant as very substantial changes in ASIO's legislation, powers, resources and priorities occurred during that time.

The *2020 Guidelines* reveal critical new issues in their review processes, content and operation. These issues should be addressed if the Guidelines are to achieve optimal, integrated and complementary performance as one of several ASIO accountability mechanisms, in turn part of ministerial responsibility under the chosen Australian parliamentary model of human rights.

There are several pressing reform issues in the *2020 Guidelines*, including: the need to improve consultative processes for review and development to match the expanding reach of ASIO security activities; the fact that the *2020 Guidelines* authorise classified ASIO policies and thereby provide insufficient public guidance; and, the capacity of the *2020 Guidelines* to interpretively enlarge the concept of relevance to security and, in particular, broaden the concept of politically motivated violence.

Further important issues and reforms arise from the treatment by the *2020 Guidelines* of exiting or remediating the intelligence gathering process, including the collation and retention of personal information, as well a need to more clearly shape proportionality matters in familiar legal principles.

* Associate Professor, School of Law, University of New England, New South Wales, Australia. The author would like to thank the two anonymous referees for their comments on this article.

Noticeable deficiencies in the *2020 Guidelines* give cause for concern and reflection. Specific and broader reforms to the processes generating, and the content informing, the Guidelines are canvassed throughout the article and in its conclusion. These reforms are intended to improve the presently understated function of the *2020 Guidelines* as part of a more integrated and responsive ASIO accountability framework.

I Introduction

In 2020, ministerial guidelines ('*2020 Guidelines*') for the performance by the Australian Security Intelligence Organisation ('ASIO') of its functions or the exercise of its powers under s 8A of the *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*') were renewed and revised by the Minister for Home Affairs ('Minister').[1] Three matters regarding the *2020 Guidelines* are of special importance.

First, the *2020 Guidelines* represent the first revision since guidelines were issued by the Attorney-General in 2007 ('*2007 Guidelines*').[2] The intervening time has seen enormous increases in ASIO's legislation, powers, resources and priorities.[3] This long interval is likely to have diminished the efficacy of the *present* Guidelines model as an accountability measure. Second, parliamentary committee processes have raised issues about the revision of Guidelines, including matters of fitness for

1 Minister for Home Affairs (Cth), *Minister's Guidelines in Relation to the Performance by the Australian Security Intelligence Organisation of Its Functions and the Exercise of Its Powers* (August 2020) ('*2020 Guidelines*').

2 The *2020 Guidelines* replaced two previous guidelines that were issued in 2007 ('*2007 Guidelines*'): Attorney-General (Cth), *Attorney-General's Guidelines in Relation to the Performance by the Australian Security Intelligence Organisation (ASIO) of Its Function of Obtaining Intelligence Relevant to Security* (29 August 2007); Attorney-General (Cth), *Attorney-General's Guidelines in Relation to the Performance by the Australian Security Intelligence Organisation of Its Functions Relating to Politically Motivated Violence* (29 August 2007). See also: Philip Ruddock, 'New Guidelines Update ASIO Accountability' (News Release 235/2007, 12 October 2007); Letter from Robert Cornall to Bill Grant, 27 June 2008.

3 ASIO activity expanded following multiple national security legislative enactments. 'Since the 9/11 terrorist attacks in 2001, the Australian Parliament has passed more than 124 Acts amending the National Intelligence Community's legislative framework': Attorney-General's Department (Cth), 'Government Response to the Comprehensive Review into Intelligence Legislation (Richardson Review)' (Media Release, 4 December 2020) ('Government Response'). See also: George Williams, 'A Decade of Australian Anti-Terror Laws' (2011) 35(3) *Melbourne University Law Review* 1136, 1144–6; Jessie Blackbourn and Nicola McGarrity, 'How Reactive Law-Making Will Limit the Accountability of ASIO', *Inside Story* (online, 24 July 2014) <https://insidestory.org.au/how-reactive-law-making-will-limit-the-accountability-of-asio/>; Rebecca Ananian-Welsh and George Williams, 'The New Terrorists: The Normalisation and Spread of Anti-Terror Laws in Australia' (2014) 38(2) *Melbourne University Law Review* 362, 365 ('The New Terrorists').

purpose and public reassurance.[4] Third, the relocation of ASIO from the Attorney-General's portfolio to the Home Affairs portfolio in 2017, as part of a broader re-assignment of functions in forming a National Intelligence Community ('NIC'),[5] accentuates concerns about ministerial responsibility and accountability, with the concentration of ASIO and other agencies in Home Affairs.[6] Those concerns are apposite for the *2020 Guidelines*, which provide ministerial mandated standards for performing some aspects of ASIO's work, but leave significant reliance upon developing and maintaining classified policies sitting below the public Guidelines, in addition to ministerial discretion. Ministerial disposition and practice therefore emerge as important considerations in whether the content and operation of the *2020 Guidelines* is shaped for controlling, or enhancing, agency power.[7]

---

4 See Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the National Security Legislation Amendment Bill (No 1) 2014* (Report, September 2014) 46 [3.51]–[3.52], recommendation 4 ('*PJCIS Advisory Report*'). See also Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 10 July 2020, 7 (Natasha Molt, Director of Policy, Law Council of Australia), 21 (Margaret Stone, Inspector-General of Intelligence and Security), 58 (Anthony Coles, First Assistant Secretary, Law Enforcement Policy Division, Department of Home Affairs).

5 ASIO, the Australian Signals Directorate ('ASD'), the Australian Secret Intelligence Service ('ASIS'), the Australian Geospatial-Intelligence Organisation ('AGO'), the Defence Intelligence Organisation ('DIO'), and the Australian Criminal Intelligence Commission ('ACIC') are the intelligence agencies, whilst the Australian Transaction Reports and Analysis Centre ('AUSTRAC'), the Australian Federal Police ('AFP'), the Department of Home Affairs and the Department of Defence (other than the AGO or DIO) are agencies with an intelligence role or function. Collectively, these ten agencies form the National Intelligence Community ('NIC'). See: *Office of National Intelligence Act 2018* (Cth) s 4 (definitions of 'national intelligence community', 'intelligence agency', 'agency with an intelligence role or function'); Greg Carne, 'Designer Intelligence or Legitimate Concern?: Establishing an Office of National Intelligence and Comprehensively Reviewing the National Intelligence Community Legal Framework' (2019) 46(1) *University of Western Australia Law Review* 144, 144. ('Designer Intelligence or Legitimate Concern?').

6 ASIO, AFP, the Australian Border Force, ACIC and AUSTRAC were the five Department of Home Affairs agencies. In 2022, the Albanese Government moved the AFP from the Department of Home Affairs to the Attorney-General's Department: Michael Pelly, 'AFP Back in the A-G's Hands amid Portfolio Reshuffle', *Australian Financial Review* (Sydney, 3 June 2022) 32.

7 See, eg, Flick J's observations regarding the previous Minister for Home Affairs ('Minister'), Peter Dutton, in light of possible non-compliance with legal obligations: *AFX17 v Minister for Home Affairs [No 4]* (2020) 279 FCR 170, 173 [9]. Karen Andrews succeeded Dutton in the Home Affairs portfolio in 2021. The present Minister is Clare O'Neil.

Part II commences with an assessment of the origins, sources, and characteristics of the legal framework of the *2020 Guidelines*,[8] founded upon a ministerial responsibility model to Parliament. A synopsis follows of the *2020 Guidelines*' five parts and appendix. Supporting historical sources are canvassed, confirming the location of the *2020 Guidelines* within responsible government and ministerial responsibility doctrines. The major ministerial responsibility consideration with the Guidelines as an ASIO accountability mechanism is ASIO's distinctive circumstances in comparison to other state institutions. Principally, these circumstances include the necessity to conduct intelligence activities in secret, as well as the risk of ASIO ministerial authority being applied in a politicised way. Both factors have generated distinctive ministerial practices, shaping the *legislated* relationship between the Minister and the Director-General of Security ('Director-General'), whilst reflecting the more problematic contextual nature of ministerial responsibility and its conventions. It is argued that these distinctive characteristics and the recent bifurcation of responsibilities between the Minister and the Attorney-General make it particularly important that the Guidelines are carefully calibrated to ensure ASIO practices are lawful and proper. The identified distinctive challenges for the doctrine of ministerial responsibility in ASIO security circumstances are of course cumulative upon existing difficulties outside a specific national security context.

The special functions of the Inspector-General of Intelligence and Security ('IGIS'), created partly to address the conundrums of ministerial responsibility in the ASIO security context, are then examined. The Guidelines' status as administratively, but not legally, enforceable, alongside the IGIS's compliance, review and monitoring functions over ASIO and the Guidelines, creates two distinctive issues. First, the Guidelines need optimal drafting for the IGIS to best perform its compliance functions. Second, breaches of the Guidelines, reported by IGIS to the Minister, then incorporated in the IGIS annual report, suggest that resultant Guidelines improvements may further reinforce the IGIS compliance function, and indirectly, ministerial responsibility.

Additional reform rationales exist for the Guidelines through their indirect influence upon other parts of the ASIO accountability framework — the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') and the Independent National Security Legislation Monitor ('INSLM') — in the effective discharge of their roles, particularly with the profusion of enacted ASIO national security laws. Principles and lessons obtained in academic commentary discussing ASIO accountability may be extrapolated to inform refinement of the Guidelines — in order to make ministerial responsibility matters more obvious and increase the responsiveness of

8 There is limited academic literature on any version of the Guidelines. See, eg: Keiran Hardy and George Williams, 'Executive Oversight of Intelligence Agencies in Australia' in Zachary K Goldman and Samuel J Rascoff (eds), *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (Oxford University Press, 2016) 315, 330–1; Greg Carne, 'Thawing the Big Chill: Reform, Rhetoric and Regression in the Security Intelligence Mandate' (1996) 22(2) *Monash University Law Review* 379, 425–9 ('Thawing the Big Chill').

other accountability mechanisms. These ministerial responsibility considerations highlight the need for improvements in the content, operation and review processes of the Guidelines.

Part III examines and critiques *selected and illustrative* priority areas for Guidelines reform.[9] These include: the fact that the Guidelines do not always provide guidance, allowing significant delegation of subject matter to maintained and classified internal ASIO policies; that the Guidelines' central criterion of *relevance to security* is an inherently broad concept, the Guidelines facilitating further expansion of this already capacious security remit in such an area as politically motivated violence; and that the Guidelines afford inadequate exit points for intelligence gathering and insufficient prescribed processes for the review, deletion and destruction of information not relevant to security.

Part IV concludes by noting that deficiencies in the Guidelines give cause for concern and reflection. Within their inherent limitations, the Guidelines need re-conceptualisation and enhanced content if they are to adequately influence ASIO's contemporary and prospective roles of engaging with activities *relevant to security*. The Guidelines are premised as an ASIO accountability measure within a complex and contested model of ministerial responsibility, indirectly affecting other accountability mechanisms. Within the preferred Australian model of the parliamentary protection of human rights, the Guidelines require refinement to facilitate the best possible ministerial responsibility-based accountability. Various review forums for the Guidelines, and overtly re-positioning them as part of a matrix of integrated and complementary ASIO accountability mechanisms, are proposed. It is further argued that the Guidelines would be coherently shaped by a stated series of objectives. The inherent limitations of the Guidelines mean that direct legislative and other accountability changes to the *ASIO Act* on occasions would be more effective and would instil greater public confidence.

II The Background of the Guidelines

A *The Legal Framework of the Guidelines*

Guidelines in relation to the performance by ASIO of its functions and the exercise of its powers are authorised under s 8A(1) of the *ASIO Act*.[10] A further ministerial authority exists to issue guidelines for the performance of ASIO's functions relating to politically motivated violence.[11] The Guidelines' objective is the provision to ASIO of guidance when performing its functions under s 17(1) of the *ASIO Act*.

---

9 Space precludes an examination of other issues such as the Minister's introduction of a proportionality test in the *2020 Guidelines*.

10 *Australian Security Intelligence Organisation Act 1979* (Cth) s 8A(1) ('*ASIO Act*').

11 Ibid ss 4 (definition of 'politically motivated violence'), 8A(2).

The *2020 Guidelines* were tabled out of session in the Senate on 13 August 2020.[12] They replaced the *2007 Guidelines*, whilst incorporating new guidelines regarding politically motivated violence.[13]

The *2020 Guidelines* constitute a distinctive ASIO accountability scheme measure. Their intention is to give practical ministerial guidance, through the Director-General, in the performance by ASIO of its functions and powers and to the Director-General in relation to specified ASIO personnel matters.[14] The Guidelines constitute an important, but understated, part of the ASIO oversight and accountability framework, which includes the PJCIS,[15] the IGIS,[16] and the INSLM.[17]

The origin of the Guidelines traces to the 1984 Royal Commission on Australia's Security and Intelligence Agencies ('Second Hope Royal Commission'), which recommended that 'there should be clear provision in the [ASIO] Act enabling the Attorney-General to lay down guidelines governing ASIO's activities in particular areas'.[18] Whilst not legislative instruments,[19] the Guidelines are administratively

12 Law Council of Australia, *Comments on the Minister's Guidelines to the Australian Security Intelligence Organisation* (Comment, 13 August 2020) 4 [1] ('*Comments on the Minister's Guidelines*').

13 Guidelines concerning politically motivated violence formed a separate set of guidelines in the *2007 Guidelines* (n 2). They are now incorporated in pt 5 of the *2020 Guidelines* (n 1), which is a single set of guidelines.

14 *ASIO Act* (n 10) ss 8A(1)(a)–(b).

15 *Intelligence Services Act 2001* (Cth) pt 4 ('*Intelligence Services Act*'). For appraisal of the PJCIS's review of national security laws, see: Greg Carne, 'Sharpening the Learning Curve: Lessons from the Commonwealth Parliamentary Joint Committee of Intelligence and Security Review Experience of Five Important Aspects of Terrorism Laws' (2016) 41(1) *University of Western Australia Law Review* 1 ('Sharpening the Learning Curve'); Greg Carne, 'Reviewing the Reviewer: The Role of the Parliamentary Joint Committee on Intelligence and Security' (2017) 43(2) *Monash University Law Review* 334 ('Reviewing the Reviewer').

16 *Inspector General of Intelligence and Security Act 1986* (Cth) s 8 ('*IGIS Act*').

17 *Independent National Security Legislation Monitor Act 2010* (Cth) s 6 ('*INSLM Act*'). For INSLM engagement with national security accountability issues, see: Jessie Blackbourn, 'The Independent National Security Legislation Monitor's First Term: An Appraisal' (2016) 39(3) *University of New South Wales Law Journal* 975, 993–5; Bret Walker, 'Reflections of a Former Independent National Security Legislation Monitor' [2016] (84) *AIAL Forum* 74; Michael Pelly, 'What Terrorism Law Expert James Renwick Learnt in Afghanistan', *Australian Financial Review* (online, 21 February 2020) <https://www.afr.com/policy/foreign-affairs/what-terrorism-law-expert-james-renwick-learnt-in-afghanistan-20200217-p541nb>.

18 *Royal Commission on Australia's Security Intelligence Agencies: Report on the Australian Security Intelligence Organization* (Report No 232/1985, December 1984) 321 [16.52] ('*Second Hope Royal Commission Report*').

19 The Guidelines are not a legislative instrument, nor a non-disallowable legislative instrument, nor a notifiable instrument: *Legislation Act 2003* (Cth) ss 7–8, 11; ibid 321–2 [16.52].

binding on ASIO,[20] setting internal standards for the performance of its functions[21] and the exercise of its powers.[22] The Guidelines are located *squarely* within a model of ministerial responsibility to Parliament, reflected in other aspects of the *ASIO Act*.[23] In the Second Hope Royal Commission's report, the Guidelines are described as '"binding" on ASIO in the sense that any action in breach of them would be in breach of a lawful ministerial direction, and the person or persons responsible for the breach would be accountable administratively'.[24] In other words, the Guidelines directly form an administrative accountability measure, but lack prescribed consequences for breach as a stronger measure of public accountability. .

B *A Synopsis of the 2020 Guidelines*

An outline of the *2020 Guidelines* is a useful tool for framing discussion and analysis. The Ministerial Foreword to the *2020 Guidelines* states:

> These Guidelines set out the principles ASIO is required to observe in order to meet the public's expectations in performing its functions, including obtaining, correlating and evaluating intelligence relevant to security, and the interpretation of politically motivated violence. In doing so, the Guidelines form a critical component of the accountability framework that provides assurance that ASIO fulfils its vital functions consistent with the values of the community it serves.[25]

The Introduction and Overview follows the Foreword. The Guidelines are divided into five Parts, with an Appendix setting out key terms. The *2020 Guidelines* are distinctive for adopting a broad, general principles approach, the omission of major security-related subject content, and the outsourcing of significant accountability measures to classified ASIO internal policies. This highlights a likely shortfall between the Guidelines' public accountability role, in how effectively the Guidelines might deliver such accountability.

---

20 *ASIO Act* (n 10) s 8A(1).

21 Ibid s 17(1)(a) lists ASIO's functions, which importantly include 'to obtain, correlate and evaluate intelligence relevant to security'.

22 See ASIO's special powers relating to politically motivated violence, espionage, acts of foreign interference and special intelligence operations: ibid pt 3 divs 3–4. Significantly, the *2020 Guidelines* (n 1) refer specifically to 'special intelligence operations': at 9. However, the *2020 Guidelines* omit reference to exercising special powers for politically motivated violence, espionage and acts of foreign interference.

23 The Attorney-General of Australia, as first law officer and a member of Cabinet, is the warrant issuing authority, exercising administrative power, for the special powers in *ASIO Act* (n 10) pt III div 2.

24 *Second Hope Royal Commission Report* (n 18) 322 [16.52(b)]. The Report notes that '[i]t would be for the Attorney-General, aided by the Inspector-General, to hold ASIO to account under the guidelines': at 322 [16.52(b)].

25 *2020 Guidelines* (n 1) 2.

Part 1[26] provides information about 'how the Guidelines should be implemented and observed, with the Director General of Security ultimately responsible for [their] implementation … and ASIO's compliance with them subject to oversight by the [IGIS]'.[27] It also includes a Guidelines review clause.

Part 2[28] provides ASIO with initial guidance on the authorisation and conduct of inquiries and investigations. It also includes content regarding review of inquiries and investigations, advice to the Minister, warrants, special intelligence operations, the requirement for the Leader of the Opposition to be kept informed on security matters, the conduct of security assessments and the use of force against a person under warrant.

Part 3[29] provides guidance relating to ASIO collection activities when performing its functions of obtaining, correlating and evaluating intelligence relevant to security. It introduces a consolidated section on the proportionality of ASIO collection of information, as well as statements about what type of collection of intelligence may be relevant to security.

Part 4[30] provides an outline of the timing and method of ASIO's handling, retention and destruction of personal information. Passing reference is made to applicable legislation and the need to maintain internal policies and practices around access, management and destruction of personal information records.

Part 5[31] provides guidance for ASIO performance in relation to its functions for politically motivated violence. This includes the interpretation of the different aspects of politically motivated violence, investigations into demonstrations and other forms of protest, and the assessment of politically motivated violence.

The Appendix[32] importantly defines a number of terms in the Guidelines, including: 'ASIO affiliate'; 'de-identified'; 'intelligence relevant to security'; 'inquiry'; 'investigation'; 'personal information'; and 'subject'.

C *Ministerial Responsibility as Framing the Guidelines in the ASIO Circumstances of Relevance to Security*

The Guidelines as an accountability measure are firmly located within the doctrine of responsible government and ministerial responsibility. As such, the special

26 Ibid 4–6.

27 Ibid 3. See also *IGIS Act* (n 16) s 8(1)(a)(ii).

28 *2020 Guidelines* (n 1) 7–10.

29 Ibid 11–12.

30 Ibid 13–16.

31 Ibid 17–21.

32 Ibid 22.

challenges of ministerial responsibility for ASIO security activities are further informed by the practical realities of the doctrine in non-security contexts.[33]

In the security context, operational control of ASIO is given to the Director-General.[34] In performing the Director-General's functions under the *ASIO Act* the Director-General is subject to the directions of the Minister.[35] This includes the capacity of the Minister to issue guidelines to the Director-General to be observed by ASIO in the performance of its functions or the exercise of its powers[36] and in the performance of ASIO in relation to politically motivated violence.[37]

These arrangements reflect the informing content of the Second Hope Royal Commission Report, the recommendatory source for the Guidelines' introduction:

> ASIO is part of the executive government of the Commonwealth and, subject to any legislation which otherwise provides, is subject to ministerial control. … The oversight of ASIO's activities in the public interest, and ASIO's accountability through the Parliament to the public, depends on the effectiveness of this ministerial control.[38]

The Second Hope Royal Commission Report recommended that the Attorney-General should be able to issue guidelines governing ASIO's activities:

---

33 On problems associated with the ministerial responsibility doctrine in non-security situations, see: JW Shaw, 'The Established Principles of Cabinet Government' (2001) 73(2) *Australian Quarterly* 21, 21; John Summers, 'Parliament and Responsible Government' in Alan Fenna, Jane Robbins and John Summers (eds), *Government and Politics in Australia* (Pearson Australia, 10th ed, 2014) 35; Patrick Weller, 'Disentangling Concepts of Ministerial Responsibility' (1999) 58(1) *Australian Journal of Public Administration* 62, 63; Kevin Martin, 'Ministerial Responsibility and Parliamentary Accountability: Observations on the Role of the Leader and Ministerial Responsibility' (2008) 23(1) *Australasian Parliamentary Review* 229, 230; Charles Lawson, 'The Legal Structures of Responsible Government and Ministerial Responsibility' (2011) 35(3) *Melbourne University Law Review* 1005, 1008–10; Suri Ratnapala and Jonathan Crowe, *Australian Constitutional Law: Foundations and Theory* (Oxford University Press, 3rd ed, 2012) 43–5, 53–5; Judy Maddigan, 'Ministerial Responsibility: Reality or Myth?' (2011) 26(1) *Australasian Parliamentary Review* 158, 158–60. In June 2022, the Albanese Government introduced a new ministerial code of conduct, replacing the Morrison Government's Statement of Ministerial Standards: Department of the Prime Minister and Cabinet, *Code of Conduct for Ministers* (June 2022); Anna Macdonald, 'Albanese Enacts Changes to Ministerial Code of Conduct', *The Mandarin* (online, 11 June 2022) <https://www.themandarin.com.au/194283-albanese-enacts-changes-to-ministerial-code-of-conduct/>.

34 *ASIO Act* (n 10) s 8.

35 Ibid.

36 Ibid s 8A(1)(a).

37 Ibid s 8A(2).

38 *Second Hope Royal Commission Report* (n 18) 309 [16.17]–[16.18].

> There is … a strong case for the Attorney-General to play a positive role in laying down general directions or guidelines to govern ASIO's conduct in particular areas. Within the framework of the legislation there will inevitably be areas of broad discretion and judgment where the setting by the responsible Minister from time to time of standards will be proper and appropriate. … The performance of that function would give substance to the notion of ministerial control and responsibility and provide valuable guidance to ASIO.[39]

Acknowledgment that the doctrines of ministerial responsibility and ministerial control underpin the Guidelines is made in the *2017 Independent Intelligence Review* ('*Independent Intelligence Review*'),[40] and also in the *Comprehensive Review of the Legal Framework of the National Intelligence Community* ('*Richardson Review*').[41] Both reviews stress the importance of ministerial control in relation to intelligence agencies.[42]

The effectiveness and importance of ministerial responsibility and ministerial control needs, however, to be considered in the operational context of the work and practices of ASIO. This particular context tempers and influences the circumstances of these accountability doctrines, demanding adjustment and innovation to maximise their efficacy.

The major accountability consideration is the unique circumstances of ASIO activities in contradistinction to other state institutions and departments. The necessary procedures, practices and tradecraft of a domestic intelligence agency such as ASIO are affected by two considerations which make ministerial responsibility and accountability problematic.

The first issue is that a significant proportion of ASIO activities are necessarily conducted in secret, directly impacting upon how a Minister might respond to parliamentary and other questions:

> Since much of the work of intelligence agencies is necessarily secret, many of the traditional means by which the broader community can determine that government agencies are operating in an appropriate manner are not fully applicable to the intelligence community.[43]

---

39 Ibid 321 [16.51].

40 Department of the Prime Minister and Cabinet, Commonwealth, *2017 Independent Intelligence Review* (Report, June 2017) 111 [7.2]–[7.4] <https://www.pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf> ('*Independent Intelligence Review*').

41 Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Report, December 2019) vol 1, 302–5 [14.1]–[14.13], vol 3, 236 [40.1] ('*Richardson Review*').

42 Ibid vol 1, 305 [14.13]–[14.15]; *Independent Intelligence Review* (n 40) 111.

43 *Independent Intelligence Review* (n 40) 111 [7.3].

> This secrecy is in contrast to the transparency and open accountability, which characterises the oversight of the non-intelligence agencies.[44]

Accordingly, distinctive security intelligence ministerial practices have emerged, such as not responding to operational subject matters,[45] claiming plausible deniability,[46] as well as engaging in the practice of neither confirming nor denying the occurrence of events with a national security aspect.[47] These examples adversely affect standard conceptions of ministerial responsibility for ASIO. The challenges to conventional application of the doctrine are tangible in the bipartisan ministerial position of declining to comment in the parliamentary chamber, before parliamentary committees, or in the media, on national security matters, often capaciously defined.[48] That practice is at odds with basic assumptions of ministerial responsibility and accountability.[49]

The second issue arises from the risk of ministerial authority being applied for partisan political advantage and politicisation of security intelligence activities: 'Intelligence agencies must be free from political control. They need to be independent from ministers to ensure the extraordinary powers afforded to them are not used for party political purposes or are subject to departmental administration.'[50]

---

44 *Richardson Review* (n 41) vol 3, 236 [40.3].

45 As favoured by then Minister for Immigration and Border Protection, Scott Morrison, in the implementation of Operation Sovereign Borders under the Abbott Government: David Wroe, 'Veil of Silence Descends on Asylum Boat Arrivals', *The Age* (online, 20 September 2013) <https://www.theage.com.au/politics/federal/veil-of-silence-descends-on-asylum-boat-arrivals-20130920-2u5t5.html>. See also Kaldor Centre for International Refugee Law, *Turning Back Boats* (Research Brief, August 2018) 3.

46 Typically, in the filtering and nuancing of information flows to the Minister from departmental and ministerial officials to facilitate ignorance or ambiguity in the Minister's mind and thereby assist deniability in public accountability fora. See generally Michael Poznansky, 'Revisiting Plausible Deniability' (2022) 45(4) *Journal of Strategic Studies* 511.

47 Known as the Glomar response. See *Philippi v Central Intelligence Agency*, 546 F 2d 1009 (DC Cir, 1976).

48 Standard responses identify the question's content as 'operational matters' or more broadly as 'national security', and neither confirm nor deny its accuracy. The PJCIS is excluded from examining operational matters: see *Intelligence Services Act* (n 15) ss 29(3)(a)–(e). The Intelligence Services Amendment (Enhanced Parliamentary Oversight of Intelligence Agencies) Bill 2018 (Cth) introduced by Senator Rex Patrick sought the removal of restrictions on the PJCIS to review operations of ASIO and other intelligence agencies. This Bill was restored in the notice paper on 4 July 2019, but lapsed again at the end of the 2022 Parliament: Commonwealth, *Notice Paper*, Senate, 4 July 2019, 7.

49 The ministerial practice of declining to comment on national security matters has been discussed in Parliament: Commonwealth, *Parliamentary Debates*, Senate, 4 December 2013, 766 (John Faulkner), 819 (George Brandis).

50 *Richardson Review* (n 41) vol 1, 305 [14.14].

The strengthening of ASIO ministerial control followed the Hope Royal Commissions,[51] and is reflected in the legislated arrangements governing the relationship between the Minister and the Director-General.[52] The qualified capacity of the Minister to direct the Director-General in the performance of ASIO functions reflects efforts to contain or excise risks of political interference or influence within a framework of ministerial control.[53] In particular, the Minister is 'not empowered to override the opinion of the Director-General concerning the nature of the advice that should be given by the Organisation'.[54] Further, the Minister has limited capacity to override the opinion of the Director-General on other matters relating to ASIO's conduct:

> **8 Control of Organisation**
>
> (5) The Minister is not empowered to override the opinion of the DirectorGeneral:
>
> (a) on the question whether the collection of intelligence by the Organisation concerning a particular individual would, or would not, be justified by reason of its relevance to security; or
>
> (b) on the question whether a communication of intelligence concerning a particular individual would be for a purpose relevant to security;
>
> except by a direction contained in an instrument in writing that sets out the Minister's reasons for overriding the opinion of the DirectorGeneral.[55]

Complementary provisions provide further responsibilities for the Director-General:

> **20 Special responsibility of Director-General in relation to functions of Organisation**
>
> The Director-General shall take all reasonable steps to ensure that:

---

51 Particularly relating to ASIO illegalities and improprieties over decades, see: Brian Toohey, *Secret: The Making of Australia's Security State* (Melbourne University Press, 2019); John Blaxland, *The Protest Years: The Official History of ASIO: 1963–1975* (Allen & Unwin, 2015); Peter Edwards, *Law, Politics and Intelligence: A Life of Robert Hope* (NewSouth Publishing, 2020).

52 *ASIO Act* (n 10) s 8.

53 'Subject to subsections (4) and (5), in the performance of the Director-General's functions under this Act, the Director-General is subject to the directions of the Minister': ibid s 8(2).

54 Ibid s 8(4).

55 Ibid s 8(5).

> (a) the work of the Organisation is limited to what is necessary for the purposes of the discharge of its functions; and
>
> (b) the Organisation is kept free from any influences or considerations not relevant to its functions and nothing is done that might lend colour to any suggestion that it is concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions.[56]

These two issues make ASIO ministerial responsibility and accountability inherently problematic, which increases the importance of the Guidelines in effectively reinforcing that framework and ensuring that ASIO practices conform to standards of lawfulness and propriety.

A further issue complicating ASIO ministerial responsibility is the revised ministerial arrangements instituted by the Turnbull Government in 2017. ASIO moved from the Attorney-General's portfolio to the portfolio of the newly created Department of Home Affairs,[57] a development not foreshadowed by the *2017 Independent Intelligence Review*.[58] The change occurred largely due to political factors.[59] However, elements of ASIO's accountability mechanisms — such as its warrant approval process — remain with the Attorney-General.[60] The Minister, in making or varying the Guidelines, must consult with the Attorney-General.[61] The change was justified on the ground that the Attorney-General's portfolio was the proper integrity and accountability portfolio amongst the ministries.[62] This more complicated ministerial accountability model for domestic national security matters risks frustrating ministerial responsibility through ministerial deniability or oscillation between the two portfolios. The Guidelines should explicitly address the dual ministerial role, consistent with the asserted integrity role of the Attorney-General's portfolio.

---

56 Ibid s 20.

57 Malcolm Turnbull et al, 'A Strong and Secure Australia' (Joint Media Release, 18 July 2017). See also Governor-General, *Administrative Arrangements Order* (29 May 2019) 26–7.

58 *Independent Intelligence Review* (n 40).

59 Then Prime Minister Malcolm Turnbull was perceived to have given Peter Dutton this senior portfolio to manage factional tensions and individual ambitions in the parliamentary Liberal Party. See: Geoff Kitney, 'Politics and Policy Meet in New Home Affairs Department', *The Interpreter* (online, 18 July 2017) <https://www.lowyinstitute.org/the-interpreter/politics-and-policy-meet-new-home-affairs-department>; Malcolm Turnbull, *A Bigger Picture* (Hardie Grant Books, 2020) 436–9.

60 *ASIO Act* (n 10) pt 3 div 2; *Home Affairs and Integrity Agencies Legislation Amendment Act 2018* (Cth) sch 2 pt 1.

61 *ASIO Act* (n 10) ss 8A(1A), (2A).

62 Turnbull et al (n 57).

D *The Special Role of the IGIS in Addressing Issues of Ministerial Responsibility for ASIO and the Effectiveness of the Guidelines*

The Guidelines further need optimal formation to enhance the effectiveness of the IGIS, the body legislated to partly address the conundrums of ministerial responsibility arising in national security matters. The Guidelines' status as administratively, but not legally, enforceable, further underlines the critical IGIS role. The integrated role of the IGIS within the model of ministerial responsibility indicates the need for sharper drafting and application of the Guidelines, to ensure continuing relevance for the ever-expanding ASIO legislative remit.

The IGIS is conferred with a series of self-enabled compliance, review and monitoring functions in relation to ASIO.[63] The IGIS is empowered to inquire into any matter that relates to 'the compliance by ASIO with directions or *guidelines* given to ASIO by the responsible Minister'.[64] The IGIS's power to conduct inquiries is extensive,[65] including a power to issue notices to give the IGIS information and documents.[66]

The IGIS has a specific function to assess compliance of ASIO with the Guidelines provided to it by the responsible Minister.[67] From one perspective, the IGIS here performs a substitute role for the Parliament, constrained by its lack of previously mentioned effective ministerial responsibility practices in national security *operational* matters.[68] The IGIS is then able to investigate, measure and determine the level of operational issue compliance with the Guidelines. As observed, 'the ASIO Guidelines provide benchmarks against which the [IGIS] may conduct oversight of ASIO's activities and make findings and advisory recommendations to the Australian Government'.[69] Further, the IGIS is able to report its findings on Guidelines compliance in the *IGIS Annual Report*.[70] This measure allows the IGIS engagement with ASIO to potentially remediate breaches of the Guidelines and the *ASIO Act* through follow up action and reporting in subsequent IGIS annual reports.

---

63 *IGIS Act* (n 16) s 8(1). For the IGIS' role in this accountability framework, see: Ian Carnell and Neville Bryan, 'Watching the Watchers: How the Inspector-General of Intelligence and Security Helps Safeguard the Rule of Law' (2006) 57(1) *Admin Review* 33; Vivienne Thom, 'Reflections of a Former Inspector-General of Intelligence and Security' [2016] (83) *AIAL Forum* 11. For the ASIO special powers regime, see Lisa Burton and George Williams, 'The Integrity Function and ASIO's Extraordinary Questioning and Detention Powers' (2012) 38(3) *Monash University Law Review* 1, 12–17.

64 *IGIS Act* (n 16) s 8(1)(a)(ii) (emphasis added).

65 Ibid s 17.

66 Ibid s 18(1).

67 *ASIO Act* (n 10) s 8A(6).

68 See above nn 45–9 and accompanying text.

69 *Comments on the Minister's Guidelines* (n 12) 4 [4].

70 See, eg, Inspector-General of Intelligence and Security, *2020–2021 Annual Report* (Report, 4 October 2021) 40 ('*IGIS 2020–2021 Annual Report*').

As part of the IGIS scheme ultimately relating to ASIO ministerial responsibility, the IGIS is obliged to provide copies of such reports to the responsible Minister[71] and inquiries by the IGIS relating to ASIO compliance with the Guidelines will appear in the *IGIS Annual Report*.[72] Examples of revealed breaches of the Guidelines are located in each of the *2017–2018*,[73] *2018–2019*,[74] *2019–2020*[75] and *2020–2021*[76] *IGIS Annual Reports*.[77] The placing of information about breached Guidelines in the public domain through the IGIS annual reports makes deliberative information available for parliamentary sittings, parliamentary committees and media commentary. Identifying issues and improvements within the existing Guidelines may assist IGIS accountability capacities through ministerial responsibility, at one step removed.

There are several other IGIS inquiry powers related to ASIO. These include the power to inquire into: 'compliance by ASIO with the laws of the Commonwealth and of the States and Territories';[78] 'the propriety of particular activities of ASIO';[79] 'the effectiveness and appropriateness of the procedures of ASIO relating to the legality or propriety of the activities of ASIO';[80] and 'an act or practice of ASIO that is or may be inconsistent with or contrary to any human right, that constitutes or may constitute discrimination, or that may be unlawful under' one or more of four Commonwealth anti-discrimination acts, 'being an act or practice referred to the [IGIS] by the Australian Human Rights Commission'.[81]

---

71 *Public Governance, Performance and Accountability Act 2013* (Cth) s 46(1). See also *IGIS Act* (n 16) s 35 for obligatory content in the annual report to the responsible minister.

72 *IGIS Act* (n 16) s 35(2A).

73 Inspector-General of Intelligence and Security, *2017–2018 Annual Report* (Report, 24 September 2018) 22–3 ('*IGIS 2017–2018 Annual Report*').

74 Inspector-General of Intelligence and Security, *2018–2019 Annual Report* (Report, 30 September 2019) 33–4 ('*IGIS 2018–2019 Annual Report*').

75 Inspector-General of Intelligence and Security, *2019–2020 Annual Report* (Report, 29 September 2020) 39–40.

76 *IGIS 2020–2021 Annual Report* (n 70) 40.

77 Amongst the breaches of the Guidelines were investigative activities undertaken without proper authorisations, some failures to review investigations on an annual basis, approvals on yearly review for continuation of investigations without sufficient seniority, the disclosure of inaccurate and misleading personal information in relation to Australian status, instances of mistaken identity in security investigations, and providing financial records to ASIO contrary to internal procedures and absent required approvals.

78 *IGIS Act* (n 16) s 8(1)(a)(i).

79 Ibid s 8(1)(a)(iii).

80 Ibid s 8(1)(a)(iv).

81 Ibid s 8(1)(a)(v).

E *The Guidelines as Part of a Broader Accountability Framework: The ASIO Accountability Experience Informing Reform of the Guidelines*

Other rationales for reform of the Guidelines exist in the fact that the Guidelines are properly considered as part of a broader ASIO accountability framework. This extends beyond the IGIS scheme, encompassing other members of the NIC. For ASIO, the most relevant elements of that accountability framework are the PJCIS[82] and the INSLM.[83] The principles and lessons contained in the academic commentary and literature about that ASIO accountability framework offer some *general* guidance around refining the Guidelines.

The Guidelines are properly conceptualised as part of that composite whole, having a distinctive, differentiated, but low-profile accountability role. The Guidelines' characteristics highlight the importance of their revision and development to contribute optimally to a distinctive ASIO ministerial responsibility. This experience may identify common or overlapping issues around ASIO accountability from other sources, as well as more broadly complementing and supporting other ASIO accountability network components.

Contextual information to better shape the Guidelines arises in academic literature around ASIO accountability,[84] including the reviews by the PJCIS and INSLM of ASIO legislation and practice. That literature principally arises as critique and analysis of serial national security legislative enactments, many relating to ASIO, following the September 11 terrorist attacks. Cyber security, espionage, politically motivated violence and foreign interference as contemporary national security topics have been more recently engaged.[85] Further factors usefully informing the content and revision of the Guidelines include recent reforms to, and enlargement

82 *Intelligence Services Act* (n 15) pt 4.

83 *INSLM Act* (n 17) pt 2 div 1.

84 See, eg: Lisa Burton, Nicola McGarrity and George Williams, 'The Extraordinary Questioning and Detention Powers of the Australian Security Intelligence Organisation' (2012) 36(2) *Melbourne University Law Review* 415; Williams, 'The New Terrorists' (n 3); Nicola McGarrity, Rishi Gulati and George Williams, 'Sunset Clauses in Australian Anti-Terror Laws' (2012) 33(2) *Adelaide Law Review* 307; Greg Carne, 'Gathered Intelligence or Antipodean Exceptionalism?: Securing the Development of ASIO's Detention and Questioning Regime' (2006) 27(1) *Adelaide Law Review* 1.

85 See, eg: Julian Lincoln, Anna Jaffe and Lara Howden, 'The Assistance and Access Act: The Controversy Continues' (2019) 21(9) *Internet Law Bulletin* 150; Arthur Kopsias, '"Going Dark": The Unprecedented Government Measures to Access Encrypted Data' [2019] (52) *Law Society Journal* 74; Peter Leonard, 'Australia's Mandatory Decryption Law' (2019) 16(8) *Privacy Law Bulletin* 150, 154; Sarah Kendall, 'Australia's New Espionage Laws: Another Case of Hyper-Legislation and Over-Criminalisation' (2019) 38(1) *University of Queensland Law Journal* 125, 142–61; Hannah Ryan, 'The Constitutional Cost of Combatting Espionage and Foreign Interference' [2018] (47) *Law Society Journal* 73; James Meehan, 'Protecting Public Interest Journalism in Australia: A Defence to Information Secrecy Offences' (2020) 23(4) *Media and Arts Law Review* 347, 352–6.

of, the ASIO legislative remit.[86] Major themes are relevantly identifiable from this ASIO academic literature, affording reasons to guide revision and upgrading of the Guidelines, in order to improve the application of ministerial responsibility, and subsequently improve other ASIO accountability mechanisms. It is convenient to summarise such themes.

The first of these themes is the exponential growth in national security laws and activity since 2001.[87] Major new powers have regularly been conferred on ASIO[88] without an integrated appraisal of how these laws collectively interact.[89] This may produce various security-related effects and potentially transformative consequences for democratic practices and institutions.

The Guidelines operate within a vastly increased quantum of ASIO-related activity[90] and establishment size.[91] Further expanded ASIO activity is likely in two respects. First, the passage of the ASIO Legislation Amendment Bill 2020 (Cth) has expanded the availability of questioning warrants beyond terrorism offences to politically motivated violence, espionage and foreign interference, and made those warrants easier to obtain by removing the independent issuing authority.[92]

---

86 The *Australian Security Intelligence Organisation Amendment Act 2020* (Cth) ('*ASIO Amendment Act*') significantly expanded ASIO questioning powers on matters relevant to security (now extended to politically motivated violence, espionage and foreign interference) and removed independent warrant issuing authorities: at sch 1 pt 1.

87 See, eg: Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge University Press, 2011); Williams, 'A Decade of Australian Anti-Terror Laws' (n 3); Williams, 'The New Terrorists' (n 3); George Williams, 'The Legal Legacy of the "War on Terror"' (2013) 12(1) *Macquarie Law Journal* 3.

88 Major examples of new powers conferred on ASIO under the *ASIO Act* (n 10) include expanded questioning powers and special intelligence operations powers, as well as extensions to ASIO's telecommunications interception powers and access to metadata.

89 The ad hoc and exponential accretion of laws, often a reactive and politicised response to real or perceived terrorism threats, has rarely engaged laws' interactivity — for example, interactions between separate terrorism-related detention provisions enacted for criminal prosecution, intelligence gathering, pre-emptive prevention, post-sentence expiration, and immigration purposes.

90 Reflected in serial amendments to the *ASIO Act* (n 10) since 2001, including pt III div 2 (Special Powers), pt III div 3 (Special Powers Relating to Terrorism Offences) and pt III div 4 (Special Intelligence Operations). See *Richardson Review* (n 41) vol 4, annex B.

91 Sally Neighbour, 'Hidden Agendas', *The Monthly* (online, November 2010) <https://www.themonthly.com.au/issue/2010/november/1289174420/sally-neighbour/hidden-agendas#mtr>; *Richardson Review* (n 41) vol 1, 267; Australian Security Intelligence Organisation, *ASIO Annual Report 2019–2020* (Report, 21 September 2020) 118–21.

92 The Bill was subject to a PJCIS report: Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Australian Security Intelligence Organisation Amendment Bill 2020* (Report, December 2020). The Bill passed the Commonwealth Parliament on 10 December 2020: Commonwealth, *Parliamentary Debates,* House of Representatives, 10 December 2020, 11284.

Second, the public release and prospective implementation of the *Richardson Review* will likely liberalise and harmonise the powers of the NIC (of which ASIO is part).[93] Critical appraisal of the coverage and efficacy of the Guidelines is desirable given the transformative character of these developments.

Second, these developments have created a significantly greater reliance on executive or ministerial *discretion* in the equitable administration of ASIO laws.[94] Those realities speak clearly to the need for more comprehensive Guidelines across the range of ASIO activities[95] *as relevant to security*, including an improved process for revision to keep pace with ongoing changes to ASIO legislation.[96] The Guidelines need to illuminate greater transparency of principles where the exercise of discretion in decisions arises around ASIO's powers *relevant to security*. Presently, the Guidelines are not calibrated to the volume nor seriousness of serially legislated ASIO security subject matters, nor to the levels of ministerial discretion embedded in them.

Third, parallel to the ongoing revision and expansion of the ASIO remit have been the constant process and substance efforts required to obtain adequate legislated checks and balances upon such expansion,[97] principally evident in parliamentary

93 *Richardson Review* (n 41); Carne, 'Designer Intelligence or Legitimate Concern?' (n 5).

94 Carne, 'Sharpening the Learning Curve' (n 15) 1, 24, 40. The claim that executive discretion is a desirable safeguard runs contrary to the fact that the executive's interests do not consistently coincide with the public interest: Greg Carne, 'Beyond Terrorism: Enlarging the National Security Footprint through the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011 (Cth)*' (2011) 13(2) *Flinders Law Journal* 177, 227–8.

95 The *2020 Guidelines* (n 1) are notable for omitting discrete ASIO activity areas: *Comments on the Minister's Guidelines* (n 12) 6–7.

96 The pace of national security legislative reform is fuelled by the urgency principle: Andrew Lynch, 'Legislating Anti-Terrorism: Observations on Form and Process' in Victor V Ramraj et al (eds), *Global Anti-Terrorism Law and Policy* (Cambridge University Press, 2nd ed, 2012) 151, 166–82; Andrew Lynch, 'Legislating with Urgency: The Enactment of the *Anti-Terrorism Act [No 1] 2005*' (2006) 30(3) *Melbourne University Law Review* 747, 767–75; Shawn Rajanayagam, 'Urgent Law Making and the Human Rights (Parliamentary Scrutiny) Act' in Julie Debeljak and Laura Grenfell (eds), *Law Making and Human Rights: Executive and Parliamentary Scrutiny across Australian Jurisdictions* (Lawbook, 2020) 647, 655–6. Repeated ministerial commitments to constantly review terrorism laws further propels legislative activity: Carne, 'Reviewing the Reviewer' (n 15) 344–6, 376.

97 This is evidenced in the generally modest uptake in report recommendations of suggested improvements and reforms from detailed submissions made by various bodies and expert individuals to the PJCIS. For example, following low uptake of suggested improvements in recommendations in the PJCIS' Inquiry into the Australian Security Intelligence Bill 2020 (Cth), legislative amendments were passed in the *ASIO Amendment Act* (n 86), which significantly extended ASIO questioning powers and removed independent warrant issuing authority safeguards.

committee review processes.[98] The ASIO accountability literature highlights important issues regarding methodologies and deficiencies, the legislative process, review of legislation and adoption of review committee recommendations in relation to ASIO matters.[99] The Guidelines' formation and content needs to avoid replicating in microcosm such legislative process difficulties. Drawing from the ASIO legislative review experience, clear measures can be taken, including: wider exposure to analysis and critique from different expert sources (and acknowledgment of their legitimacy); greater Guidelines coverage; and greater receptivity to instituting checks and balances. These measures are preferable to the present narrowly conceived, Minister approved and departmentally derived Guidelines.[100]

Fourth, the enlargement of the ASIO mandate has occurred without the tempering effect of a statutory or constitutional charter of rights.[101] Preference is for reliance

98 Legislative amendments to the *ASIO Act* are principally reviewed by the PJCIS. Other review is conducted by the Parliamentary Joint Committee on Human Rights ('PJCHR'), and formerly (prior to the Abbott Government) the Senate Legal and Constitutional Affairs Committee. Positioning of the PJCHR as inferior to the PJCIS is evident in several examples: Carne, 'Sharpening the Learning Curve' (n 15) 367–76.

99 The effectiveness of parliamentary committee review is appraised differently by different commentators. See, eg: Dominique Dalla-Pozza, 'A Dual Scrutiny Mechanism for Australia's Counter-Terrorism Law Landscape: The INSLM and the PJCIS' in Julie Debeljak and Laura Grenfell (eds), *Law Making and Human Rights: Executive and Parliamentary Scrutiny across Australian Jurisdictions* (Lawbook, 2020) 673; Dominique Dalla-Pozza,'The Parliamentary Joint Committee on Intelligence and Security: A Point of Increasing Influence in Australian Counter-Terrorism Law Reform?' in Ron Levy et al (eds), *New Directions for Law in Australia: Essays in Contemporary Law Reform* (ANU Press, 2017) 397; Carne, 'Sharpening the Learning Curve' (n 15); Carne, 'Reviewing the Reviewer' (n 15); Sarah Moulds, 'Forum of Choice? The Legislative Impact of the Parliamentary Joint Committee of Intelligence and Security' (2018) 29(4) *Public Law Review* 287; Sarah Moulds, 'Committees of Influence: Parliamentary Committees with the Capacity to Change Australia's Counter-Terrorism Laws' (2016) 31(2) *Australasian Parliamentary Review* 46.

100 Formally, the 'Guidelines are given by the Minister for Home Affairs to the Director-General under subsections 8A(1) and 8A(2) of the ASIO Act': *2020 Guidelines* (n 1) 4 [1.1].

101 National Human Rights Consultation Committee, *National Human Rights Consultation Report* (Report, September 2009) xxxiv, recommendation 18 ('*Brennan Report*'). The Rudd Government declined the recommended implementation of a statutory rights charter: Robert McClelland, *The Protection and Promotion of Human Rights in Australia* (October 2009) 4 <http://web.archive.org/web/20110312104038/http://www.attorneygeneral.gov.au/www/ministers/RWPAttach.nsf/VAP/(3273BD3F76A7A5DEDAE36942A54D7D90)~091008_NHRC_Statement.pdf/$file/091008_NHRC_Statement.pdf> ('*The Protection and Promotion of Human Rights in Australia*'); David Erdos, 'The Rudd Government's Rejection of an Australian Bill of Rights: A Stunted Case of Aversive Constitutionalism?' (2012) 65(2) *Parliamentary Affairs* 359, 359–60.

upon parliamentary processes, committees,[102] and statutory appointments[103] as the mechanism of human rights protection.[104] The absence of a charter of rights highlights that the Guidelines are conceptualised and located within the Australian parliamentary-based model of human rights protection,[105] institutionally encompassing a ministerial responsibility doctrine. A rationale for rejecting a statutory charter or constitutional bill of rights is that Parliament is the most institutionally proper, effective and politically representative method of rights protection.[106] That choice carries a logical corollary that the Guidelines need drafting to deliver optimal performance within that selected parliamentary-based model, including ministerial responsibility.

The Guidelines importantly function within the Parliamentary-based model to provide public reassurance and confidence of the legality and propriety of ASIO's activities.[107] The Guidelines formally but pragmatically express the legal relationship between the Minister and the Director-General regarding the performance by

---

102 This included the establishment of the PJCHR to review legislation for compatibility with Australia's seven major international human rights covenants: *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) s 3 (definition of 'human rights'). For assessment of the PJCHR's work, see: Zoe Hutchinson, 'The Role, Operation and Effectiveness of the Commonwealth Parliamentary Joint Committee on Human Rights after Five Years' (2018) 33(1) *Australasian Parliamentary Review* 72; George Williams and Daniel Reynolds, 'The Operation and Impact of Australia's Parliamentary Scrutiny Regime for Human Rights' (2018) 41(2) *Monash University Law Review* 469.

103 For example, the specialist Australian Human Rights Commission appointments under s 8(1) of the *Australian Human Rights Commission Act 1986* (Cth).

104 Initially this was in the form of a National Human Rights Framework, which implemented limited aspects of the *Brennan Report* (n 101): see Robert McClelland, 'Australia's Human Rights Framework' (Media Release, 21 April 2010); Robert McClelland, 'Enhancing Parliamentary Scrutiny of Human Rights' (Media Release, 2 June 2010). This position was maintained in Australia's 2021 United Nations Universal Periodic Review before the Human Rights Council: Human Rights Council, *National Report Submitted in Accordance with Paragraph 5 of the Annex to Human Rights Council Resolution 16/21: Australia*, UN Doc A/HRC/WG.6/37/AUS/1 (28 December 2020).

105 George Williams and Lisa Burton, 'Australia's Exclusive Parliamentary Model of Rights Protection' (2013) 34(1) *Statute Law Review* 58; Williams and Reynolds (n 102).

106 Australian rights charter opponents favour this argument: James Allan, 'Human Rights: Can We Afford To Leave Them to the Judges?' (2005) 16(2) *Commonwealth Judicial Journal* 4; James Allan, 'Bills of Rights as Centralising Instruments' (2006) 27(1) *Adelaide Law Review* 183; James Allan, 'Oh That I Were Made Judge in the Land' (2002) 30(3) *Federal Law Review* 561.

107 The contested issue of public trust of intelligence activities is raised in relation to the *Australian Security Intelligence Organisation Amendment Bill 2020* (Cth): 'ASIO Bill Highlights Why the Government Has a Problem with Public Trust', *Digital Rights Watch* (Web Page, 27 May 2020) <https://digitalrightswatch.org.au/2020/05/27/asio-bill-highlights-government-trust-problem/>.

ASIO of its functions and the exercise of its powers including its functionality as an aspect of representative government. In fulfilling this role, the drafting of the Guidelines should provide accessible, practical and contemporary guidance over the *full scope* of the security referenced functions in s 17 of the *ASIO Act*, including restraints upon such functions implemented by s 17A of the *ASIO Act*.[108]

Each of these four themes, summarised from the ASIO accountability literature, provide important rationales to refine ASIO accountability mechanisms along more integrated and synchronous lines, commencing with the Guidelines. These reasons clearly justify highlighting the selected major Guidelines' shortcomings, with the ultimate aim of increasing the effectiveness of the doctrine of ministerial responsibility underpinning the Guidelines. Consistent with that aim, the article now critically appraises *selected key features* of the Guidelines requiring improvement. The review, content and operation of the Guidelines requires attention around the following priority items so that the Guidelines can evolve into a more effective ministerial responsibility mechanism.

III Selected Guidelines Features: Review Processes, Content and Operation To Strengthen Ministerial Responsibility

A *The Guidelines Do Not Always Provide Guidance: The Significant Role of Maintained and Classified ASIO Policies Made under the Guidelines' Authority*

An emergent problem facing the Guidelines has been one of fidelity to the original concepts of ministerial direction, responsibility and accountability. It has been difficult to crisply encapsulate these in a unique, statutorily mandated document,[109] providing operational accessibility for daily security-related activities.[110] The *2020 Guidelines* now extend to 21 pages, reflecting the new ministerial bifurcation of responsibilities between the Department of Home Affairs and the Attorney-General's Department, alongside the vast post-2001 growth of ASIO's legislated activities.[111] The *2007 Guidelines*[112] combined statutory obligations relating to the

108 Section 17A of the *ASIO Act* (n 10) provides that the 'Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly'.

109 Note also the ministerial obligation to give written notice to the Director-General regarding politically motivated violence Guidelines: ibid s 8A(2).

110 This was probably contemplated in Hope J's recommendation that the Attorney-General should be able to issue guidelines governing ASIO's activities: *Second Hope Royal Commission Report* (n 18) 321 [16.51]–[16.52].

111 See above n 3 and accompanying text. See also Christian Porter, 'Attorney-General Welcomes Committee Report on Espionage and Foreign Interference Bill' (Media Release, 7 June 2018).

112 *2007 Guidelines* (n 2).

obtaining of intelligence relevant to security and for politically motivated violence into a single 11-page publication.

More importantly, the *2020 Guidelines* rely in two primary examples upon references to maintaining internal policies (in the form of an additional document): (1) the use of authorised force under an ASIO warrant against a person;[113] and (2) ASIO access to, and retention of, personal information.[114] A third example exists in the obligation to maintain policies in respect of para 3.5 of the *2020 Guidelines*.[115]

Maintaining such internal policies raises an inherent conundrum around the conceptual integrity of the Guidelines. The Guidelines collide at an early point with standard national security practices of not disclosing operational matters, intelligence techniques, or tradecraft. The Guidelines in the two primary mentioned areas realistically are minimalist exercises. The Guidelines' function as a visible, public accountability reassurance mechanism is in tension with the practice of not making public (even in part) information of how internal ASIO controls are drafted and actioned. Such tension should be preferably candidly acknowledged, to alert, inform and shape effective accountability responses. Alongside that acknowledgment, it is of paramount importance for the IGIS to be fully informed and adequately resourced to enable regularly scheduled reviews of these two primary matters — to discharge *in camera* its extensive powers, reporting publicly, as linked to ministerial responsibility.[116]

In other words, limits upon the direct application of ministerial responsibility need clarity in relation to how, and to what extent, at one step removed (in the form of maintained and classified ASIO policies) ministerial responsibility is maintained or contested, including in IGIS interactions. Importantly, such measures will encourage a realistic public appreciation of how effectively the Guidelines underpin ministerial responsibility.

Further, the *2020 Guidelines* as an ASIO accountability measure need reconceptualisation as a composite: comprising public Guidelines and undisclosed internal policies made under the Guidelines authority. This substantiality of internal policies carries distinctive risks. First, the emergence of executive discretion exercised within those policies, which is at variance with the import of the Guidelines. Second, the policies by default practice becoming the practical operational document for the

113 *2020 Guidelines* (n 1) 10 [2.13]–[2.15].

114 Ibid 13–14 [4.3].

115 Where the Director-General is considering requesting assistance to ASIO under s 21A of the *ASIO Act* (assistance provided in accordance with a request by the Director-General) or pt 15 of the *Telecommunications Act 1997* (Cth) 'in circumstances where a civil or criminal immunity could arise, proportionality must be considered. In determining proportionality, the Director-General should consider the seriousness of any offence or conduct to which the immunity may apply and the impact on innocent parties': ibid 12 [3.5].

116 See above Part II(D).

organisation, being not necessarily synchronous with the Guidelines, nor consistent with a plain reading of the parent *ASIO Act*.

The necessary generality of the *2020 Guidelines* in the two primary examples mentioned above is evident in their language and structure.

In relation to authorised force under an ASIO warrant against a person:

> **Use of force against the person under warrant**
>
> 2.13 The Director-General will take all reasonable steps to ensure that persons, including ASIO employees, who are authorised to use force against a person under an ASIO warrant are appropriately trained.[117]
>
> 2.14 The Director-General is entitled to presume that the following categories of persons are appropriately trained:
>
> a) Sworn members of the Australian Federal Police, or of a police force of a State or Territory.
>
> b) Other Commonwealth, State and Territory officials, who would ordinarily be expected to use force as part of their duties.[118]
>
> 2.15 ASIO will maintain policies in respect of paragraphs 2.13 and 2.14.[119]
>
> 2.16 Section 2.13 does not limit the inherent right of an ASIO employee or ASIO affiliate to self-defence.[120]

In relation to ASIO access to and treatment of personal information, 'personal information' is generously defined:

> "**personal information**" means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> a) whether the information or opinion is true or not; and
>
> b) whether the information or opinion is recorded in material form or not.[121]

---

117 *2020 Guidelines* (n 1) 10 [2.13]. This is obviously a statement of broad generality, with the Organisation itself making a self-determination of what constitutes appropriate training.

118 Ibid 10 [2.14].

119 Ibid 10 [2.15].

120 Ibid 10 [2.16]. This clearly contemplates the use of force capacities conferred by ASIO warrant authority as distinctive from rights of self-defence under statute or at common law.

121 Ibid appendix 1.

Personal information therefore need not be factually accurate, it can be simply an opinion. It need not be reduced to a recorded form (in any of the myriad ways of recording) and the matching of such 'information' or 'opinion' need not be identity proven, but simply ascribable to 'an individual who is reasonably identifiable'. From one perspective, the definition of personal information in the Guidelines, copying the definition from the *Privacy Act 1988* (Cth) ('*Privacy Act*')[122] and the Australian Privacy Principles,[123] *might* create circumstances offering broader protection and legal consistency with other bodies. On the other hand, the breadth of the definition of personal information is particularly sensitive, as it applies to the distinctive context of gathering intelligence relevant to security, that is intelligence, and not factually accurate information. This is a complex question ultimately turning upon the efficacy of the Guidelines in facilitating ministerial responsibility for the processing and deletion of information that never was, or no longer is, of relevance to security, and in preventing information misuse.

Statements of broad generality open pt 4 of the *2020 Guidelines*, titled 'Treatment of Personal Information':

> 4.1 ASIO will only collect, use, handle, retain or disclose personal information for purposes related to the performance of its functions or exercise of its powers, or where otherwise authorised, or required, by law.[124]
>
> 4.2 The Director-General will take all reasonable steps to ensure that ASIO's collection, retention, use, handling and disclosure of personal information is limited to what is reasonably necessary to perform its functions. This includes having reasonable controls to prevent the collection and processing of information in breach of a warrant or statutory authority, and procedures for appropriate remediation and reporting should this occur.[125]
>
> 4.3 ASIO will maintain policies about its access to, and retention of, personal information.
>
> a) These policies must provide clear guidance on:
>
> i. the type of personal information ASIO collects and retains
>
> ii. how ASIO should collect, hold, retain, protect and access personal information
>
> iii. the circumstances and associated requirements around the de-identification of personal information

122 *Privacy Act 1988* (Cth) s 6 (definition of 'personal information') ('*Privacy Act*').

123 Ibid sch 1.

124 *2020 Guidelines* (n 1) 13 [4.1].

125 Ibid 13 [4.2].

> iv. the purposes for which ASIO may collect, hold, retain, use, access and disclose personal information
>
> v. the disclosure of information overseas, including its effect on individual privacy interests
>
> vi. processes for periodic review of its holdings, including personal information, to determine whether retention is reasonable, and
>
> vii. setting, reviewing and undertaking disposal actions in accordance with the ASIO Records Authority and any other Commonwealth recordkeeping directives or legislative requirements.[126]

Paragraph 4.3(b) of the *2020 Guidelines* creates other requirements for ASIO around the use of 'personal information':

> b) These policies must require ASIO to:
>
> i. ensure that it retains personal information only:
>
> a. when it is relevant to the proper performance of its functions or the exercise of its powers, or
>
> b. where otherwise authorised, or required, by law
>
> ii. ensure only ASIO employees and ASIO affiliates who require access to data and information, which may include reference data, for the proper performance of their duties are authorised to do so;
>
> iii. maintain internal audit mechanisms which provide assurance that ASIO employees and ASIO affiliates who are authorised to access data and information, which may include reference data, do so only for the proper performance of their duties; and
>
> iv. report to the IGIS any collection of, or access to, data which may include reference data, which are inconsistent with, or in contravention of legislation.[127]

The opening statement at para 4.2 of the *2020 Guidelines* obliging the Director-General to 'take all reasonable steps ensuring that ASIO's collection, retention, use, handling, and disclosure of personal information is limited to what is reasonably necessary

126 Ibid 13 [4.3(a)].

127 Ibid 13–14 [4.3(b)].

to perform its functions'[128] is drafted in overtly objective terms, but organisationally interpretable to be consistent with internalised and institutionalised national security norms. The broadly descriptive terms, and the use of words 'reasonable' and 'reasonably', import a nominally objective, but executive determined element into the personal information interactions. The further inclusion of reasonable controls to prevent the collection and processing of information in breach of a warrant or statutory authority, and procedures (in that event) for appropriation, remediation and reporting of such breaches, impresses an expansive executive scope.

The practical effect is that para 4.2 of the *2020 Guidelines* minimises public obligatory content, as the substantive regulatory framework of ASIO is framed by the para 4.3 obligation — that is to maintain policies about access to, and retention of, personal information, the content of the policies having to provide 'clear guidance' on listed items (i) to (vii). The bulk of the regulatory framework, and its responsiveness to the listed issues, is invisible to public scrutiny. The public scrutiny arises through proxy by the IGIS, becoming public if and when the IGIS publishes details relating to the treatment of personal information[129] in an annual report.[130] It is therefore important to scrutinise the positively presented adoption of the *Privacy Act* language (wherever it might arise) against concrete experience.

Two illuminating experiential points arise. In contrast to the Guidelines, in the case of ASIS, AGO and ASD, the relevant responsible Minister in discharging the obligation to make rules regulating the privacy — the communication and retention of such intelligence information concerning Australian persons — is under *three obligations*: (1) to consult the IGIS;[131] (2) to provide the IGIS a copy of the proposed rules;[132] and (3) for the IGIS to brief the PJCIS on the rules if requested, or if the rules change.[133] This places the IGIS in a stronger position, early and subsequently, for the non ASIO agencies to facilitate ministerial responsibility, in contrast to the Guidelines position.[134] Second, several significant breaches of the ASIO guidelines in relation to investigative activity and personal information were previously identified by the IGIS.[135]

---

128 Ibid 13 [4.2].

129 The policy requires ASIO to 'report to the IGIS any collection of, or access to, data, which may include reference data, which are inconsistent with, or in contravention of legislation': ibid 14 [4.3(b)(iv)]. The accompanying note to this paragraph of the *2020 Guidelines* further advises that '[t]his section of the Guidelines does not apply to ASIO's corporate business information or data' and '[u]nder the *Inspector-General of Intelligence and Security Act 1986*, the IGIS may review access by ASIO employees and ASIO affiliates to data and information': at 14. See also *IGIS Act* (n 16) s 8(1)(a).

130 See: *IGIS 2017–2018 Annual Report* (n 73) 22–3; *IGIS 2018–2019 Annual Report* (n 74) 33–4.

131 *Intelligence Services Act* (n 15) s 15(3)(c).

132 Ibid s 15(4).

133 Ibid s 15(6)(b).

134 *ASIO Act* (n 10) s 8A.

135 *IGIS 2017–2018 Annual Report* (n 73) 43.

Other limitations of the *2020 Guidelines* need further consideration in assessing their effectiveness. The ensuing para 4.4 of the *2020 Guidelines* includes matters relating to security and access to personal information holdings. In this paragraph, there is simply directive content to the Director-General, rather than an obligation to maintain a policy. The structural minimalism is again likely intended to avoid disclosure of operational and internal methods:

> 4.4 Where ASIO retains personal information, the Director-General will ensure that:
>
> a) the information is protected, by such safeguards as are reasonable in the circumstances, against:
>
> i. loss
>
> ii. unauthorised access, use, modification or disclosure, and
>
> iii. other misuse or interference,
>
> b) access is limited to those ASIO employees or ASIO affiliates who require it for the performance of their roles and functions, consistent with the ASIO Act, ASIO Code of Conduct and ASIO's security and information management policies, and
>
> c) access is available to the IGIS and authorised IGIS staff, in the performance of their functions.[136]

The Director-General's obligation to ensure the content of para 4.4 reflects the bare structural arrangements of control of the Organisation by the Director-General,[137] subject to the IGIS review powers for Guidelines compliance.[138] Other measures augment this arrangement. These measures include: the obligation of providing the IGIS as soon as practicable with a copy of the Guidelines;[139] the tabling of the Guidelines in Parliament;[140] the obligation to provide the Leader of the Opposition with a copy of the Guidelines;[141] and the obligation to provide a copy to the PJCIS, unless considered by the Minister inappropriate to do so.[142]

Overall, the Guidelines' arrangements for the treatment of personal information spotlight significant limits as an accountability device. Much is reliant upon the

136 *2020 Guidelines* (n 1) 14 [4.4].

137 *ASIO Act* (n 10) s 8(1).

138 See *IGIS Act* (n 16) s 8(1)(ii).

139 *ASIO Act* (n 10) s 8A(6).

140 Ibid ss 8A(3)–(4).

141 Ibid s 8A(4).

142 Ibid s 8A(6).

qualitative nature of reporting and supervisory lines between the Minister and Director-General, and the good faith of the Director-General in conforming to both the directive paragraphs and paragraphs requiring implementation of undisclosed policies. The ability to monitor and confirm such adherence ultimately depends upon the legislated level of involvement, resourcing and priorities of the IGIS. This aspect of the treatment of personal information demonstrates that the Guidelines are an important and pragmatically focused accountability mechanism, albeit with substantial limitations. The practical connection with ministerial responsibility is contingent and contained. These limitations, unpacked above, are neither publicly articulated nor appreciated. The inherent limitations of the Guidelines logically demand that other ASIO accountability framework components compensate and balance through influencing better drafting of the Guidelines. Enhanced efficacy of these other accountability roles, including operational optimisation is a practical contribution to redressing limitations and improving ministerial responsibility.

B *Relevance to Security: The Special Case of Politically Motivated Violence, Extending and Expanding Relevance to Security by the Operation of the Guidelines*

The content of ASIO's functions is organised around the concept of relevance to security,[143] broadly defined.[144] Several of these security listed elements are separately and expansively defined.[145] The legislative definition of 'security' capaciously applies to the three initial ASIO functions in ss 17(1)(a)–(c) of the ASIO Act.[146] Significantly, the Guidelines further extend the practical meaning of security, linked to these three initial examples of security relevance. The Guidelines' capacity, conceived as a mechanism of ministerial responsibility, to instead increase the reach of aspects of relevance to security, is anomalous and needs clarification. It is inconsistent with the original Guidelines conception of accountability and constraint. It confirms the need for stronger Guidelines consultation and review processes,[147] to ensure closer adherence to first principles of ministerial responsibil-

---

143 See ibid s 17(1):

> The functions of the Organisation are:
>
> (a) to obtain, correlate and evaluate intelligence relevant to security;
>
> (b) for purposes relevant to security, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes;
>
> (c) to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are *relevant to* their functions and responsibilities … (emphasis added).

144 Ibid s 4 (definition of 'security').

145 See definitions in ibid s 4 in relation to several components of security, namely politically motivated violence (which subsequently incorporates a further definition of 'terrorism offence'), promotion of communal violence, attacks on Australia's defence system, and acts of foreign interference.

146 See above n 143 and accompanying text.

147 See above Part II(B).

ity, with more tightly defined items relevant to security, instead of a mechanism to enlarge executive based discretion. Intelligence practices also must allow latitude (in the sense of preliminary, precursor and preparatory information) for effective obtaining, correlating and evaluating intelligence relevant to security,[148] but that should be clearly circumscribed.

The Guidelines' practical extension of the meaning of security arises most sharply in the example of politically motivated violence.[149] The history of ASIO's interactions with political protest and dissent[150] led to the 1977 and 1984 Hope Royal Commission reforms. This is a timely reminder against the weakening of the accountability framework, for example, by Guidelines' changes interacting with *ASIO Act*'s changes. The concept of politically motivated violence post-Hope Royal Commission became the marker in security activities of what would properly constitute legitimate political expression and dissent.[151] The Guidelines in the politically motivated violence example have tilted towards enlarging the scope of ministerial authority and ASIO activities in their application of relevance to security.

Politically motivated violence comprises five distinctive elements.[152] These elements traverse a range of violent and potentially violent activity, to which the Guidelines apply. The elements are:

> ***politically motivated violence*** means:
>
> (a) acts or threats of violence or unlawful harm that are intended or likely to achieve a political objective, whether in Australia or elsewhere, including acts or threats carried on for the purpose of influencing the policy or acts of a government, whether in Australia or elsewhere;[153] or
>
> (b) acts that:
>
> (i) involve violence or are intended or are likely to involve or lead to violence (whether by the persons who carry on those acts or by other persons); and

148 *ASIO Act* (n 10) s 17(1)(a).

149 See ibid s 4 (definition of 'security' para (a)(iii)). Politically motivated violence is one of the security elements.

150 See: Blaxland (n 51); Frank Cain, 'Australian Intelligence Organisations and the Law: A Brief History' (2004) 27(2) *University of New South Wales Law Journal* 296.

151 Carne, 'Thawing the Big Chill' (n 8) 379, 413–16.

152 *ASIO Act* (n 10) s 4 (definition of 'politically motivated violence' paras (a)–(d)).

153 Ibid s 4 (definition of 'politically motivated violence' para (a)). The political objective refers to an objective anywhere in the world, with the 'acts or threats including those carried on for the purpose of influencing the policy or acts of a government, whether in Australia or elsewhere'.

> (ii) are directed to overthrowing or destroying, or assisting in the overthrow or destruction of, the government or the constitutional system of government of the Commonwealth or of a State or Territory;[154] or
>
> (ba) acts that are offences punishable under Subdivision A of Division 72, or Part 5.3, of the *Criminal Code*;[155] or
>
> (c) acts that are offences punishable under Division 119 of the *Criminal Code*, the *Crimes (Hostages) Act 1989* or Division 1 of Part 2, or Part 3, of the *Crimes (Ships and Fixed Platforms) Act 1992* or under Division 1 or 4 of Part 2 of the *Crimes (Aviation) Act 1991*;[156] or
>
> (d) acts that:
>
> (i) are offences punishable under the *Crimes (Internationally Protected Persons) Act 1976*;[157] or
>
> (ii) threaten or endanger any person or class of persons specified by the Minister for the purposes of this subparagraph by notice in writing given to the Director-General.[158]

The *2020 Guidelines* reduce and remove the preparatory, descriptive and discursive content of the *2007 Guidelines*.[159] The 2007 content provided useful guidance in applying criteria for the obtaining, correlating and evaluating of intelligence relevant to politically motivated violence. In particular, this content constructively included restraining, triaging and prioritising mechanisms. Prominent examples (removed from the comparable section of the *2020 Guidelines*) are:

> 3.5 ASIO is not required to inquire into every instance, actual or potential, of [politically motivated violence]. The Director-General must always make a judgment as to the potential seriousness of any matter or information, the Organisation's priorities, and available resources.[160]

154 Ibid s 4 (definition of 'politically motivated violence' paras (b)(i)–(ii)).

155 Ibid s 4 (definition of 'politically motivated violence' para (ba)). However, a person can commit a terrorism offence against pt 5.3 of the *Criminal Code Act 1995* (Cth) even if no terrorist act (as defined in that part) occur: see *Criminal Code Act 1995* (Cth) pt 5.3.

156 *ASIO Act* (n 10) s 4 (definition of 'politically motivated violence' para (c)).

157 Ibid s 4 (definition of 'politically motivated violence' para (d)(i)).

158 Ibid s 4 (definition of 'politically motivated violence' para (d)(ii)).

159 This content prefaced the individual sub-paragraph descriptions in the *2007 Guidelines* (n 2), comprising one and two thirds content pages in small typeface.

160 Ibid [3.5].

> 3.6 In deciding whether to conduct an investigation and the investigatory methods to be employed, the Director-General shall consider all of the circumstances, including —
>
> (a) the magnitude of the threatened or perceived violence or harm;
>
> (b) the likelihood it will occur;
>
> (c) the immediacy of the threat; and
>
> (d) the privacy implications of any proposed investigation.[161]
>
> …
>
> 3.9 The gravity of risk to security will be a factor in determining the investigative techniques that are appropriate where an investigation is decided upon. Where, for example, there is little information to indicate that serious acts of politically motivated violence are in prospect, the degree of intrusion into individual privacy should, so far as is practicable consistent with resolution of the investigation, be limited.[162]

Elsewhere, the relevant preparatory, descriptive and discursive content of the *2007 Guidelines* has been absorbed into the *2020 Guidelines*, with changes made in the latter to increase ASIO investigative activities. For example, para 3.12(a) in the *2007 Guidelines* stated that 'ASIO is not to make inquiries into demonstrations or other protest activity unless (a) there is a risk of serious premeditated violence for the purpose of influencing government acts or policy …'.[163] This paragraph is relaxed in the *2020 Guidelines*, now stating 'there is a risk of pre-meditated use of violence against persons or property for the purposes of achieving a political objective, or pre-meditated use of tactics that can be reasonably assessed as likely to result in violence …'.[164]

The same contrast emerges between the *2007 Guidelines* and the *2020 Guidelines*, in relation to para (a) of the definition of politically motivated violence. Both versions include prioritising ASIO activities 'to persons or groups likely to be involved in: (a) acts or threats of serious violence or unlawful harm designed to provoke violent reaction …'.[165] However, the *2020 Guidelines* go further, including as an alternative, 'the use of tactics that can reasonably be assessed as likely to result in violence'.[166]

---

161 Ibid [3.6(d)].

162 Ibid [3.9].

163 Ibid [3.12(a)].

164 *2020 Guidelines* (n 1) 20 [5.18(a)].

165 Ibid. See also *2007 Guidelines* (n 2) [2.2(b)(i)].

166 *2020 Guidelines* (n 1) 18 [5.4(b)].

Changed circumstances and experiential evidence from the 13 years of operation of the *2007 Guidelines* may justify a more relaxed and liberalised interpretation. Unfortunately, the reasons substantiating change are neither publicly accessible nor justified. This indicates confusion over the Guidelines' roles of ministerial responsibility and ministerial accountability. These changes to the Guidelines may be precursors and enablers for the expanded ASIO questioning warrants, which now include politically motivated violence.[167] These measures significantly ease the availability of questioning warrants as being relevant to security,[168] especially with the legislative deletion of an independent issuing authority.[169]

A further feature of the Guidelines' politically motivated violence aspect arises at the junction of political protest and political communication. Section 17A of the *ASIO Act*'s foundational principle states:

> **17A Act not concerned with lawful dissent etc.**
>
> This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.[170]

Section 17A of the *ASIO Act* is referred as an operational meaning in the Guidelines, forming the perimeter of ASIO activities:[171]

> 5.17 ASIO is not to undertake investigations where the only basis for the investigation is the exercise of a person's right of lawful advocacy, protest or dissent (section 17A of the ASIO Act).[172]

The prefacing wording of s 17A of the *ASIO Act* in the *2020 Guidelines* points to other possible situations.[173] These situations might arise in parallel, differentiated circumstances to those of lawful advocacy, protest and dissent; where ambivalence exists around the nature of activity as constituting lawful advocacy, protest and dissent; and further, the intersection of political protest and communication with

---

167 See *ASIO Amendment Act* (n 86) ss 34B, 34AD(1).

168 In interpretations of politically motivated violence relating to activist groups: see Daniel Hurst, 'Asio Boss Denies Expanded Powers Could Be Used to Target Black Lives Matter Protesters', *The Guardian* (online, 10 July 2020) <https://www.theguardian.com/australia-news/2020/jul/10/asio-boss-denies-expanded-powers-could-be-used-to-target-black-lives-matter-protesters>.

169 *ASIO Amendment Act* (n 86). See above Part II(E) regarding deletion of the independent issuing authority for ASIO questioning warrants.

170 *ASIO Act* (n 10) s 17A.

171 Ibid s 20 provides a further administrative constraint on performance of ASIO functions.

172 *2020 Guidelines* (n 1) 20 [5.17].

173 See also ibid 5 [1.10].

politically motivated violence, drawing in preliminary, exploratory investigative ASIO activity.[174] The modification of the *2007 Guidelines* content in the *2020 Guidelines*, facilitating increased ASIO investigative activities, demonstrates insufficient ministerial attention to the tenor of s 17A of the *ASIO Act*.

The *2020 Guidelines* have further distinctive features confirming their practical operational interpretive influence over politically motivated violence, opening the gateway to security investigation, beyond that apparent from a conventional textual reading of relevant *ASIO Act* sections. As seen, paras 3.11 and 3.12 from the *2007 Guidelines* are copied over to become paras 5.20, 5.18 and 5.21 of the *2020 Guidelines*, with the content of para 3.12 significantly changed in its new guise.

The *2020 Guidelines* provide a second set of examples in relation to para (b) of the definition of politically motivated violence.[175] Three paragraphs are transpositions from the *2007 Guidelines*.[176] Another paragraph had the first sentence deleted, then was carried over unamended, from the *2007 Guidelines*.[177] Paragraph 3.20 of the *2007 Guidelines* is replaced by para 5.8 in the *2020 Guidelines*. Paragraph 5.8 sharpens up the language, with direct reference to a person or group as actors as not requiring an intention to initiate violence to achieve classification as politically motivated violence. Instead, an objective test applies for activities potentially leading to violence, merely requiring a 'reasonable likelihood that the activity will produce violence from others'.[178]

The Guidelines' liberalised content similarly supports an expansive interpretation of the politically motivated violence aspect of security. Probability of success or imminence of the violence are not determinative factors, but merely factors relevant in setting investigative priorities.[179] Though para (b) of the definition of politically motivated violence is both prefaced and conditioned upon the performance of 'acts',[180] the *2020 Guidelines* capaciously treat both lawful and non-public

---

174 The tension between s 17A of the *ASIO Act* and the *2022 Guidelines* likely arises from two sources: (a) the ample and definitive language of s 17A, protective of core political rights of expression, association and assembly, contrasted with the *2020 Guidelines* approach being more specious about the content of such rights; and (b) the effluxion of time since the *2007 Guidelines* influencing and eliding, through serial legislative terrorism law enactments, the thresholds at which it is considered proper to investigate politically motivated violence, of which terrorism is a subset: see *ASIO Act* (n 10) s 4 (definition of 'politically motivated violence' paras (a)–(d)). This is substantiated by the fact that s 17A was introduced in 1986: *ASIO Amendment* Act (n 86).

175 *ASIO Act* (n 10) s 4 (definition of 'politically motivated violence' para (b)).

176 Paragraphs 3.18, 3.21 and 3.22 of the *2007 Guidelines* (n 2) respectively became paras 5.6, 5.9 and 5.10 of the *2020 Guidelines* (n 1).

177 Paragraph 3.19 of the *2007 Guidelines* (n 2) became para 5.7 of the *2020 Guidelines* (n 1).

178 *2020 Guidelines* (n 1) 19 [5.8].

179 Ibid 19 [5.7].

180 *ASIO Act* (n 10) s 4 (definition of 'politically motivated violence' para (b)).

advocacy of violence as an act, stating that 'preparations directed at the overthrow of government are likely to be clandestine and their early manifestations are deceptive'.[181] The understanding of politically motivated violence as an element of security becomes predictive and pre-emptive as classes of non-violent activities, minimally contemplating violence, are included, potentially warranting ASIO investigation in ascertaining a risk of politically motivated violence.[182]

This very elastic interpretation in the Guidelines — aiding the collation, correlation and evaluation of the politically motivated violence aspect of security — is highly adaptable to increasing ASIO activity, such as liberalised questioning warrants covering politically motivated violence.[183] How the Guidelines might further elasticise the boundaries of what constitutes politically motivated violence, triggering this new aspect of ASIO's investigative powers regime, remains to be seen. The above politically motivated violence examples demonstrate a formalistic level of ministerial responsibility underpinning the Guidelines, combined with relaxed thresholds and an increased ASIO mandate, with the Guidelines enabling various expansive enabling features as relevant to security. This is a silently occurring phenomenon, under the nominal device of ministerial responsibility, requiring closer review and scrutiny ensuring that new restraints — for example a revised IGIS mandate — are more clearly calibrated to ministerial responsibility accountability principles.

C *The Capacity for Exiting or Remediating the Intelligence Gathering Process: Review, Deletion and Destruction of Information Not Relevant to Security*

The preceding discussion has highlighted the capacity of the Guidelines to interpretively extend ASIO investigative activities as relevant to one or more of the aspects of security, exceeding a conventional textual interpretation of the *ASIO Act*. That capacity is also prominent in relation to preliminary and determinative investigations, as to whether conduct falls within one of the components of security, or more specifically falls within the latitudinal accommodations of investigating politically motivated violence.

The converse of that question also arises. This is whether exit points exist for ASIO investigations after commencement, allowing ascertaining of whether contemporary circumstances are reasonably determinative of continuing relevance to

---

181 *2020 Guidelines* (n 1) 19 [5.9].

182 Ibid 19 [5.10] states:

> If apparently non-violent activities directed at destabilising or undermining constitutional government are associated with what purports to be no more than contemplation of the prospect of the violent overthrow of government, ASIO may investigate those activities to the extent necessary to establish (with some confidence) whether the activities involve a real risk or danger that violence will flow from those activities.

183 Introduced in the *ASIO Amendment Act* (n 86) which significantly expanded ASIO questioning powers on matters relevant to security (now extended beyond terrorism offences to politically motivated violence, espionage and foreign interference, whilst removing independent warrant issuing authorities: at sch 1 pt 1.

security, and whether the continuity of that relevance remains as an ASIO function. That issue is not resolved in the Guidelines. The necessary criteria and information might only appear in classified, publicly unavailable ASIO policies. Such apparent gaps in the Guidelines are not aligned with a best practice Guidelines accountability approach. The issues examined below indicate several lacunae and weaknesses in the Guidelines falling short of their optimisation as a ministerial responsibility and accountability measure — there is a significant reliance on ministerial and ASIO interpretative discretion around these issues, which may unnecessarily complicate the IGIS's review role.

First, a need exists for an accountable scheme for the deletion and destruction of such ASIO acquired information, which is not relevant, or no longer relevant, to security, to be incorporated into the Guidelines.[184] That would provide a default setting for information acquisition and retention issues in ongoing ASIO security investigations.

Further relevant Guidelines' observations arise. Ongoing investigations require review no less than annually.[185] Arguably, such internal review is insufficiently frequent, with compulsory internal periodic review likely to be better served at strategic intervals such as the expiration of various warrant authorities under div 2 of the *ASIO Act*. Such review should be more independent, carried out only by a senior ASIO official not involved in the instant security investigation.

Part 4 of the *2020 Guidelines*[186] (the treatment of personal information), lacks sufficiently specific obligations and timelines,[187] including for deletion and destruction. This looseness assimilates s 31 of the *ASIO Act* drafting, which is the obligation to destroy records or copies made from information sourced under ASIO warrant authority, when the Director-General is satisfied that the record or copy is not required for the purposes of the performance of functions or exercise of powers under the *ASIO Act*.[188]

---

184 Rule 2.18 of the original Guidelines (prior to 2007) included an obligation for ASIO 'to destroy records of any investigation that ends up being irrelevant to national security': 'Govt To Reissue ASIO Guidelines', *ABC News* (online, 21 September 2007) <https://www.abc.net.au/news/2007-09-21/govt-to-reissue-asio-guidelines/676296>. See also: 'New ASIO Rules Cause Concern', *ABC Local Radio* (ABC News, 21 September 2007) 08:08:00 <https://www.abc.net.au/am/content/2007/s2039346.htm>. This paragraph was reinstated in modified form in the *2007 Guidelines* (n 2) [2.18].

185 *2020 Guidelines* (n 1) 8 [2.5].

186 See ibid pt 4. Part 4 is titled 'Treatment of Personal Information', and includes subheadings on 'Security and Access to Personal Information Holdings', 'Compliance with Commonwealth Recordkeeping Requirements' and 'Disposal of Records'.

187 See above Part III(A) for examination of pt 4 of the *2020 Guidelines* (n 1). The Guidelines do not always provide guidance — the significant role of maintained and classified ASIO policies made under Guidelines' authority.

188 This provision is open ended, imposing no interval or time requirement for the Director-General's active engagement in such an assessment.

Part 4 of the Guidelines commences with textual invocations of reasonableness,[189] immediately devolving responsibility for access to and retention of personal information to the maintenance of classified ASIO policies.[190] Following these principles, the policies must provide clear guidance in 'processes for periodic review of its holdings, including personal information, to determine whether retention is reasonable'.[191] Such periodic reviews will be useful if the maintained policies faithfully and substantively implement this aspect of the Guidelines. The Law Council observed that '[t]his requirement may assist in remediating or preventing ASIO from retaining large volumes of personal information for prolonged periods of time, without regular assessment of whether the relevant individuals remain of security interest'.[192] It is a useful improvised step in response to the lack of a precise statutory obligation of regular review and destruction of personal information not relevant to security, or no longer relevant to security.[193] Reforming the *ASIO Act* provision[194] would be a superior, direct and more durable alternative.

Specified inclusion in policies includes retaining personal information only: (a) when it is relevant to the proper performance of ASIO's functions or the exercise of its powers; or (b) where otherwise authorised, or required, by law.[195] The Law Council highlighted the risk that the lack of a comprehensive ASIO personal information destruction requirement — in the *ASIO Act* or in the Guidelines — might mean that information not explicitly captured, by default would otherwise be authorised by law, allowing retention.[196] It also called for a definition of 'reference data'[197] to be included in the Appendix to the Guidelines, to avoid any specialised, unknown meaning that ASIO might settle upon.[198]

The vexed contest of maintaining ASIO operational and methodological secrecy and ensuring accountability emerges again, in establishing obligations maintaining these

189 See above n 125 and accompanying text.

190 *2020 Guidelines* (n 1) 13–14 [4.3(a)–(b)]. The policies are formed under broad principles.

191 Ibid 13 [4.3(a)(vi)].

192 *Comments on the Minister's Guidelines* (n 12) 23 [77].

193 See, eg: *PJCIS Advisory report* (n 4) 45 [3.48]–[3.50], 46 [3.51]–[3.52]; Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Report, 27 February 2015) 259–62 [6.217]–[6.225], 262, recommendation 28.

194 For example, s 31 of the *ASIO Act* (n 10) applies to records obtained under div 2 in the Act.

195 See *2020 Guidelines* (n 1) 13–14 [4.3(b)(i)]. See also discussion under Part III(A) above.

196 *Comments on the Minister's Guidelines* (n 12) 24 [81].

197 *2020 Guidelines* (n 1) 14 [4.3(b)(ii)].

198 *Comments on the Minister's Guidelines* (n 12) 25 [89]–[91].

policies, against the policies' approach to classified documents.[199] The maintained policies require '[reporting] to the IGIS any collection of, or access to, data, which may include reference data, which are inconsistent with, or in contravention of legislation'.[200] This is a useful accountability mechanism, but the Guidelines would be strengthened by an improved accountability of obligations and timelines — in turn facilitating a more focused IGIS role in auditing, investigation and annual reporting.

Part 4 of the *2020 Guidelines*[201] assigns the Director-General of ASIO direct responsibilities, not separately contingent upon maintaining policies. This includes a responsibility relating to security and access to personal information holdings.[202] Distinctively, the *2020 Guidelines* deal with Director-General post-retention of personal information, in compliance with Commonwealth recordkeeping requirements;[203] along with disposal of records,[204] under the *Archives Act 1983* (Cth).[205] The preconditions for these Director-General's specified responsibilities are nonetheless loose and accommodative:

> 4.11 ASIO must take reasonable steps to destroy or otherwise dispose of personal information where that personal information is:
>
> a) not required by ASIO for the performance of its functions or exercise of its powers, and

---

199 Ibid 25–6. This issue is approached differently when highlighting PJCIS objections to no ASIO obligation to provide it with the maintained policies.

200 *2020 Guidelines* (n 1) 14 [4.3(b)(iv)].

201 See discussion under Part III(A) above.

202 *2020 Guidelines* (n 1) 14 [4.4(a)–(c)].

203 Ibid 15 [4.8]: 'The Director-General will ensure that appropriate internal policies and procedures are in place to inform the setting and reviewing of disposal classes applied to records under the ASIO Records Authority.'

204 Ibid 16 [4.13]:

> Subject to paragraph 4.11, the Director-General will ensure that in accordance with applicable legislative requirements: (a) after the minimum retention period for a record (including a record containing personal information) has expired, and (b) where ASIO's review processes have determined the record is no longer needed for the proper performance of ASIO's functions, the relevant record will be destroyed in accordance with the ASIO Records Authority.

205 See *Archives Act 1983* (Cth) ss 29(1)(a)–(b), (8)(a). See also National Archives of Australia, *Australian Security Intelligence Organisation: Foreign Intelligence Collection; Protection of Agency Personnel and Personnel Records; Security Intelligence Assessment and Advice; Security Intelligence Collection* (Records Authority 2012/00324244, 26 October 2016) listing ASIO records under the categories of Foreign Intelligence Collection, Protection of Agency Personnel and Personnel Records, Security Intelligence Assessment and Advice and Security Intelligence Collection, including sub-categories of these records to be retained as national archives or to be destroyed after prescribed expiration of years by ASIO itself.

> b) not required to demonstrate propriety, compliance by ASIO with laws of the Commonwealth and of States and Territories, or directions and guidelines given to ASIO by the Minister.[206]

The term 'disposal' marks the finality of the personal information holdings, in contradistinction to ASIO's preceding access and retention of information, involving the management of that personal information. Disposal may include de-identified personal information.[207] ASIO may retain de-identified information (therefore making it no longer personal information), for the performance of functions and the exercise of its powers consistent with legislative requirements.[208]

These are open textured provisions – — the breadth of ASIO's functions and investigative powers has sizeably increased since the inception of the ministerial guidelines, diminishing the circumstances of personal information being 'not required'[209] for ASIO performance. Similarly, 'not required' might have been more precisely expressed as 'demonstrably not required' or 'reasonably not required'. Refining the wording would have created a lower threshold for the Director-General's specific obligations to dispose of information.

The phrase 'directions or guidelines given to ASIO by the Minister',[210] contemplates the use of ss 8 (Directions from the Minister) and 8A (Ministerial Guidelines) of the *ASIO Act* for other purposes consistent with the functions of the organisation, potentially overriding the obligation to take reasonable steps to destroy or otherwise dispose of personal information. Additionally, the capacity to de-identify information (which is categorised as disposal) allows and may even encourage the retention of substantial security subject matter information, organisations and groups in civil society in a residual form as long as the appendix threshold of 'de-identified'[211] information is reached. This leaves open the possibility to augment ASIO's existing long-term information holdings on subject matters, organisations and groups, considered as of continuing relevance to security.

206 Ibid 15–16 [4.11].

207 Ibid 22 (definition of 'de-identified').

208 Ibid 16 [4.12].

209 Ibid 15–16 [4.11]. See above n 206 and accompanying text.

210 *2020 Guidelines* (n 1) 16 [4.11(b)].

211 See ibid 16 [4.12]. See also at 22 for the meaning of 'de-identified': 'the removal of direct identifiers and one or both of the removal or alteration of other information that could potentially be used to re-identify an individual, and/or the use of controls and safeguards in the data access environment to prevent re-identification'.

IV Concluding Observations: Renewing and Reforming the Guidelines To Enhance Ministerial Responsibility and ASIO Accountability

This article's identification of noticeable Guidelines' deficiencies gives cause for both concern and reflection. The conception of the Guidelines emerged from the Second Hope Royal Commission, conceived within a distinctive context of ASIO improprieties and illegalities,[212] a much narrower compass of security-related activities, and an organisation of significantly smaller scale and budget.

Nearly forty years on, the Guidelines' conception and content invite re-imagination and reform to simultaneously engage exponentially evolved national security authority with principles of ministerial responsibility. The *2020 Guidelines* presently fall noticeably short of such an objective.

The Guidelines need to be a contemporary document, conceptualised as one of many integrated ASIO accountability measures and attuned to Australia's preference for a parliamentary model of rights protection involving explicit rejection of a statutory charter of rights.[213] A reasonable public policy expectation for the Guidelines is that they should operate optimally as a part of that ministerial responsibility model, facilitating representative government system accountability. The legitimacy of that expectation is vindicated by the secretive nature of ASIO functions, alongside the potentially sensitive and damaging nature of security intelligence to individual rights and to the proper institutional and procedural functioning of representative government. Reform of the Guidelines therefore needs to enhance the operatives of ministerial responsibility, whilst affording consequential benefits for the other ASIO accountability mechanisms indirectly reflecting ministerial responsibility.

The Guidelines speak, when best, in pragmatic ways for providing ministerial guidance to the Director-General in carrying out ASIO's functions relevant to security. Reforms are achievable in this pragmatic spirit. The earlier sections of this article raised background issues and perspectives informing reform of the Guidelines around ministerial responsibility. The article then canvassed selected and important reforms to the Guidelines, to meet contemporary accountability expectations for ASIO consistent with ministerial responsibility.

The confluent timelines of periodic Review in para 1.14 of the *2020 Guidelines* and in the scheduling of the next Independent Intelligence Review[214] provide the opportunity for extensive review of the concept, content and connectivity of the *2020 Guidelines*. Enhancing the effectiveness of the Guidelines within the suite

---

212 See above n 51 and accompanying text.

213 See, eg: Robert McClelland, 'Australia's Human Rights Framework' (Media Release, 21 April 2010); McClelland, *The Protection and Promotion of Human Rights in Australia* (n 101).

214 The last independent intelligence review was in 2017: *Independent Intelligence Review* (n 40).

of ASIO accountability measures requires genuine independent review. Inadequacies in the newly revised *2020 Guidelines* suggest that task exceeds the capacity of the Minister and the Department of Home Affairs, acting in consultation with the Attorney-General.

Paragraph 1.14 of the *2020 Guidelines* interestingly refers to the 'operation and continued suitability of these Guidelines'.[215] This may simply presume internal ministerial review in conjunction with the operation of s 8A of the *ASIO Act*. This, however, is not textually explicit. The structural arrangements for review of the Guidelines are therefore sufficiently opaque to accommodate different review models.

Alternatively, there could be a reference of the Guidelines by the Prime Minister or the Attorney-General for INSLM review under the *INSLM Act*.[216] The INSLM review could advantageously engage directly with international human rights obligations and proportionality like standards when conducting such a review.[217]

A further alternative would be for Guidelines review to be included within a larger, Royal Commission review into intelligence agencies.[218] This approach could be accommodated within the existing Guidelines review paragraphs. This is a desirable model when the next Independent Intelligence Review is due, following release of the public version of the *Richardson Review* and the Government Response to it.[219] This is a plausible approach given the substantial human rights and representative government system implications ensuing from a probably liberalised, harmonised and integrated NIC security intelligence approach. This recommended course of action would focus upon critical aspects of the *Richardson Review*, providing a broad forum for greater public policy participation, including review of ministerial responsibility and other accountability measures.

More immediate Guidelines reforms (other than review) are achievable. The Guidelines that inform oversight and accountability objectives, and the explicit embrace and articulation of ministerial responsibility for ASIO, could usefully be incorporated in a preamble, forming a presumptive interpretive source. That statement should clearly set the Guidelines' role and utility given: (1) the unique identified ministerial responsibility circumstances in matters relevant to security; and (2) the identification of the Guidelines as part of an interlocking and reciprocally informing accountability framework immediately with the IGIS, but further affecting the INSLM, PJCIS and PJCHR.

215 *2020 Guidelines* (n 1) 5 [1.14].

216 *INSLM Act* (n 17) s 7.

217 See ibid ss 3(c)(i), (d), 8(a)(i).

218 See Kim McGrath, 'Drawing the Line: Witness K and the Ethics of Spying' (2020) 9(1) *Australian Foreign Affairs* 53, 77; Edwards (n 51) 334–5.

219 See *Richardson Review* (n 41) vols 1–4; Government Response (n 3).

Mindful of the latter of these two important principles, a productive Guidelines reform initiative would draw upon proposed integrated national security accountability reforms of former Labor, Senator John Faulkner and present Labor Senators Penny Wong and Jenny McAllister, adapting and integrating the role of the Guidelines explicitly in a renewed ASIO accountability package. Senator Faulkner suggested building stronger, beneficial relationships between the PJCIS, the IGIS, and the INSLM.[220] Senator Wong introduced a Bill in 2015[221] to allow the INSLM and IGIS to provide copies of their reports to the PJCIS and for the INSLM and National Security Adviser to consult with PJCIS. Senator McAllister introduced a further 2020 Bill[222] extending PJCIS capacities, information, advice and expertise.[223]

Importantly, the other ASIO accountability mechanisms can be informed by the operation of the Guidelines for their own purposes, namely how the Guidelines might increase the effectiveness of these other accountability mechanisms — IGIS, INSLM, PJCIS and PJCHR, including reviews of them. These other accountability mechanisms could in turn offer differently informed perspectives on Guidelines' reform.

Other reforms need grounding in the reality of the Guidelines' conception nearly forty years ago in a more placid national security environment, including a decidedly narrower ASIO official security remit. National security circumstances have changed dramatically. The Guidelines require re-setting around principles of flexibility, adaptability and responsiveness if they are to remain an effective ministerial responsibility mechanism. This involves several sequenced reforms.

---

220 See: John Faulkner, 'Surveillance, Intelligence and Accountability: An Australian Story' (Web Document) 46–7 <https://apo.org.au/sites/default/files/resource-files/2014-10/apo-nid41934.pdf>; 'Greater Oversight of Spies Needed, Says Faulkner', *Australian Financial Review* (online, 24 October 2014) <https://www.afr.com/politics/greater-oversight-of-spies-needed-says-faulkner-20141023-11aw8z>.

221 Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 (Cth) sch 1 items 1, 3, 10. The Bill lapsed at the dissolution of the 44th Parliament on 9 May 2016, and was restored to the Notice Paper on 31 August 2016, the second reading adjourned on 13 October 2016, and eventually lapsed with the 44th Parliament conclusion on 1 July 2019.

222 Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020 (Cth) was introduced into the Senate by Senator McAllister on 26 February 2020. This Bill is intended to implement several recommendations of the *Independent Intelligence Review* (n 40).

223 Under the Bill, the PJCIS would have capacity for self-activated review of existing, proposed, repealed, expiring, lapsing or ceasing laws relating to counter-terrorism or national security. The Bill would also allow the PJCIS to request reports on counter-terrorism or national security matters referred to the INSLM and to require regular briefings to the PJCIS by the IGIS and the Director-General of National Intelligence. A majority only report (with an ALP dissenting report) recommended that the Bill *not* be passed: Senate Finance and Public Administration Committee, Parliament of Australia, *Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020* (Report, December 2020) 6–7 [1.23].

The first of these reforms is to amend the language of s 8A of the *ASIO Act* to create obligations, rather than options, for the making of ministerial guidelines, and to do so within specified timeframes. Two timeframes would beneficially assist ministerial accountability. First, an adoption of the practice that Bills amending the *ASIO Act* must be simultaneously accompanied by a Bill appendix setting out corresponding changes to the Guidelines. This would allow periodic examination of the Guidelines by parliamentary and PJCIS processes at the time of the amending Bill. A more positive interactive interpretive relationship of the Guidelines with the legislation would be promoted than has hitherto occurred.[224]

The second change would be inclusion within s 8A of the *ASIO Act* and s 6 of the *INSLM Act*, a function that the INSLM review and report upon the Guidelines every three years, and communicate such reviews to the Minister, the Attorney-General and the IGIS. This would advantageously propel a regular Guidelines review schedule, such review then being informed by the INSLM report, prior to consultation with a wider category of stakeholders.

These two measures amending s 8A of the *ASIO Act* are appropriate and adapted to the realities of serial national security legislative reform, with constant review of national security laws (which include the *ASIO Act*). Both measures would ensure, over time, that substantial content omissions in the Guidelines would be remediated and new omissions not emerge, when the *ASIO Act* is further amended consistent with government claims of a changing security environment.

Enhancing the Guidelines' responsiveness to ongoing and rapid national security change will render the Guidelines of greater contemporary relevance. It will orientate Guidelines' culture as more responsive to the likely horizontal expansion of national security activity, and increased ASIO harmonised co-operative arrangements with other NIC members. This is likely to be of increased urgency now that the Richardson Review,[225] along with the Government Response[226] to that Review, are in the public domain. A more expeditious response is desirable due to a likely increase in ASIO questioning warrant activity for politically motivated violence, foreign interference and espionage.[227] Both items will increase the volumetrics and intrusiveness of ASIO activities relevant to security, which the Guidelines need address.

These reform initiatives will also usefully ventilate the Guidelines' inherent structural limitations as an instrument of ministerial responsibility. It might then be concluded that different accountability alternatives to the Guidelines are preferable in guiding discrete examples of ASIO activities relevant to security and in enhancing ministerial responsibility. Actual amendments to the *ASIO Act* may be

224 See the discussion under Part III(B) above.

225 *Richardson Review* (n 41).

226 Government Response (n 3).

227 Following the passage of the *ASIO Amendment Act* (n 86). *ASIO Amendment Act* (n 86) sch 1 pt 1 is now incorporated into the *ASIO Act* (n 10) div 3.

more effective. Internal ASIO organisational culture, ministerial and departmental attitudes will obviously affect the Guidelines' efficacy, making a broadened IGS scrutiny of these desirable. Parts of the Guidelines might warrant reclassification as disallowable instruments, improving parliamentary scrutiny.

Each of these issues involves a balancing both of ASIO and executive Ministers' accountability, as against the need to protect ASIO operational methods and sources. It also recognises that the Guidelines are, of course, executive sponsored instruments, with the IGIS acting as a proxy or medium for full ministerial accountability through parliamentary scrutiny. These are complex questions best examined by the suggested independent review mentioned above. The Guidelines have an important, but constrained, role as a ministerial responsibility mechanism. The progressive reforms outlined in this article would maximise the Guidelines' ministerial responsibility performance, by improving the integration and workability of the ASIO accountability suite.