LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

Research Paper Series, 2017–18
ISSN 2203-5249

Oversight of Intelligence Agencies: A Comparison of the 'Five Eyes' Nations

Cat Barker and Claire Petrie (Parliamentary Library, Australia)
Joanna Dawson and Samantha Godec (House of Commons Library, United Kingdom)
Holly Porteous (Library of Parliament, Canada)
Pleasance Purser (Parliamentary Library, New Zealand)

13 December 2017

This paper is a collaboration between parliamentary researchers from four countries. Each is separately responsible for the content and accuracy of the contributions. We are grateful to authors from Canada, New Zealand and the United Kingdom for their contributions to the paper.

EXECUTIVE SUMMARY

- Australia, Canada, New Zealand, the United Kingdom and the United States each have some combination of parliamentary/congressional, independent and judicial oversight of their intelligence agencies, in addition to accountability through the executive branch. However, there are differences in the nature and scope of each of those components.
- The six agencies comprising the **Australian** intelligence community are overseen by a parliamentary committee that examines their administration and expenditure and an independent Inspector-General of Intelligence and Security, who examines the legality and propriety of their activities. Most of the agencies' activities and powers are authorised by the responsible ministers. A review completed in June 2017 recommended that the remits of the committee and the Inspector-General be expanded to include four additional agencies, and that the Inspector-General's resources be significantly increased.
- **Canada** has passed legislation creating a committee of parliamentarians to review the policy, administration, finance and operations of Canada's national security and intelligence community. At present, only two agencies are subject to dedicated independent expert review for lawfulness. Canada's national police force, which has responsibility for investigating security offences, is subject to independent expert review. However, this review is limited to handling public complaints about police officer conduct and, with the consent of the Public Safety Minister, undertaking public interest studies of specified activities. A Bill has been introduced that would create a single expert review body mandated to investigate complaints made in relation to the activities of three agencies and to examine the lawfulness, reasonableness and necessity of all national security and intelligence activities undertaken in the federal government. The Bill also proposes the creation of an Intelligence Commissioner to give final approval to certain activities undertaken by Canada's signals intelligence and security intelligence agencies.
- **New Zealand's** Intelligence and Security Act 2017 replaces the four acts that previously applied to the two intelligence and security agencies and their oversight bodies, and implements recommendations from the first periodic review of the agencies. The agencies are overseen by a parliamentary committee, which scrutinises their policies, administration and expenditure, and an independent Inspector-General of Intelligence and Security, who ensures that the agencies act with propriety and operate lawfully and effectively. Intelligence warrants may be issued by a responsible minister either solely, or jointly with a Commissioner of Intelligence Warrants.
- In the **United Kingdom**, the main focus of the Intelligence and Security Committee is to oversee the expenditure, administration, policies and (with some limitations) operations of the three key intelligence agencies, though it has scope to examine the work of other intelligence, security and law enforcement agencies. The Investigatory Powers Commissioner provides independent oversight of the use of intrusive powers by the three key intelligence agencies. The Commissioner, along with several judicial commissioners, is required to keep under review the exercise by public bodies of various statutory functions, and may be directed by the Prime Minister to review any other functions of the three key intelligence agencies. Legislation has been passed under which warrants, currently issued by ministers, will only come into force after being reviewed by a judicial commissioner. The Investigatory Powers Tribunal investigates complaints about public bodies' use of investigatory powers.

- The **United States** intelligence community comprises 17 executive branch entities. Congressional oversight of the intelligence community is spread across several committees, including specialised committees on intelligence in the House and the Senate. While each has some limits on what it may examine, taken collectively the committees have the ability to inquire into all of the intelligence-related activities of the US Government. The Executive Office of the President houses several key mechanisms for overseeing the intelligence community, including the President's Intelligence Advisory Board and the Privacy and Civil Liberties Oversight Board. These are augmented by a network of Inspectors General and legal counsels. In addition to Inspectors General attached to specific agencies and departments, the Inspector General of the Intelligence Community conducts audits, inspections and investigations of cross-cutting programs and activities. The federal judiciary examines a wide range of intelligence activities under a number of laws, including the Constitution. Most notably, the Foreign Intelligence Surveillance Court reviews applications for warrants related to the collection of foreign intelligence by the US Government.
- Despite differences in the approach taken, each of the five countries has developed a framework that includes a system of checks and balances that spans the various branches of government, and which aims to ensure that agencies are accountable for both their administration and expenditure and the legality and propriety of their activities.
- The intelligence communities have evolved to meet new challenges as they arise, and will continue to do so. It will be important for the oversight arrangements to keep pace with such changes.

CONTENTS

Page

CONTRIBUTORS

This research paper represents a collaborative effort between researchers in Australia, Canada, New Zealand, and the United Kingdom, all of whom work in research organisations supporting their respective national Parliaments.

The project was led by Cat Barker (Parliamentary Library, Australia). The other contributors were Claire Petrie (Parliamentary Library, Australia), Holly Porteous (Library of Parliament, Canada), Pleasance Purser (Parliamentary Library, New Zealand), and Joanna Dawson and Samantha Godec (House of Commons Library, United Kingdom).

The Congressional Research Service's (CRS, United States) publication policies precluded it from participating at this time.[1] Information on US arrangements has been included in the comparative section of this paper on the basis of research conducted by Cat Barker and Samantha Godec.

1. CRS does not publish the reports it provides to parliamentarians and committees; however, recipients of the reports have historically been free to publish them on their own websites, and some third parties collect the reports on publicly accessible websites. A Bill that would require the Government Publishing Office to make CRS reports accessible online was re-introduced in May 2017: H.R.2335—Equal Access to Congressional Research Service Reports Act of 2017; J Haggarty, 'Congressmen reintroduce bill to make CRS reports public', Congressional Data Coalition blog, 9 May 2017.

GLOSSARY OF ACRONYMS

AAT	Administrative Appeals Tribunal (Aus)
ACIC	Australian Criminal Intelligence Commission
AFP	Australian Federal Police
AGO	Australian Geospatial-Intelligence Organisation
AIC	Australian Intelligence Community
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
CBSA	Canada Border Services Agency
CFINTCOM	Canadian Forces Intelligence Command
CRCC	Civilian Review and Complaints Commission for the RCMP
CSE	Communications Security Establishment (Can)
CSIS	Canadian Security Intelligence Service
DIBP	Department of Immigration and Border Protection (Aus)
DIO	Defence Intelligence Organisation (Aus)
DND	Department of National Defence (Can)
ETHI	House of Commons Standing Committee on Access to Information, Privacy and Ethics (Can)
FINTRAC	Financial Transactions and Reports Analysis Centre (Can)
GCHQ	Government Communications Headquarters (UK)
GCSB	Government Communications Security Bureau (NZ)
HPSCI	House Permanent Select Committee on Intelligence (US)
IG	Inspector-General (US)
IGIS	Inspector-General of Intelligence and Security (Aus; NZ)
INSLM	Independent National Security Legislation Monitor (Aus)
IPA	*Investigatory Powers Act 2016* (UK)
IPC	Investigatory Powers Commissioner (UK)
ISA	*Intelligence Services Act 1994* (UK)
IS Act	*Intelligence Services Act 2001* (Aus)
ISC	Intelligence and Security Committee (NZ; UK)
IPT	Investigatory Powers Tribunal (UK)
JIC	Joint Intelligence Committee (UK)
JSA	*Justice and Security Act 2013* (UK)
MI5	Security Service (UK)
MI6	Secret Intelligence Service (UK)
NSIA	National Security and Intelligence Advisor to the Prime Minister (Can)
NSICOP	National Security and Intelligence Committee of Parliamentarians (Can)
NSICPA	*National Security and Intelligence Committee of Parliamentarians Act* (Can)
NSIRA	National Security and Intelligence Review Agency (Can)
NZSIS	New Zealand Security Intelligence Service
OCSEC	Office of the Communications Security Establishment Commissioner (OCSEC)
ONA	Office of National Assessments (Aus)
PCLOB	Privacy and Civil Liberties Oversight Board (US)

PIAB	President’s Intelligence Advisory Board (US)
PJCIS	Parliamentary Joint Committee on Intelligence and Security (Aus)
PSC	Public Safety Canada
RCMP	Royal Canadian Mounted Police
RIPA	R*egulation of Investigatory Powers Act 2000* (UK)
SECD	Standing Senate Committee on National Security and Defence (Can)
SECU	House of Commons Standing Committee on Public Safety and National Security (Can)
SIRC	Security Intelligence Review Committee (Can)
SIS	Secret Intelligence Service (UK)
SSCI	Senate Select Committee on Intelligence (US)
USIC	US Intelligence Community

INTRODUCTION

The size and powers of Western national security and intelligence agencies have increased significantly since the 9/11 terrorist attacks. Information revealed by Edward Snowden in 2013 and further reforms to intelligence agency powers, including those aimed at dealing more effectively with threats associated with the Islamic State group and 'foreign fighters', have ensured that the accountability framework that applies to those agencies is of continuing interest.

The intelligence communities and associated oversight frameworks in Australia, Canada, New Zealand, the United Kingdom and the United States have each evolved to meet the particular needs of those countries and the specific contexts in which they operate. However, as Western democratic nations facing similar challenges in balancing the imperative of accountability with the need for intelligence agencies to operate with a degree of secrecy, and that share a close intelligence sharing and co-operation relationship under the Five Eyes arrangements, these countries serve as relevant and useful comparators to one another.[2] The independent oversight bodies in the five countries agreed in September 2016 to establish the *Five Eyes Intelligence Oversight and Review Council* 'to facilitate the sharing of experiences and best practice in oversight and review' that will meet annually in person and quarterly by secure electronic communication.[3]

A. Outline and purpose

This Research Paper first provides information on the intelligence communities, key mechanisms for oversight of the intelligence community and any recent changes to, or reviews of, the oversight frameworks in Australia, Canada, New Zealand and the UK by country. This is followed by comparative analysis that highlights some of the similarities and differences between those countries, and also the US, in the arrangements that exist for intelligence oversight.

In each country, there is some combination of parliamentary/congressional, independent and judicial oversight in place, in addition to accountability through the executive branch. However, there are differences in the nature and scope of each of those components. Examples include the extent to which parliamentary or congressional committees can access classified material, and to which they may examine the operations (as distinct from administration, expenses and policies) of the intelligence agencies; and whether independent oversight is primarily centralised or distributed. In all but the US, significant reviews of, or reforms to, intelligence oversight arrangements have been undertaken in the previous five years, and further specific reforms are currently under consideration in Australia and Canada. It is hoped that by drawing out some of the similarities and differences between these systems, this paper will support parliamentarians in each of the countries covered in their consideration of current arrangements and any potential reforms.

---

2. Cooperation between the UK and US on foreign signals intelligence was formalised with the signing of the BRUSA (now known as UKUSA) Agreement in 1946. In 1955, the Agreement was revised to explicitly cover Australia, Canada and NZ. It was the basis for what is informally referred to as the 'Five Eyes' alliance, recently referred to as 'the most comprehensive and closest intelligence sharing and co-operation arrangement' in the world: M Cullen and P Reddy, *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand*, 29 February 2016, p. 46; National Security Agency Central Security Service, 'UKUSA Agreement Release 1940–1956', National Security Agency website. In April 2017, Canada released a redacted version of the 1949 CANUSA agreement: B Robinson, 'CANUSA Agreement declassified', Lux Ex Umbra blog, 23 April 2017.

3. Inspector-General of Intelligence and Security (IGIS) (Australia), *Annual report 2016–17*, IGIS, 2017, p. v.

B. Scope

The information on each country's intelligence oversight framework is focused mainly on the key mechanisms in place in the parliamentary/congressional, independent and judicial spheres. Less detail is included on broader systems of executive oversight and other accountability mechanisms such as auditors-general, whose jurisdiction may include, but is not specifically focused on, intelligence agencies.

The agencies considered 'in-scope' for each country are those that are defined or considered by that country to comprise its intelligence community at the time of publication. The oversight arrangements described are, except where otherwise noted, those in place at the time of publication. Reforms being considered at the time of publication are covered in the sections on recent developments and reform proposals in each of the country sections.

AUSTRALIA

A. Overview of intelligence agencies

The Australian Intelligence Community (AIC) comprises the six agencies outlined below. The AIC is part of the broader national security community that includes law enforcement, border protection and policy agencies.[4]

The Australian Security Intelligence Organisation (ASIO) is Australia's national security intelligence agency. Its role is to identify, investigate, and provide advice on threats to security and it is responsible to the Attorney-General.[5]

The Australian Secret Intelligence Service (ASIS) is Australia's overseas secret intelligence collection agency. Its main functions are to collect and distribute across the Australian Government foreign intelligence that may impact on Australia's interests, carrying out counter-intelligence activities and liaising with overseas intelligence and security agencies. ASIS is responsible to the Minister for Foreign Affairs.[6]

The Office of National Assessments (ONA) is responsible for analysing and providing advice on information (including open source) relating to international matters of political, strategic or economic interest to Australia. It also plays a role in coordinating and evaluating Australia's foreign intelligence activities. ONA is responsible to the Prime Minister.[7]

There are three intelligence agencies within the Department of Defence, two of which have responsibilities beyond that portfolio. The Australian Signals Directorate (ASD; formerly known as the Defence Signals Directorate, or DSD) collects and analyses foreign signals intelligence and provides information and communications security advice and services to the Australian Government.[8] The Australian Geospatial-Intelligence Organisation's (AGO) main role is to collect and analyse geospatial and imagery intelligence for the purposes of informing the Government about the capabilities, intentions or activities of people or organisations outside Australia, supporting Australian Defence Force (ADF) activities and supporting the national security functions of Commonwealth and state authorities.[9] The Defence Intelligence Organisation (DIO) assesses and analyses intelligence on countries and foreign organisations to support ADF operations, capability and policy development, and broader decision-making on defence and national security issues.[10]

---

4. A recently completed review assessed that looking ahead, a more realistic frame of reference for the intelligence community would also include the Australian Criminal Intelligence Commission, the Australian Transaction Reports and Analysis Centre and parts of the Australian Federal Police and the Department of Immigration and Border Protection: Department of the Prime Minister and Cabinet (PM&C), *2017 Independent Intelligence Review*, Commonwealth of Australia, Canberra, June 2017, pp. 46–48.

5. *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*), see in particular sections 17 (functions) and 4 (definition of security); Australian Security Intelligence Organisation (ASIO), 'About ASIO', ASIO website.

6. *Intelligence Services Act 2001* (*IS Act*), Part 3 (establishment) and sections 6 and 11 (functions); Australian Secret Intelligence Service (ASIS), 'About us' and 'Governance', ASIS website.

7. *Office of National Assessments Act 1977*, particularly section 5 (functions); Office of National Assessments (ONA), 'Overview' and 'Legislation', ONA website.

8. *IS Act*, sections 7 and 11; Australian Signals Directorate (ASD), 'About ASD' and 'Accountability', ASD website.

9. *Intelligence Services Act 2001*, sections 6B and 11; Australian Geospatial-Intelligence Organisation (AGO), 'About AGO, 'GEOINT support to Government and Defence', 'GEOINT support to national security' and 'GEOINT support to military operations', AGO website.

10. Defence Intelligence Organisation (DIO), 'About us', 'What we do', 'General intelligence', 'Scientific intelligence analysts' and 'Technical intelligence', DIO website. DIO's functions are not set out in legislation.

B. Oversight

1. Oversight summary

Two Royal Commissions led by Justice Robert Marsden Hope in the 1970s and 1980s, and further major reviews in the 1990s and early 2000s have played a significant role in shaping Australia's framework for oversight of its intelligence agencies.[11] While the AIC has grown and evolved significantly in the intervening period, the key oversight mechanisms have remained largely unchanged.

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Inspector-General of Intelligence and Security (IGIS) perform complementary roles. The Committee oversees the administration and expenditure of the intelligence agencies, while the Inspector-General reviews their operational activities. These standing mechanisms are supplemented by external reviews of the intelligence agencies, with the most recent completed in June 2017.[12] Changes to oversight arrangements recommended by the most recent review are outlined below in the section titled 'Recent developments and reform proposals'.

Judicial oversight of intelligence activities is limited, with the courts having little involvement in the issuing or monitoring of warrants. The only specialised tribunal is the Security Division of the Administrative Appeals Tribunal, which conducts merits review of most categories of adverse security assessments issued by ASIO.[13]

The budgets of ASIO, ASIS and ONA are published in annual Portfolio Budget Statements, and the agencies can be held to account at related hearings of Senate committees (see below under 'Senate Standing Committees'; ASIO is the only agency to routinely appear at those hearings).[14] However, additional funding for ASIO and ASIS provided in the 2017–18 Budget was not included in the totals set out in the Portfolio Budget Statements, and it is unclear whether other amounts might have also been excluded.[15]

ASIO is the only agency which produces a publicly available annual report, which is then also tabled in Parliament. A classified version of ASIO's annual report is provided to the Attorney-General, who must share it with the Leader of the Opposition.[16] All AIC agencies are subject to financial and administrative audits by the Australian National Audit Office.[17]

---

11. Royal Commission on Intelligence and Security, *Report*, Australian Government Printing Service, Canberra, 1977 (note there are several volumes); Royal Commission on Australia's Security and Intelligence Agencies; *General report*, Australian Government Printing Service, Canberra, December 1984 (this Royal Commission also presented several reports on specific agencies and issues); Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service: public edition* (Samuels Inquiry), Commonwealth of Australia, 1995; P Flood, *Report of the Inquiry into Australian intelligence agencies* (Flood Review), Commonwealth of Australia, 2004.
12. The 2004 Flood Review recommended that in addition to standing review mechanisms, the AIC should be subject to 'periodic external review every five to seven years': Flood Review, op. cit., p. 63. R Cornall and R Black, *2011 Independent Review of the Intelligence Community report*, Commonwealth of Australia, 2011; PM&C, *2017 Independent Intelligence Review*, op. cit.
13. *ASIO Act*, Division 4 of Part 4; ASIO, 'ASIO's security assessment function', Information Brief, ASIO website.
14. Portfolio Budget Statements are tabled in Parliament on the night the Federal Budget is handed down. See Australian Government, 'Portfolio Budget Statements', Budget 2016–17 website.
15. C Barker, 'National security overview', *Budget review 2017–18*, Research paper series, 2016–17, Parliamentary Library, Canberra, May 2017; P Maley, 'Budget 2017: ISIS threat sparks funding boost', *The Australian*, 10 May 2017, p. 11.
16. *ASIO Act*, section 94.
17. *Auditor-General Act 1997*, section 56; *Crimes Act 1914*, section 85ZL; Australian National Audit Office website.

The Independent National Security Legislation Monitor (INSLM) does not oversee the agencies themselves, but has a related function of reviewing the operation, effectiveness and implications of counter-terrorism and national security legislation, including ASIO's special powers relating to terrorism.[18]

2. Parliamentary oversight

a. Parliamentary Joint Committee on Intelligence and Security

The PJCIS was first established in 1988 as the Parliamentary Joint Committee on the Australian Security Intelligence Organisation.[19] ASIS was brought under the Committee's remit in 2002, implementing a recommendation of the Commission of Inquiry into the Australian Secret Intelligence Service (Samuels Inquiry) that reported in 1995.[20] ASD was added at the same time.[21] The PJCIS has overseen all six AIC agencies since 2005, when its mandate was extended to include ONA, DIO and AGO in response to a recommendation of the 2004 *Report of the Inquiry into Australian Intelligence Agencies* (the Flood Review).[22]

b. Functions

The PJCIS is established under Part 4 of the *Intelligence Services Act 2001* (*IS Act*), with additional detail set out in Schedule 1 to the Act. Section 29 sets out what the PJCIS's functions are, and just as importantly, what they are not. With respect to oversight of the AIC, the PJCIS's functions are (subject to the limitations set out below) to:[23]

- review the administration and expenditure of the AIC agencies, including their annual financial statements
- review any matter in relation to an AIC agency referred to it by the responsible minister or a House of Parliament

---

18. *Independent National Security Legislation Monitor Act 2010* (*INSLM Act*), sections 3, 4 and 6; Independent National Security Legislation Monitor website.

19. Parliamentary Joint Committee on Intelligence and Security (PJCIS), 'History of the Intelligence and Security Committee', Australian Parliament website. The *Australian Security Intelligence Organization Amendment Act 1986* inserted Part VA into the *Australian Security Intelligence Organisation Act 1979* (since repealed and replaced by provisions in the *IS Act*).

20. PJCIS, 'History of the Intelligence and Security Committee', ibid.; Samuels Inquiry, op. cit., Chapter 5 (pp. 40–63). The PJC on ASIO, ASIS and DSD was established by Part 4 of the *IS Act*.

21. The initial version of the originating Bill would have established a committee to oversee ASIO and ASIS. The Bill was amended to include DSD in the committee's mandate to accord with a recommendation made by the Joint Select Committee on Intelligence and Security in its report on the Bill and two others: Parliament of Australia, 'Intelligence Services Bill 2001 homepage', Australian Parliament website; Joint Select Committee on Intelligence and Security, *An advisory report on the Intelligence Services Bill 2001, the Intelligence Services (Consequential Provisions) Bill 2001 and certain parts of the Cybercrime Bill 2001*, Parliament of Australia, August 2001.

22. PJCIS, 'History of the Intelligence and Security Committee', op. cit.; Flood Review, op. cit., pp. 57–59. The *Intelligence Services Legislation Amendment Act 2005* amended Part 4 and Schedule 1 of the *IS Act*.

23. The PJCIS also has a role in overseeing particular functions of the Australian Federal Police, specifically its counter-terrorism functions (added in 2014: *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*) and activities relating to Australia's telecommunications data retention scheme (since 2015: *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*): *IS Act*, paragraphs 29(1)(baa), (bab), (bac), and (be) and subsection 29(5). That role and other functions of the PJCIS provided for under the *IS Act* and other laws fall outside the scope of this paper. For a brief summary, see PJCIS, 'Role of the Committee', Australian Parliament website.

- review any matter in relation to ASIO's activities relating to the telecommunications data retention scheme that are set out in an annual report about the scheme by ASIO and
- report its comments and recommendations to each House of Parliament and the responsible minister.[24]

The PJCIS is specifically precluded from reviewing:

- the intelligence gathering and assessment priorities of the AIC agencies
- the sources of information, other operational assistance or operational methods available to the AIC agencies
- particular operations that have been, are being or are proposed to be undertaken by ASIO, ASIS, AGO, DIO, or ASD[25]
- information provided by a foreign government (or one of its agencies) where that government does not consent to the disclosure of the information
- an aspect of the activities of an AIC agency that does not affect an Australian person
- rules made about protecting the privacy of Australians
- the content of, or conclusions reached in, assessments or reports made by DIO or ONA, or reviewing sources of information on which such assessments or reports are based and
- the coordination and evaluation activities undertaken by ONA.[26]

c. Powers and performance of functions

The PJCIS conducts annual reviews of the administration and expenditure of the AIC agencies. These reviews are based on information provided by the AIC agencies, the IGIS and the Auditor-General in submissions (most of which are classified) and at closed hearings.[27] The reports on these reviews are tabled in each House of Parliament and published on the PJCIS's website. They include commentary from the PJCIS on relevant matters, and sometimes specific recommendations to government. For example, in its report for 2011–13, the PJCIS recommended that the Government review the continued application of the efficiency dividend and other savings measures to AIC agencies, and that it consider the reforms necessary to equip the AIC to meet the challenges posed by technological changes.[28]

---

24. *IS Act*, subsection 29(1).
25. Except to the very limited extent allowed under subsections 29(4) and (5), that is, 'for the sole purpose of assessing, and making recommendations on, the overall effectiveness of Part 5–1A of the *Telecommunications (Interception and Access) Act 1979* (telecommunications data retention).
26. *IS Act*, subsection 29(3). The PJCIS's functions also do not include dealing with individual complaints about AIC agencies (paragraph 29(3)(g)).
27. Generally, the IGIS's submission is unclassified, and ASIO and ONA provide unclassified submissions or unclassified summaries of classified submissions. The PJCIS's reports include appendices listing submissions and their classification. Unclassified submissions and summaries can be accessed from the relevant inquiry homepages: PJCIS, 'Completed inquiries and reports', Australian Parliament website.
28. PJCIS, *Review of administration and expenditure: no. 11 and no. 12–Australian intelligence agencies*, Australian Parliament, September 2014, pp. 10, 61. The efficiency dividend is an annual funding reduction that applies the operational budget of Australian Government departments and agencies. Some agencies are exempt: N Horne, *The Commonwealth efficiency dividend: an overview*, Background note, Parliamentary Library, Canberra, 13 December 2012.

The PJCIS does not have the power to initiate its own inquiries into matters relating to the activities of an AIC agency. However, it may, by resolution, request that the responsible minister refer such a matter (though ministers may decline such requests).[29] As noted above, matters may also be referred by a House of Parliament. In practice, most inquiries conducted by the PJCIS or its predecessors into matters relating to the activities of an AIC agency were initiated by a referral from the minister, and almost all have concerned potential or proposed reforms to legislation.[30] A notable exception on both counts was the referral to the PJC on ASIO, ASIS and DSD of an inquiry into intelligence on Iraq's weapons of mass destruction by the Senate in June 2003, one of only three inquiries referred by a House of Parliament to the PJCIS or a predecessor committee.[31] There appear to have been only two instances of a minister referring a matter at the request of the PJCIS or a predecessor committee—the first in February 2000, on the nature, scope and appropriateness of ASIO's public reporting, and the second in March 2015, on the authorisation of access to telecommunications data to identify a journalist's source.[32]

The *IS Act* grants powers to the PJCIS to support its functions. The PJCIS may request a briefing from the head of an AIC agency or from the IGIS.[33] It may also require a person to appear before it and give evidence or produce documents if it has reasonable grounds to believe the person is capable of giving the information or documents sought, though there are some constraints on this power.[34] The PJCIS cannot use that power on the IGIS or any of the IGIS's staff.[35] For AIC agencies, the power may only be used on the heads of agencies (though an agency head may nominate a staff member).[36] In line with limits on its functions, the PJCIS must not require anyone to disclose to it any information that is operationally sensitive, or that might prejudice Australia's national security or the conduct of its foreign relations.[37] A minister responsible for an AIC agency may issue a certificate to the PJCIS to prevent a person from disclosing operationally sensitive information where a person is about to produce a document or is giving, or about to give, evidence.[38]

---

29. *IS Act*, paragraph 29(1)(b) and subsection 29(2).

30. Details of inquiries completed by the PJCIS and its predecessor committees can be accessed from PJCIS, 'Completed inquiries and reports', op. cit.

31. Australia, Senate, 'ASIO, ASIS and DSD—Joint Statutory Committee—Reference', *Journals*, 80, 18 June 2003. The other two were referrals for consideration of Bills initiated by motions moved by government ministers: Australia, House of Representatives, 'Bill—Reference to committee', *Votes and Proceedings*, 14, 21 March 2002 (Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill); Australia, House of Representatives, 'Bill—Reference to committee', *Votes and Proceedings*, 128, 15 October 2003 (Intelligence Services Amendment Bill 2003).

32. PJC on ASIO, *A watching brief: the nature, scope and appropriateness of ASIO's public reporting activities*, Australian Parliament, September 2000; PJCIS, *Inquiry into the authorisation of access to telecommunications data to identify a journalist's source*, Australian Parliament, 8 April 2015. Both referrals were in response to recommendations of the relevant committee in earlier reports: PJC on ASIO, *An advisory report on the Australian Security Intelligence Organisation Legislation Amendment Bill 1999*, Australian Parliament, May 1999, p. 44; PJCIS, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, Australian Parliament, 27 February 2015, p. 258. It is possible that other ministerial references resulted from suggestions or requests from the committee; such matters may not always be explicitly mentioned in inquiry reports.

33. *IS Act*, section 30. This section also applies to the Commissioner of the Australian Federal Police and the Secretary of the Department of Immigration and Border Protection.

34. Ibid., clauses 2 and 3 of Schedule 1.

35. Ibid., clause 2 of Schedule 1

36. Ibid., clause 3 of Schedule 1.

37. Ibid., clause 1 of Schedule 1. 'Operationally sensitive information' is defined in clause 1A of Schedule 1.

38. Ibid., clause 4 of Schedule 1. Subclause 4(4) states that the decision to issue a certificate preventing or restricting the giving of such evidence 'must not be questioned by any court or tribunal'.

The PJCIS has the power to take evidence on oath or affirmation and, subject to limitations around sensitive information, to disclose or publish evidence and the contents of documents that it receives.[39] It may only conduct a review in public with the approval of the ministers responsible for the AIC agencies.[40]

The PJCIS's reports on its reviews and inquiries are tabled in Parliament and are publicly available online, as are the annual reports on its own activities that it is required to make under the *IS Act*.[41]

d. Composition and appointment

The PJCIS is required to comprise five senators and six members of the House of Representatives. It must also have a majority of government members and be chaired by a government member. Members of the PJCIS are appointed by a resolution of each House of Parliament, following nomination by the Prime Minister (for the House of Representatives) and the Leader of the Government in the Senate (for the Senate). Nominations are to be made following consultation with each recognised non-government party represented in each House of Parliament, and with regard to 'the desirability of ensuring that the composition of the Committee reflects the representation of recognised political parties in the Parliament'. Ministers, the President of the Senate and the Speaker of the House of Representatives are not eligible to be appointed to the PJCIS. The PJCIS is re-established following the commencement of each new Parliament, and appointments are generally for the term of the Parliament.[42]

The PJCIS and its predecessors have generally comprised six government and five Opposition members, but has not included members from the crossbench.[43] This has attracted criticism from crossbench parliamentarians.[44]

e. Resourcing

The PJCIS is supported by a secretariat provided by the Department of the House of Representatives. The secretariat has two dedicated research staff. The research staff are responsible to a Committee Secretary and are supported by an administrative staff member, both of whom work across the PJCIS and another committee. Additional research staff are allocated across committees supported by the Department of the House of Representatives according to the needs of those committees at any given time. Under a standing agreement reached with the Government in 2015, the PJCIS also seconds technical advisors to its secretariat as needed from the Attorney-General's Department and other agencies, including ASIO. The *IS Act* requires all staff supporting the PJCIS to be security-cleared to the same level and at the same frequency as staff of ASIS (Positive Vetting, which is the highest level).[45]

---

39. Ibid., clauses 5, 6 and 7 of Schedule 1.

40. Ibid., clause 20 of Schedule 1.

41. PJCIS, 'Completed inquiries and reports', op. cit. Annual reports on PJCIS activities are required under section 31 of the *IS Act*. Note restrictions on disclosure to Parliament of certain information: *IS Act*, clause 7 of Schedule 1.

42. *IS Act*, section 28 and clauses 14–16A of Schedule 1.

43. Independent MP, Andrew Wilkie, is a notable exception: Parliament of Australia, 'Mr Andrew Wilkie MP', Australian Parliament website. He served on the PJCIS in the 43rd Parliament (2010–2013), during which the Labor Party relied on the support of independent MPs Andrew Wilkie, Tony Windsor and Rob Oakeshott, and that of the Australian Greens, to form a minority government.

44. See, for example, N McKim, 'Second reading speech: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015', Senate, *Debates*, 13 October 2016, pp. 1722–1726; N Xenophon, 'Second reading speech: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015', Senate, *Debates*, 13 October 2016, pp. 1729–1732.

45. PJCIS Secretariat, personal communication, 8 March 2017; IC Harris, ed., *House of Representatives practice*, 5th ed., Department of the House of Representatives, Canberra, 2005, pp. 642–643; *IS Act*, section 21.

f. Senate Standing Committees: Senate Estimates

The Legislation Committee of each Senate Standing Committee examines the estimates of proposed and additional expenditure for public service departments and other Commonwealth agencies, generally three times per year. The committees hold public hearings at which they have the opportunity to question ministers (or their representatives in the Senate) and government officials about the administration of government.[46]

These hearings provide an additional means of imposing financial accountability, though in practice the extent to which AIC agencies are subject to scrutiny through the Senate Estimates process varies. ASIO is the only AIC agency to routinely appear at Senate Estimates hearings in its own right.[47] Questions relating to the other AIC agencies tend to be addressed to the lead portfolio departments.[48] The IGIS also appears at Senate Estimates.[49]

3. Inspector-General of Intelligence and Security

The office of the IGIS was recommended by the Royal Commission on Australia's Security and Intelligence Agencies in 1984.[50] The Commissioner considered there would be merit in an independent oversight body to provide the public with greater assurance that the activities of the AIC agencies are proper, and 'to clear [agencies] or bring [them] to task, as the case may be, if allegations of improper conduct are made'.[51] The IGIS was established by the *Inspector-General of Intelligence and Security Act 1986* (*IGIS Act*) and commenced operation in February 1987.[52]

The IGIS is an independent statutory office-holder appointed by the Governor-General. Broadly, the IGIS's role is 'to ensure that the agencies act legally and with propriety, comply with ministerial guidelines and directives and respect human rights'.[53]

a. Functions

The IGIS has several main functions: AIC agency inquiry functions, intelligence and security matter inquiry functions, AIC agency inspection functions, and public interest disclosure functions.[54]

---

46. The Senate, *Consideration of estimates by the Senate's Legislation Committees*, Senate brief, 5, Australian Parliament, n.d.; The Senate, *Standing orders*, Chapter 5: Standing and select committees (see in particular orders 25 and 26), Australian Parliament, n.d.
47. ASIO appears before the Senate Legal and Constitutional Affairs Legislation Committee, which covers the Attorney-General's and Immigration and Border Protection portfolios.
48. The relevant committees are the Senate Foreign Affairs, Defence and Trade Legislation Committee and the Senate Finance and Public Administration Legislation Committee.
49. The IGIS appears before the Senate Finance and Public Administration Legislation Committee.
50. Royal Commission on Australia's Security and Intelligence Agencies; *General report*, op. cit., pp. 23–25.
51. Ibid.
52. *Inspector-General of Intelligence and Security Act 1986* (*IGIS Act*); IGIS, *Annual report 1986–87*, IGIS, 1987.
53. IGIS, 'About IGIS', IGIS website. The description summarises the objects of the *IGIS Act* (section 4) and aspects of the IGIS's inquiry functions under section 8.
54. *IGIS Act*, section 8 and subsections 9(1) and (2) (intelligence agency inquiries), subsections 9(3) and (4) (intelligence and security matter inquiries), section 9A (inspections) and section 8A (public interest disclosures).

The IGIS's AIC agency inquiry functions differ somewhat across the six AIC agencies, and are broadest in relation to ASIO.[55] The IGIS may inquire into the compliance by AIC agencies with Australian laws and any guidelines or directions given by the responsible minister; the propriety of the agencies' activities; any act or practice of an agency that may be inconsistent with or contrary to human rights law; and the procedures of the agencies relating to the redress of grievances of their employees.[56] Whether an inquiry may be initiated at the request of the responsible minister, of the IGIS's own motion, and/or in response to a complaint, differs somewhat across matters and agencies. In most instances, the IGIS may initiate an inquiry at least at the request of the responsible minister, or of the IGIS's own motion.[57] The IGIS requires ministerial approval to inquire into a matter relating to a Commonwealth agency that occurred outside Australia or before commencement of the *IGIS Act*.[58]

The Prime Minister may request that the IGIS inquires into a matter relating to an AIC agency, or an intelligence or security matter relating to any Commonwealth agency, and the IGIS must generally comply with such a request.[59] The IGIS may not, of its own motion, inquire into an intelligence or security matter relating to a non-AIC agency.

The IGIS may conduct inspections of AIC agency records as the IGIS considers appropriate, to ensure agencies are acting legally, with propriety and in accordance with human rights.[60] The IGIS indicates that its inspections enable it to 'identify issues or concerns before they develop into systemic problems that could require major remedial action'.[61] The IGIS's inspection activities include reviewing records relating to ASIO's use of special powers, including supporting materials accompanying warrant applications; reviewing ministerial authorisations issued to ASIS, AGO and ASD; reviewing ASIS operational files and its application of weapons guidelines; and monitoring agency compliance with relevant legislation.[62]

The IGIS is also responsible for overseeing AIC agency handling of public interest disclosure matters and investigating such matters where they relate to AIC agencies.[63]

---

55. These differences reflect the differences in functions across the AIC, particularly between the collection and assessment of intelligence, and foreign and domestic focus.

56. *IGIS Act*, section 8. For ASIO, the IGIS also has inquiry functions under that section relating to the effectiveness and appropriateness of procedures ASIO has in place relating to the propriety of its activities (subparagraph 8(1)(a)(iv)), certain matters relating to ASIO's security assessment function (paragraph 8(1)(c)) and the justification for the collection and communication of certain intelligence (paragraph 8(1)(d)). Note that section 9AA places restrictions on the IGIS's functions, including in relation to matters that occurred outside Australia.

57. Ibid., section 8. An inquiry under paragraph 8(1)(c) (relating to a security assessment) may only be undertaken at the minister's request.

58. Ibid., paragraph 9AA(a). Paragraphs 9AA(b) and (c) prohibit the IGIS from inquiring into action taken by a minister and matters that are, or could be, the subject of a review by the Security Division of the Administrative Appeals Tribunal, except in very limited circumstances.

59. Ibid., section 9.

60. Ibid., sections 4 (objects of the Act), 9A (inspections).

61. IGIS, 'Frequently asked questions' (under 'How does the IGIS ensure that Australian intelligence agencies act legally and with propriety?'), IGIS website.

62. Ibid. The IGIS's annual reports detail inspections carried out each year. See, for example, IGIS, *Annual report 2016–17*, op. cit., pp. 13–34.

63. *IGIS Act*, section 8A; *Public Interest Disclosure Act 2013*.

b. Powers and performance of functions

The IGIS has significant powers, broadly comparable to a Royal Commission, to support the performance of its inquiry functions, including powers to obtain information and documents, take evidence and enter Commonwealth agency premises.[64] Due to the sensitive nature of the matters and activities into which the IGIS may inquire, inquiries are required to be conducted in private.[65]

The IGIS must produce reports on its inquiries and provide them to the relevant agency heads (unless the matter concerns an agency head) and the responsible ministers.[66] Summaries of inquiries are generally included in the IGIS's annual reports, and unclassified versions of inquiry reports are sometimes published on the IGIS's website.[67] The current IGIS and former holders of the office have recognised the importance of making public as much of the IGIS's work as possible within security constraints.[68]

If an agency head has taken, or proposes to take, action in response to conclusions or recommendations in an IGIS inquiry report, he or she must provide details of any such action to the IGIS. If the IGIS does not consider that adequate and appropriate action has been taken in a reasonable period, the IGIS may prepare a report on the matter for the responsible minister or the Secretary of the Department of Defence.[69]

The IGIS has full access to information and records held by the AIC agencies for the purpose of fulfilling its inspection functions.[70] The responsible minister must provide the IGIS with copies of any guidelines or directions issued to ASIO, ASIS, AGO and ASD as soon as practicable.[71] AIC agencies must provide the IGIS with copies of reports given to a responsible minister or the Secretary of the Department of Defence if requested to do so by the IGIS.[72] AIC agencies must also notify the IGIS of the authorisation of and use of particular powers. For example, copies of emergency warrants or authorisations made by agency heads (in place of a minister) must be provided, and ASIO must notify the IGIS of any use of force against a person during the execution of a warrant, the authorisation of a 'special intelligence operation', and matters relating to its special terrorism powers.[73]

In 2006, the IGIS noted that 60 to 70 per cent of its resources were devoted to proactive inspection activities and 30 to 40 per cent to inquiry work.[74] More recent data on the proportional distribution of resources does not appear to have been made public.

---

64. *IGIS Act*, Division 3 of Part II.
65. Ibid., subsection 17(1).
66. Ibid., sections 21 and 22.
67. IGIS, 'Annual reports', and 'Public reports', IGIS website.
68. IGIS, *Corporate plan 2016–20*, IGIS, 2016, p. 4; V Thom, 'Reflections of a former Inspector General of Intelligence and Security', *AIAL Forum*, 83, April 2016, pp. 11–17.
69. *IGIS Act*, section 24. 24A makes equivalent provision for reports given to the responsible minister or the Secretary of the Department of Defence.
70. Ibid., section 9A.
71. Ibid., section 32B; *ASIO Act*, section 5A and subsections 8(6) and 8A(6).
72. *IGIS Act*, section 32A.
73. *IS Act*, section 9B and *ASIO Act*, section 29; *ASIO Act*, sections 31A (use of force), 35PA (special intelligence operations; see also section 35Q), and 34ZI and 34ZJ (special powers relating to terrorism offences).
74. I Carnell and N Bryan, 'Watching the watchers: how the Inspector-General of Intelligence and Security helps safeguard the rule of law' Administrative Review Council, 2006.

c. Appointment

The IGIS is appointed by the Governor-General, and may be appointed on a full or part-time basis.[75] The Prime Minister is required to consult with the Leader of the Opposition before recommending an appointee to the Governor-General.[76] The IGIS may be appointed for a period of up to five years, and may be re-appointed no more than twice.[77] If a person was appointed to the office of IGIS as a Judge and ceases to be a Judge, the Governor-General may terminate the person's appointment.[78] Otherwise, the Governor-General may terminate the IGIS's appointment by reason of misbehaviour or physical or mental incapacity.[79]

d. Resourcing

As at 30 June 2017, the IGIS was supported by 15 ongoing public service employees (including an Assistant IGIS), four of whom worked part-time.[80] The IGIS's budgeted expenses for 2017–18 amount to AUD3.32 million.[81] Unfortunately, it is not possible to determine the staffing and resources of the IGIS as a proportion of those of the AIC agencies because that information is not made available for the three defence intelligence agencies.

While the IGIS's key functions have remained the same in recent years, the powers of the AIC agencies, most notably ASIO, have expanded in that time. So, while the nature of the IGIS's oversight role has not changed, the breadth of powers it now oversees (and in the current security environment, possibly the increased use of some powers[82]) has placed additional resourcing pressures on the agency. However, the IGIS noted in its *Annual Report 2015–16* that it had received additional funding as part of the package in the 2014–15 Mid-Year Economic and Fiscal Outlook, and had been exempted from the efficiency dividend from 2015–16 onwards.[83] It also stated that this was allowing additional staff to be recruited 'to enable the office to continue to provide a comprehensive and effective oversight program'.[84]

---

75. *IGIS Act*, sections 6 and 63. Section 6A allows the Prime Minister to appoint a person to act as IGIS during a vacancy or absence.
76. *IGIS Act*, section 6.
77. Ibid., section 26.
78. The Constitution provides a mechanism for a judge to be removed 'on the ground of proved misbehaviour or incapacity': *Australian Constitution*, section 72.
79. Ibid., section 30.
80. IGIS, *Annual Report 2016–17*, p. 53.
81. Australian Government, *Portfolio budget statements 2017–18: budget related paper no. 1.14: Prime Minister and Cabinet Portfolio*, Commonwealth of Australia, Canberra, 2017, p. 255.
82. ASIO is the only one of the operational intelligence agencies that produces a public annual report, and that report is only required to contain details on the number of warrants/authorisations for selected powers (*ASIO Act*, section 94).
83. IGIS, *Annual report 2015–16*, op. cit., p. v. For information on the budget changes, see C Barker, 'Countering terrorism and violent extremism', *Budget review 2015–16*, Research paper, 2014–15, Parliamentary Library, Canberra, May 2015.
84. Ibid. While additional resourcing has been provided, the IGIS has experienced delays to recruitment due to lengthy security clearance processes, leading to salary underspends in 2015–16 and 2016–17: Ibid., p. 10; IGIS, *Annual report 2016–17*, op. cit., p. 60.

4. Judicial oversight

a. Warrants

Judicial oversight of, or involvement with, the authorisation of AIC agency powers is limited. Ministerial authorisation is required for certain activities of ASIS, AGO and ASD, and subject to the exception noted below, warrants for ASIO's exercise of powers are issued by the Attorney-General.[85]

ASIO has access to special powers in relation to terrorism offences, under which it may obtain a warrant either to question a person without detention for a maximum of 24 hours (Questioning Warrants), or to detain a person for questioning for a maximum of seven continuous days (Questioning and Detention Warrants).[86] To apply for such a warrant, the Director-General of ASIO must obtain the consent of the Attorney-General, and then apply to an 'issuing authority' for the warrant's issue.[87] An issuing authority is a current federal magistrate or judge of a federal, state or territory court who has been appointed by the Attorney-General, though there is the capacity for the Attorney-General to declare persons in a specified class to be issuing authorities regardless of their position or expertise.[88] Once the warrant is granted, the person is brought before a 'prescribed authority'—usually a former judge of a state or territory District or Supreme Court—who oversees and supervises exercises of power under the warrant.[89]

Importantly, a judge appointed as an issuing authority or prescribed authority is acting in a personal, not judicial, capacity.[90] Furthermore, the role played by both is limited. To issue a warrant, an issuing authority need only be satisfied that there are reasonable grounds for believing it will substantially assist the collection of intelligence that is important in relation to a terrorism offence.[91] He or she does not have to consider whether there may be other effective methods for collecting the evidence, or, in the case of a Questioning and Detention Warrant, whether detention is necessary—these are matters considered by the Attorney-General in consenting to the warrant request.[92] A judge acting as a prescribed authority can

85. *IS Act*, sections 9 and 9A (sections 9B and 9C allow agency heads to make emergency authorisations that remain in force for a shorter period if ministers are unavailable); *ASIO Act*, sections 25, 25A, 26, 27, 27AA, 27A, 27C and 35C (section 29 allows the head of ASIO to issue an emergency warrant for most warrant types that remains in force for a shorter period in certain circumstances); *Telecommunications (Interception and Access) Act 1979*, Part 2–2 (including emergency warrants by head of ASIO under section 10).

86. For Questioning Warrants: *ASIO Act*, sections 34D, 34E and subsection 34R(6). The maximum time limit is extended from 24 to 48 hours if a person is being questioned with an interpreter present: subsection 34R(11). For Questioning and Detention Warrants: *ASIO Act*, sections 34F, 34G and 34S.

87. As at October 2016, ASIO had never applied for a Questioning and Detention Warrant: R Gyles, *Certain questioning and detention powers in relation to terrorism*, Independent National Security Legislation Monitor, October 2016, p. 40.

88. *ASIO Act*, subsection 34AB(3).

89. *ASIO Act*, section 34B. Where the minister is of the view there are insufficient people to act as a prescribed authority, he or she may appoint a currently serving judge, or a President or Deputy President of the Administrative Appeals Tribunal: subsections 34B(2) and (3).

90. *ASIO Act*, subsection 34ZM(2); L Burton and G Williams, 'The integrity function and ASIO's extraordinary questioning and detention powers', *Monash University Law Review*, 38(3), 2012, p. 4; Australian Human Rights Commission (AHRC), 'A human rights guide to Australia's counter-terrorism laws', AHRC website, 2008.

91. *ASIO Act*, sections 34E and 34G.

92. The Attorney-General must be satisfied that relying on other methods of collecting the intelligence would be ineffective, and in the case of a Questioning and Detention Warrant, that if not detained, the person may alert a person involved in a terrorism offence that the offence is being investigated, may not appear for questioning, or may destroy, damage or alter a record or thing (subsections 34D(4) and 34F(4)); Burton and Williams, 'The integrity function and ASIO's extraordinary questioning and detention powers', op. cit., pp. 4–5.

supervise and steer the questioning process, but these powers are also restricted—for example, a prescribed authority cannot generally make a direction inconsistent with the terms of a warrant.[93]

b. Role of the courts

Decisions made in relation to special terrorism powers warrants are not subject to merits review, and the *ASIO Act* expressly excludes the jurisdiction of state and territory courts while the warrant is in force.[94] Decisions under the *ASIO Act*, the *IS Act* and other intelligence legislation are also excluded from the statutory judicial review framework set out in the *Administrative Decisions (Judicial Review) Act 1977*.[95] However, a person may apply to the Federal Court of Australia or High Court of Australia for judicial review of actions by officers of the Commonwealth to ensure these actions are carried out within their statutory and constitutional limits.[96]

The only specialised tribunal providing oversight in relation to intelligence matters is the Security Division of the Administrative Appeals Tribunal (AAT), which conducts merits review of most categories of adverse security assessments made by ASIO.[97] Hearings in this division are conducted in private, and the Attorney-General may issue a public interest certificate to require sensitive national security information to be withheld from the applicant.[98] Judicial review of the process of ASIO making a security assessment is also available through the Federal Court and High Court.[99]

c. Immunities and prosecutions

Staff members and agents of ASIS, ASD and AGO have immunity from civil and criminal liability for activities carried out by the agencies in the proper performance of their functions, which might otherwise be prohibited by the unintended consequences of certain Australian laws.[100] This immunity can only be overridden by other Commonwealth, state or territory laws if those laws explicitly provide otherwise.[101] Similarly, ASIO officers participating in a 'special intelligence operation' (SIO) are not subject to civil or criminal liability in relation to conduct engaged in during the course of, and for the purposes of, the SIO, and in accordance with the SIO authority. There are exceptions to this immunity for conduct which causes death or serious injury; constitutes torture; involves the commission of a sexual offence; or in

93. Burton and Williams, 'The integrity function and ASIO's extraordinary questioning and detention powers', op. cit., p. 5.

94. *ASIO Act*, section 34ZW.

95. *Administrative Decisions (Judicial Review) Act 1977* (Cth), Schedule 1.

96. Access to the original jurisdiction of the High Court of Australia is provided for under section 75(v) of the *Constitution*, and the Federal Court of Australia under section 39B(1) of the *Judiciary Act 1903* (Cth). For more information, see: Administrative Review Council, *The scope of judicial review—report to the Attorney-General*, report no. 47, April 2006, pp. 5–7.

97. *ASIO Act*, Division 4 of Part 4; ASIO, 'ASIO's security assessment function', op. cit.; G Downes, 'The Security Appeals Division of the Administrative Appeals Tribunal—functions, powers and procedures', address to the National Security Law Course, University of Sydney, 13 September 2006.

98. G Downes, ibid.

99. ASIO, 'ASIO's security assessment function', op. cit.

100. *Intelligence Services Act 2001* (Cth), section 14.

101. Ibid., subsection 14(2AA).

which the participant induces another person to commit an offence that the other person would not have intended to commit.[102]

Australian courts have prosecuted intelligence officers, and other persons who have been entrusted with intelligence information, for unauthorised disclosures of such information.[103]

d. Inadmissibility of evidence

The courts have previously ruled as inadmissible intelligence sought to be admitted in evidence in criminal prosecutions, due to impropriety in the process of obtaining the intelligence. An example is the matter of *R v Ul-Haque* [2007] NSWSC 1251, in which evidence of admissions made by the defendant in a counter-terrorism prosecution to ASIO and Australian Federal Police (AFP) officers was excluded by the NSW Supreme Court under section 138 of the *Evidence Act 1995* (Cth) (which provides for the exclusion of improperly or illegally obtained evidence) and section 84 (which excludes evidence of admissions that were influenced by 'violent, oppressive, inhuman or degrading conduct').[104] In finding the evidence inadmissible, the trial judge was highly critical of the conduct of ASIO officers in the case, finding them to have 'assumed unlawful powers of direction, control and detention'.[105] The proceedings were subsequently discontinued.[106]

5. Information sharing and cooperation between oversight bodies

The functions of the PJCIS and the IGIS are complementary rather than overlapping, and the PJCIS is prohibited from seeking 'operationally sensitive information', meaning the scope for cooperation between the two is fairly limited. However, some information is shared between them, mainly from the IGIS to the PJCIS.

As noted above, the PJCIS may request briefings from the IGIS. The IGIS makes submissions to, and provides evidence at hearings for, the PJCIS's reviews of AIC agency administration and expenditure. The IGIS will often also provide evidence to PJCIS inquiries into legislation that is being proposed or reviewed which is relevant to the IGIS's oversight role or the functions of the AIC agencies more broadly, and to reviews conducted by the INSLM.[107] The IGIS's annual report for 2015–16 describes its cooperation with the AAT and the Australian Information Commissioner as assisting in 'enhancing oversight and promoting good practice in the [AIC] agencies'.[108]

---

102. *ASIO Act*, section 35K. Subsection 35K(2) allows the minister to issue further requirements/conditions on this immunity by legislative instrument; to date, this has not been done.

103. Examples include: *R v Scerba (No 2)* [2015] ACTSC 359, in which a Department of Defence graduate employee was convicted of downloading a classified sensitive document from the Defence Secret Network (DSN) and posting it to an image-sharing website; *Sievers v R* [2010] ACTA 9, in which an ASIO officer was convicted of communicating information in his possession which had been prepared or acquired on behalf of ASIO in connection with its functions or performance; *R v Lappas* (2003) 152 ACTR 7, in which an employee of the Defence Intelligence Organisation was convicted of giving classified documents to an unauthorised person to sell to a foreign country.

104. *Evidence Act 1995*; *R v Ul-Haque* [2007] NSWSC 1251.

105. *R v Ul-Haque* at 95.

106. 'Terror charges against student dropped', SBS News website, 12 November 2007.

107. See, for example, IGIS, Submission to PJCIS, *Review of administration and expenditure no. 15 (2015–16)*, 8 December 2016; IGIS, Submission to PJCIS, *Inquiry into the Counter-Terrorism Legislation Amendment Bill (No. 1) 2014*, 10 November 2014; IGIS, Submission to INSLM, *Review of certain questioning and detention powers in relation to terrorism*, July 2016.

108. IGIS, *Annual report 2015–16*, op. cit., p. 8.

The INSLM may consult with the IGIS when performing functions relating to Australia's counter-terrorism and national security legislation.[109] The PJCIS may refer a matter to the INSLM that it becomes aware of in the course of performing its functions.[110]

C. Recent developments and reform proposals

1. Jurisdiction of the PJCIS

The PJCIS's functions have gradually expanded in recent years, in response to its own recommendations.[111] However, those changes have largely related to functions other than AIC agency oversight; in particular, expansion of its legislative review functions and the inclusion of a new function to monitor and review the AFP's counter-terrorism functions.[112]

2. PJCIS amendment Bill

Opposition senator Penny Wong introduced the Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 on 10 August 2015. The Bill lapsed ahead of the 2016 federal election but was restored to the notice paper on 31 August 2016.[113] It would amend the composition, functions and powers of the PJCIS.

The Bill would allow the PJCIS to conduct own-motion inquiries into matters relating to one or more of the AIC agencies, providing it had first consulted the responsible minister. It would not affect the existing restrictions preventing the PJCIS from inquiring into operational matters.

As noted above, the PJCIS must currently comprise five senators and six members of the House of Representatives, have a government majority, and a government chair. The Bill would retain the requirement for a government majority, but relax the Senate/House of Representatives ratio so that there would be one senator and one member of the House of Representatives from each of the government and the Opposition, with the remaining members able to be drawn from either House of Parliament. The purpose of this proposed change is to provide more flexibility to ensure the PJCIS has the most qualified membership. However, the Bill would not require any cross-bench representation. Australian Greens senator Nick McKim stated in the second reading debate that the Greens would move an amendment requiring a senator who is not from the government or the Opposition to be one of the eleven members of the PJCIS.[114]

---

109. *INSLM Act*, subsection 10(2).

110. Ibid., section 7A.

111. See the PJCIS's advisory reports on the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*, the *Australian Citizenship Amendment (Allegiance to Australia) Bill 2015*, the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* and the *Criminal Code Amendment (High Risk Terrorist Offenders) Bill 2016*.

112. These changes are reflected in the *IS Act*, paragraphs 29(1)(baa), (bab), (bac) and (be) (AFP function); and 29(1)(bc) and (ca) (legislative reviews); *Criminal Code Act 1995*, subsection 119.3(7) (review of areas declared by Foreign Minister); *Australian Citizenship Act 2007*, subsection 35AA (declaration of a terrorist organisation for the purposes of that Act).

113. Parliament of Australia, 'Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 homepage', Australian Parliament website. The Bill draws on work completed by former senator, John Faulkner. See: J Faulkner, *Surveillance, intelligence and accountability: an Australian story*, 23 October 2014.

114. N McKim, 'Second reading speech: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015', Senate, *Debates*, 13 October 2016, pp. 1722–1726.

Amongst other changes, the Bill would also require the IGIS to provide the PJCIS with copies of its inquiry reports within three months of giving them to the Prime Minister or responsible minister, and to add the INSLM and the National Security Adviser (in the Department of the Prime Minister and Cabinet) to the list of office-holders from whom the PJCIS can request a briefing.

3. 2017 Independent Intelligence Review

The most recent independent review of the AIC agencies was completed in June 2017, with a public version of the report released in July 2017.[115] The report recommended several changes relating to oversight of Australia's intelligence agencies.

The reviewers assessed that 'the intelligence enterprise that supports Australia's national security is no longer limited to the six AIC agencies' and considered that a more appropriate frame of reference would be a 'National Intelligence Community' comprising the six AIC agencies, the Australian Criminal Intelligence Commission (ACIC), the Australian Transaction Reports and Analysis Centre (AUSTRAC), and parts of the AFP and the Department of Immigration and Border Protection (DIBP).[116] Accordingly, they recommended that the jurisdiction of both the PJCIS and the IGIS be expanded to include AUSTRAC in its entirety and the intelligence functions of the AFP, ACIC and the DIBP.[117]

The reviewers also recommended that the:

- the PJCIS be given the ability to request that the IGIS conduct an inquiry into the legality and propriety of particular operational activities of any of the ten above-mentioned agencies and report to the PJCIS, the Prime Minister and the responsible minister (in line with the powers of the New Zealand ISC)
- the PJCIS be given the ability to initiate its own inquiries into the administration and expenditure of the ten above-mentioned agencies
- the PJCIS be empowered to request briefings from the INSLM and refer matters to the INSLM for report
- the IGIS and the Director-General of the proposed Office of National Intelligence be required to provide regular briefings to the PJCIS and
- IGIS's resources should be significantly increased from 17 to around 50 full-time staff.[118]

115. PM&C, *2017 Independent Intelligence Review*, op. cit.; M Turnbull (Prime Minister), *Press Conference with the Attorney-General, Senator the Hon. George Brandis QC, Minister for Immigration and Border Protection, The Hon. Peter Dutton MP and Minister for Justice, The Hon. Michael Keenan MP Parliament House, Canberra*, media release, 18 July 2017.

116. PM&C, *2017 Independent Intelligence Review*, op. cit., pp. 46–48, 115.

117. Ibid., p. 116.

118. Ibid., pp. 111–125. The reviewers also recommended changes to: the architecture of Australia's intelligence arrangements (including expanding the ONA into an Office of National Intelligence and making ASD a separate statutory agency reporting to the Minister for Defence); capability and funding; and the legislation that governs the agencies.

While not a recommendation of the review, on the same day the report was released, the Prime Minister also announced the creation of a new Home Affairs portfolio (modelled broadly on the UK Home Office) that will bring together Australia's immigration, border protection, law enforcement and domestic security agencies under a single portfolio.[119]

A task force led by the Department of the Prime Minister and Cabinet will consider the recommendations of the independent review and then manage in tandem the implementation of those that are adopted and the establishment of the Home Affairs portfolio.[120]

119. Turnbull, *Press Conference*, op. cit.; M Turnbull (Prime Minister), G Brandis (Attorney-General), P Dutton (Minister for Immigration and Border Protection), and M Keenan (Minister for Justice), *A strong and secure Australia*, media release, 18 July 2017. On the Home Affairs portfolio, see further C Barker and S Fallon, *What we know so far about the new Home Affairs portfolio: a quick guide*, Research paper series, 2017–18, Parliamentary Library, Canberra, 2017.

120. Ibid.

CANADA

A. Overview of intelligence agencies

The Government of Canada's intelligence-related activities and structures span many organizations, some of which are listed in two locations:

- Schedule 3 of the *Security of Canada Information Sharing Act*, which identifies 17 different federal institutions that acquire, analyze and share information for the purpose of protecting Canada against activities that undermine its security; and
- Canada's 2013 national counter-terrorism strategy, which lists 21 departments and agencies with counter-terrorism responsibilities.[121]

Given that intelligence is created and consumed for purposes other than national security, it is likely that these two lists fail to capture the entire Canadian security and intelligence community.

Canada's core intelligence collector agencies comprise the following:[122]

- *Communications Security Establishment* (CSE), which is Canada's foreign signals intelligence agency. CSE's workforce stands at roughly 2,000 employees.[123] Operating as a separate agency under the Department of National Defence (DND),[124] CSE is mandated under section 273.64(1) of the *National Defence Act* to:
  - acquire and use information from the global information infrastructure to provide foreign intelligence;
  - provide advice, guidance and services to protect electronic information and information infrastructure of importance to the Government of Canada; and
  - provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

  To shield itself from liability under Part VI of the *Criminal Code*, which prohibits unauthorized interception of private communications, CSE seeks authorization from the Minister of National Defence to undertake foreign intelligence collection and cyber defence activities where there is an unavoidable risk of such interception. These ministerial authorizations have effect for no more than a year and come with a set of conditions that CSE is expected to satisfy.

- *Canadian Security Intelligence Service* (CSIS), which provides intelligence on threats to the security of Canada using primarily, but by no means exclusively, human sources. With a workforce of over 3,200,[125] CSIS is part of the Public Safety Canada (PSC) portfolio[126] and is mandated under

---

121 See Public Safety Canada, "Annex A: Roles and Responsibilities Relating to Counter-terrorism," *Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy*, 2013.

122 Canada's Financial Transactions Analysis and Reporting Centre (FINTRAC) has not been included in this list because although it is a financial intelligence agency, it does not have capabilities or authorities to actively target and collect the data it receives. Rather, Canada's *Proceeds of Crime (Money Laundering) and Terrorism Financing Act* imposes reporting requirements on financial institutions and other affected sectors.

123 This figure represents an average employee population. See Government of Canada, *Inventory of Government Organizations*. To access CSE "People Management Data," readers will need to scroll down to "National Defence" and click on "Communications Security Establishment."

124 Prior to the issuing of an order in council making CSE a stand-alone agency in December 2011, CSE reported to the Minister of National Defence through the Deputy Minister of National Defence on financial and administrative matters and through the National Security Advisor on operational and policy matters. CSE now reports directly to the Minister of National Defence.

125 See Canadian Security Intelligence Service, "A Unique Workplace," *Public Report 2014–2016*.

126 Public Safety Canada comprises the Canada Border Services Agency, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, Correctional Service Canada, and the Parole Board of Canada.

section 12 of the *Canadian Security Intelligence Service Act* (CSIS Act). To use certain intrusive investigative techniques, CSIS is required under section 21 of the CSIS Act to obtain a warrant from the Federal Court, which has designated a group of judges to examine CSIS applications in *ex parte* (from one party) and *in camera* (closed) hearings. In 2015, under two separate bills,[127] the CSIS Act was amended to, among other things, give the Federal Court jurisdiction to issue warrants enabling the Service to use intrusive measures on overseas operations and to authorize CSIS to engage in threat reduction activities.

- *Canadian Forces Intelligence Command* (CFINTCOM), which uses a full range of collection methods to provide defence intelligence to the Canadian Armed Forces and DND. CFINTCOM receives its direction from the Chief of Defence Intelligence, whose authority derives from the *National Defence Act*. Most, but not all, of CFINTCOM's intelligence collection targets are foreign and, thus, most of its collection and information-sharing activities are conducted under Crown prerogative.[128] CFINTCOM's counter-intelligence activities can, however, entail collection of information on Canadians. At present, DND relies on internal accountability mechanisms in place to ensure that CFINTCOM's counter-intelligence activities are lawful and comply with departmental policies and regulations. However, some elements of external accountability may be put in place under proposed legislation that is discussed below.
- *Royal Canadian Mounted Police* (RCMP), which, as Canada's federal law enforcement agency, is responsible under the *Security Offences Act* to conduct criminal investigation of security offences, such as facilitation of or engagement in terrorism or espionage. The RCMP – which is also contracted to provide police services in every province and territory in Canada, save Ontario and Quebec – derives its mandate from the *Royal Canadian Mounted Police Act* (RCMP Act). Its workforce stands at around 6,500.[129]

B. Oversight summary

While the ministers of public safety and national defence are responsible for activities that take place within their respective portfolios, the prime minister is ultimately accountable to Parliament on national security matters. The prime minister thus chairs the Cabinet Committee on Intelligence and Emergency Management.[130]

---

127 Bill C-44, An Act to amend the Canadian Security Intelligence Service Act and other Acts, received Royal Assent on 23 April 2015, and Bill C-51, An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts, received Royal Assent on 18 June 2015. See Holly Porteous, Dominique Valiquet and Julie Béchard, *Legislative Summary of Bill C-44: An Act to amend the* Canadian Security Intelligence Service Act *and other Acts*, Publication no. 41-2-C44-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 28 November 2014. See also Julie Béchard, Tanya Dupuis, Christine Morris, Dominique Valiquet and Holly Porteous, *Legislative Summary of Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, Publication no. 41-2-C51-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 19 June 2015.

128 Department of National Defence, "Executive Summary," *Defence Intelligence Review: Report to the CDS*, Ottawa, 20 May 2004, p. iv. Released under Access to Information and Privacy request number A0280236.

129 Government of Canada, *Inventory of Government Organizations*. To access the RCMP's "People Management Data," readers will need to scroll down to "Public Safety and Emergency Preparedness" and click on "Royal Canadian Mounted Police."

130 The Minister of Public Safety and Emergency Preparedness chairs another important cabinet committee, the Cabinet Committee on Canada in the World and Public Security, which is responsible for issues related to domestic and global security.

The National Security and Intelligence Advisor to the Prime Minister (NSIA)[131] serves as the prime minister's eyes and ears on security and intelligence issues. The NSIA also coordinates the federal security and intelligence community but must rely on suasion alone to do so, as he or she is an appointee with no statutory authorities. Assisted by a deputy NSIA, the NSIA oversees the Privy Council Office's[132] Intelligence Assessment Secretariat and its Security and Intelligence Secretariat.

At present, the executive branch relies on three expert review bodies to investigate complaints and examine the lawfulness of the activities of Canada's intelligence and national security agencies (discussed in greater detail below):

- the Security Intelligence Review Committee (SIRC);
- the Office of the Communications Security Establishment Commissioner (OCSEC); and
- the Civilian Review and Complaints Commission for the RCMP (CRCC).

Each of these review bodies has been established by statute. Though each claims independence, all three are required by law to submit their annual reports to responsible ministers[133] and all are subject to executive branch direction or constraint.[134] Ministers must table unclassified versions of these annual reports in each house of Parliament during the first 15 days on which that house is sitting after the day they are received.

None of the intelligence and national security agencies is required to provide an annual report to Parliament. CSIS does, nonetheless, prepare public reports. However, the timing of these reports varies, and the organization's most recent report covers a two-year time frame. The content of these reports has shrunk in size over time and often focuses on broad generalities.

---

131 On 28 April 2017, the title of the National Security Advisor to the Prime Minister was changed to National Security *and Intelligence* Advisor to the Prime Minister [emphasis added by author]. See Privy Council Office, *PC Number: 2017-0411*, 28 April 2017.

132 The Privy Council Office is part of the Public Service and provides non-partisan support to the prime minister as well as Cabinet and its decision-making structures.

133 The CSE Commissioner reports to the Minister of National Defence, while the chairs of SIRC and of the CRCC report to the Minister of Public Safety and Emergency Preparedness. Since all of Canada's provinces and territories, save Ontario and Quebec, contract the RCMP for policing services, the chair of the CRCC is also required to provide annual reports to provincial ministers who have primary responsibility for policing and have entered into such arrangements. Each annual report, copied to the Minister of Public Safety and Emergency Preparedness and the RCMP Commissioner, sets out the number and nature of complaints relating to RCMP conduct that occurred in the province in question, describes how those complaints were disposed of, and identifies any trends.

134 For example, arguing that the existing law enables cooperation between his organization and SIRC, the CSE Commissioner noted the following in his 2011-2012 Annual Report:

> Paragraph 273.63(6) of the *National Defence Act* allows the Governor in Council to authorize me to engage in any related activity. Article 54 of the *Canadian Security Intelligence Service Act* allows the Minister of Public Safety and Emergency Preparedness to request from SIRC a 'special report concerning any matter that relates to the performance of its duties and functions.' I am of the opinion that my office and SIRC could, by virtue of these provisions, be asked to conduct a joint review or complementary reviews of certain activities involving both CSEC and CSIS.

See Office of the Communications Security Establishment Commissioner, "Commissioner's Message," *2011-2012 Annual Report* June 2012. At present, section 45.34 of the *Royal Canadian Mounted Police Act* stipulates that, prior to undertaking a self-initiated review, the Commissioner of the CRCC must provide a rationale to the Minister of Public Safety and Emergency Preparedness for his or her belief that the Commission is sufficiently resourced to undertake the review and why the review does not duplicate the work of any other review or inquiry.

The primary parliamentary reporting obligation for federal departments and agencies takes the form of budget documentation.[135] Federal organizations request parliamentary approval to spend funds through the estimates process and outline their funding needs in main and supplementary estimates. In order to provide parliamentarians with more detailed information about what they intend to achieve with the resources provided to them, departments and agencies prepare departmental plans. When the fiscal year is complete, they explain in departmental performance reports how much was spent and what was achieved.

However, neither CSIS nor CSE prepare departmental plans and performance reports. Instead, parliamentarians are provided high-level financial information, as outlined in main and supplementary estimates. Thus, other than what they can glean through questioning officials in public committee hearings, parliamentarians have no information about these agencies' plans, activities or results, despite the significant funds being provided to them. When, during the year through supplementary estimates, these agencies request additional funds – which can be substantial – little or no explanation is provided. Without additional information, it is very difficult for parliamentarians to provide effective financial oversight of these organizations.

On 22 June 2017, Bill C-22, An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts (hereafter, the *National Security and Intelligence Committee of Parliamentarians Act* or NSICPA), received Royal Assent.[136] Having come into force on 6 October 2017,[137] the NSICPA will create another executive review body – the National Security and Intelligence Committee of Parliamentarians (NSICOP) – which will report to the prime minister. NSICOP members will have access to classified information, including legal opinions, but will also be permanently bound to secrecy.

Some have expressed disappointment with the NSICPA, arguing that, by creating a committee of parliamentarians rather than a parliamentary committee, it will only bring Canada in line with where the United Kingdom was in 2012, when that country's Intelligence and Security Committee was still part of the executive branch. In Canada, the notion of a parliamentary review committee permitted to hear and view classified information has been raised in numerous commissions of inquiry, starting with the 1969 Mackenzie Commission, which examined the state of Canada's security system in the aftermath of a series of Soviet spy scandals.

Since neither the Senate nor the House of Commons has committees whose members are authorized to access classified information, Canada's legislature is unable to comprehensively review national security and intelligence activities. Instead, the legislative branch relies on a number of "officers of Parliament" that can, if necessary, gain access to certain classified information and facilities relevant to each officer's

---

135 To read further on the financial cycle of Canada's parliament, see Alex Smith, *The Parliamentary Financial Cycle*, Publication no. 2015-41-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 27 January 2016.

136 For a summary of the original text of Bill C-22, see Holly Porteous and Dominique Valiquet, *Legislative Summary of Bill C-22: An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts*, Publication no. 42-1-C22-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 22 August 2016.

137 "Order Fixing the Day on which this Order is made as the Day on which the Act Comes into Force," SI/2017-63, *Canada Gazette*, Part II, Vol. 151, No. 21, October 18, 2017, p. 2902.

mandate. Appointed by orders in council,[138] these officers undertake statutorily assigned review work and report their findings to Parliament. Although officers of Parliament may work at the classified level, the reports they submit to Parliament and any subsequent parliamentary testimony they provide must be unclassified.

Neither the Senate nor the House of Commons has established a standing committee whose sole remit is to examine questions of national security. Instead, the Standing Senate Committee on National Security and Defence and the House of Commons Standing Committee on Public Safety and National Security treat national security issues as part of a broader menu of potential study topics. Given their respectively broad remits, these two committees generally address national security matters, including intelligence, in an episodic manner.

The provisions in the NSICPA directing the Senate and the House of Commons to refer NSICOP annual and special reports to these two committees for study will routinize the attention Parliament pays to national security. However, unless these committees' mandates are narrowed down, there are no guarantees that NSICOP reports will be subject to in-depth examination and debate.

From time to time, special parliamentary committees have been struck to dive deeper into national security policy. An example of this is the Special Senate Committee on the Anti-terrorism Act, which was created in 2004 as part of the mandated review of anti-terrorism laws passed in 2001. However, the committee was dissolved in 2013.[139]

C. Executive oversight

1. Security Intelligence Review Committee

SIRC was created in 1984 under the CSIS Act.[140] SIRC comprises a chair plus not fewer than two and not more than four members. Committee members are all privy councillors appointed by the Governor in Council after consultation by the prime minister with the leaders of the opposition parties. SIRC meets approximately nine times a year to set priorities and review the work of its staff. Under section 39(2) of the CSIS Act, SIRC has unfettered access to all information under the control of CSIS, save Cabinet confidences.

---

138 An order in council is a legal instrument made by the Governor in Council pursuant to a statutory authority or, less frequently, the royal prerogative. All orders in council are made on the recommendation of the responsible minister of the Crown and take legal effect only when signed by the Governor General. See Library and Archives Canada, *Orders-in-Council*.

139 Some members of the committee were unhappy about the dissolution of the Special Senate Committee on the Anti-terrorism Act. Senator Serge Joyal argued against dissolving it, saying he feared it would eliminate the only Senate committee that was examining national security issues on an ongoing basis. Though the committee's chair, Senator Hugh Segal, supported dissolution, his support was contingent on the hope that it would be replaced by a new standing committee fashioned along the lines of the U.K.'s Intelligence and Security Committee. See Senate of Canada, *Debates*, 1st Session, 41st Parliament, 29 May 2013 (Hon. Serge Joyal); and Senate of Canada, *Debates*, 1st Session, 41st Parliament, 6 June 2013 (Hon. Hugh Segal).

140 CSIS and its review body, SIRC, were created in the aftermath of revelations about questionable disruption operations conducted by the RCMP Security Service in the early 1970s. These RCMP disruption operations were the subject of the 1981 *Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police* (the McDonald Commission), which recommended that a separate civilian security intelligence agency be created and made accountable through an independent review body, as well as a joint parliamentary committee. Only the former recommendation was implemented.

An executive director oversees the day-to-day operations of SIRC staff. In the 2017–2018 federal budget, SIRC received just under CAD1.9 million in "strategic funding" (i.e., temporary funding) until 2019–2020, which SIRC says it will use to increase to 24.5 its current complement of 13.7 full-time-equivalent staff positions used for lawfulness review work and investigation of complaints.[141] Since this funding is temporary, SIRC says it is being forced to rely on short-term staffing options, such as secondments, to fill these positions and that this is causing the organization to experience major human resources challenges.

Until the position of Inspector General of CSIS was eliminated in June 2012, the Minister of Public Safety and Emergency Preparedness, CSIS's responsible minister, relied on the incumbent to provide annual certification that the Service's operations and activities adhered to the minister's policies and directives. SIRC has now assumed the Inspector General's duties.[142]

Excluding non-permanent funds, SIRC's total annual budget now stands at around CAD2.8 million.[143] By contrast, CSIS's annual budget is approximately CAD577 million.[144]

2. Office of the CSE Commissioner

OCSEC was created in June 1996 under an order in council. Until the *National Defence Act* was amended in 2001 to codify CSE and OCSEC authorities and duties, both CSE and OCSEC operated under orders in council.[145]

OCSEC is headed by a supernumerary judge who is appointed by the Governor in Council and mandated under section 273.63(2) of the *National Defence Act* to investigate and respond to public complaints and to review CSE activities for lawfulness. If the CSE Commissioner believes CSE has engaged in unlawful activities, he or she must immediately inform the Minister of National Defence and the Attorney General of Canada. Drawing from authorities provided under Part II of the *Inquiries Act*, the CSE Commissioner has unfettered access to CSE information – with the exception of Cabinet confidences – facilities and staff. Under section 273.65(8) of the *National Defence Act*, the CSE Commissioner must review CSE activities carried out under ministerial authorization and confirm, in an annual report to the Minister of National Defence, whether these activities were authorized.

Section 273.63(3) of the *National Defence Act* states:

> The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

---

141 Security Intelligence Review Committee, "Spending and Human Resources," *Security Intelligence Review Committee: 2017–18 Departmental Plan*.

142 The University of Ottawa maintains an online archive of CSIS Inspector General reports dating from 2000 to 2010. See University of Ottawa, Centre for International Policy Studies, *CSIS Inspector General Certificate Reports*.

143 Security Intelligence Review Committee, "Spending and Human Resources," *Security Intelligence Review Committee: 2017–18 Departmental Plan*.

144 CSIS's total budget for 2015–2016 was CAD537 million, and the 2017–2018 Main Estimates indicated that this budget would increase to CAD577 million. See Canadian Security Intelligence Service, "Financial Resources," *Public Report: 2014–2016*; and Treasury Board Secretariat of Canada, "2017–18 Expenditures by Program or Purpose: Canadian Security Intelligence Service," *Government Expenditure Plan and Main Estimates (Parts I and II)*, 23 February 2017.

145 In CSE's case, these orders in council were classified.

The CSE Commissioner serves on a part-time basis only but is supported by a small full-time staff of 11.5 (including the executive director), of which 8.5 full-time equivalent positions are held by the subject matter experts who conduct review work.[146] Total annual funding for OCSEC stands at CAD2.1 million, of which CAD1.6 million is used for review work. In its 2017–2018 departmental plan, OCSEC indicated that it intends to request additional permanent funding so as to hire one additional review staff member and modernize its "technology assets."[147] By contrast, CSE's total annual budget stands at CAD596 million.[148]

3. Civilian Review and Complaints Commission for the RCMP

The CRCC was created in 2014 through legislation amending the RCMP Act.[149] Under this Act, the CRCC is mandated to review complaints made by the public about the on-duty conduct of RCMP members. It also has authority to initiate public interest reviews of RCMP activities but must provide a rationale to the Minister of Public Safety and Emergency Preparedness prior to doing so.[150] The CRCC has 67 full-time-equivalent employees, of which 45 are used to conduct investigations. Its total annual budget stands at just under CAD10 million, with CAD7.3 million of this total being used for review activities.[151] By contrast, the RCMP's total annual budget stands at roughly CAD3.4 billion.[152]

D. Parliamentary oversight

Canada's national security and intelligence agencies are subject to oversight by several officers of Parliament. As a result, the committees that consider the reports of these officers may also examine the activities of national security and intelligence agencies. For example, the House of Commons Standing Committee on Public Accounts examines the reports of the Auditor General of Canada who, from time to time, investigates the management of national security programs.

Similarly, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) examines the reports of the Privacy Commissioner of Canada and the Information Commissioner of Canada, whose work increasingly implicates national security and intelligence agencies, all of which are subject to the *Privacy Act* and the *Access to Information Act*. In connection with its recent study of the aforementioned *Security of Canada Information Sharing Act*, ETHI has also taken testimony directly from implicated departments and agencies, as well as from the three expert review bodies.

---

146 For reference to the number of subject matter experts on OCSEC staff, see Office of the Communications Security Establishment Commissioner, "Program 1.1: Commissioner's Review Program," *2016–2017 Report on Plans and Priorities*.

147 Office of the Communications Security Establishment Commissioner, "Spending and Human Resources," *2017–2018 Departmental Plan*. See also Alex Boutillier, "Review agency for Canada's spies says it needs more funding," *The Toronto Star*, 14 March 2017.

148 Treasury Board Secretariat of Canada, "Main Estimates: 2017–18 Estimates: Communications Security Establishment," *Government Expenditure Plan and Main Estimates (Parts I and II)*.

149 See Lyne Casavant and Dominique Valiquet, *Legislative Summary of Bill C-42: An Act to amend the Royal Canadian Mounted Police Act and to make related and consequential amendments to other Acts*, Publication no. 41-1-C42-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 7 November 2012.

150 See footnote 13.

151 See Civilian Review and Complaints Commission for the RCMP, "Spending and Human Resources," *Departmental Plan 2017–2018*.

152 See RCMP, "Spending and human resources," *Royal Canadian Mounted Police 2017–18 Departmental Plan*.

While spreading parliamentary review of national security and intelligence activities over multiple committees has the benefit of bringing many "fresh eyes" to examine issues, it also has the downside of reducing the ability of individual parliamentarians to build subject matter expertise. Examining the national security enterprise at an unclassified level and through a narrow lens has challenged the ability of parliamentarians to study its issues in a truly comprehensive fashion.

Only by formulating policy issues within a strategic construct – for example, identifying Canada's intelligence priorities and then routinely addressing the question of how well national capabilities align with this need – can these committees develop the necessary insights and expertise to hold national security and intelligence agencies to account.

However, the Standing Senate Committee on National Security and Defence and the House of Commons Standing Committee on Public Safety and National Security have the potential to develop expertise because they are specifically mandated to examine national security matters. These two committees are considered below.

1. Standing Senate Committee on National Security and Defence

The Senate created SECD on 15 March 2001, mandating it to examine "matters relating to national defence and security generally, including veterans affairs."[153] Prior to this time, the Senate had only examined national security and intelligence issues in the context of special committees, such as the Senate Committee on Intelligence, which convened in 1987, 1988 and then again in 1999 to examine anti-terrorism activities. The Senate Committee on Intelligence was notable in that its chair attempted to elicit candid responses from agency officials by taking their testimony *in camera*.

Though SECD's specific orders of reference can change from session to session, this committee has interpreted its broad mandate as permitting examination of DND/Canadian Armed Forces and PSC capabilities, working relationships between various agencies involved in intelligence-gathering and analysis, intelligence agency review mechanisms, and the security of borders and critical infrastructure.[154]

SECD works at the unclassified level. Under *Rule 12-9-2 of The Rules of the Senate*, SECD is empowered to send for persons, papers and records.

2. House of Commons Standing Committee on Public Safety and National Security

Until SECU was created by the passing of a motion amending the House of Commons Standing Orders on 5 April 2006, issues involving public safety and national security had been referred to the then House of Commons Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness or its subcommittees. As per Standing Order 104 of the *Standing Orders of the House of Commons*, SECU comprises 10 members. At present, six SECU members, including the chair, come from the governing party – the Liberal Party of Canada – and four come from the two opposing parties (three from the Conservative Party of Canada and one from the New Democratic Party of Canada). SECU's chair and two vice-chairs (one from each opposition party) are elected by committee members.

---

153 See Senate of Canada, "Chapter 12: Committees," *Rules of the Senate*, Rule 7(15).

154 Standing Senate Committee on National Security and Defence, *Introduction to the Standing Senate Committee on National Security and Defence*.

Standing Order 108 mandates standing committees and empowers them to examine and inquire into all matters referred to them by the House of Commons and to report to the House. As a standing committee, SECU is authorized to send for persons, papers and records, and to delegate all or any of its powers to subcommittees. It may meet while the House of Commons is in session and during adjournment periods. SECU can also sit jointly with other standing committees.

Working at the unclassified level, SECU is mandated to examine the policies and activities of one of the largest departmental portfolios – PSC – including the close to 140 statutes this department and its agencies administer. Specifically, SECU is mandated to examine the policies, programs and statutes of PSC, Canada Border Services Agency, CSIS, Correctional Service Canada, Parole Board of Canada, RCMP, SIRC, CRCC, Office of the Correctional Investigator, and the RCMP External Review Committee.[155]

Thus, and as alluded to above, SECU examines national security issues, but only as part of a broader menu of items that includes matters related to criminal law, corrections and conditional release of federal offenders, border security, policing and law enforcement, crime prevention and emergency management.

SECU recently examined and reported on the NSICPA and on the government's consultation paper on national security. Under the House of Commons Standing Orders, if a committee chair requests a response to a report, the government is required to provide one within 120 days of the report's being presented.

E. Recent developments and reform proposals

1. National Security and Intelligence Committee of Parliamentarians

As noted above, on 22 June 2017, Canada's Parliament passed the NSICPA, under which a National Security and Intelligence Committee of Parliamentarians (NSICOP) will be created to examine national security and intelligence issues. Section 8 mandates the NSICOP to review:

> a) the legislative, regulatory, policy, administrative and financial framework for national security and intelligence;
>
> (b) any activity carried out by a department that relates to national security or intelligence, unless the activity is an ongoing operation and the appropriate Minister determines that the review would be injurious to national security; and
>
> (c) any matter relating to national security or intelligence that a minister of the Crown refers to the Committee.

Under the new legislation, after consultation with specified leaders in the Senate and the House of Commons, NSICOP members will be selected by and report to the prime minister. On 8 January 2016, six months before the legislation was tabled in the House of Commons, the Prime Minister appointed Member of Parliament David McGuinty to take a "leadership position" on the committee and permitted national security and intelligence agencies to brief Mr. McGuinty on issues of

---

155 The RCMP External Review Committee is an administrative tribunal that reviews cases and issues findings and recommendations for appeal decisions in certain RCMP labour relations matters.

concern.[156] As a condition of their participation in the NSICOP, all members will be permanently bound to secrecy. Because the NSICOP will not be a parliamentary committee, its members will not enjoy parliamentary privilege, including with respect to any unauthorized disclosures they might make during the course of their other work in Parliament.

The eleven-member NSICOP will comprise currently serving parliamentarians who are not serving ministers or parliamentary secretaries. Up to three members of the committee could come from the Senate, with up to five of the remaining eight members coming from the governing party in the House of Commons. The chair will only be permitted to vote in the event of a tie.

In many respects, the scope of the NSICOP's remit will be determined by its ability to access required information. For example, the original text of the legislation would have effectively eliminated the NSICOP's ability to examine defence intelligence activities by prohibiting access to "information pertaining to ongoing defence intelligence activities supporting ongoing military operations, including the nature and content of plans in support of these military operations." This language was removed from the legislation, as was language that would have prohibited any form of direct scrutiny of the Financial Transactions and Reports Analysis Centre (FINTRAC), Canada's financial intelligence agency. The Act enables the NSICOP to access FINTRAC strategic analyses or any other information FINTRAC has not disclosed and that does not reveal the identities of individuals or entities.

Under the NSICPA, committee members will be automatically denied access to Cabinet confidences, information that provides the names of current or intended confidential human sources, and information pertaining to an ongoing law enforcement investigation that may lead to a prosecution. Significant constraints will also be placed on the committee's access to certain types of information, particularly special operational information. However, if a minister were to invoke the provision to deny the NSICOP access to information to which it would otherwise be entitled and which is under the control of a department (section 16), he or she will have to inform the committee of this decision and provide reasons for it. In instances where the denied information was controlled by CSIS, CSE or the RCMP, the appropriate minister will also be required to inform the agency's expert review body and provide reasons for his or her decision. This is meant to ensure that the NSICOP cannot circumvent the minister's denial of access by approaching any of the expert review bodies. The NSICPA seeks to limit ministers' use of this authority by requiring the NSICOP to provide in its annual reports a tally of access denial decisions made under section 16.

Focusing primarily on questions of efficacy, the NSICOP will examine the policies, administration and activities of the national security and intelligence community as a whole. Generally, its reviews of national security activities would be *ex post* (after the fact), but the NSICPA holds out the possibility that a minister might permit examination of ongoing operational activities.[157]

---

156 Most have taken this to mean that Mr. McGuinty will chair the new committee of parliamentarians. See Prime Minister of Canada, "Prime Minister of Canada announces new leadership role for MP McGuinty," News release, 8 January 2016. To obtain a redacted copy of the briefing materials presented to MP McGuinty, which were released under an Access to Information and Privacy request, please contact the Library of Parliament in Canada.

157 Section 8(1)(b) of the legislation prohibits the NSICOP from reviewing ongoing operations if a minister determined such an examination to be injurious to national security. Sections 8(2) and 8(3), respectively, require the minister to explain why the review would be injurious to national security and to notify the NSICOP when its review would no longer be injurious.

The NSICOP will be supported by a small secretariat staffed and run by an appointed executive director who will have deputy minister status.[158] Very little public information is available on the expected resourcing of the NSICOP's secretariat. However, based on a table included in the annex of the federal government's Fall 2016 Economic Statement, it appears that the secretariat will have an annual budget of around CAD3.2 million, enough to pay the salaries of the executive director, internal services staff, and three or four research staff.[159]

F. Other developments

The adoption of the NSICPA is just one in a series of recent changes to the authorities and governance framework of the Canadian security and intelligence community. Some of the more controversial changes took place under Bill C-51 – an omnibus anti-terrorism law passed in June 2015 that provided new "threat reduction" authorities to CSIS, enhanced the Public Safety minister's ability to deny disclosure of national security information used in security certificates issued under Division 9 of the *Immigration and Refugee Protection Act*, and greatly expanded information-sharing among departments and agencies with national security responsibilities. The current government, which came to power in October 2015, campaigned on a pledge to roll back "problematic" provisions of Bill C-51,[160] which it aims to do through the 20 June 2017 tabling of Bill C-59, An Act respecting national security matters.[161]

If enacted, Bill C-59 will introduce profound changes to the bodies that currently scrutinize national security and intelligence agencies. For example, Bill C-59 would effectively consolidate OCSEC and SIRC into a single body, the National Security and Intelligence Review Agency (NSIRA). The CRCC would continue to exist, but all of its national security-related work would be transferred to the NSIRA. Beyond reviewing the activities of CSIS and CSE, the NSIRA would be required (under clause 8) to review "any matter that relates to national security or intelligence that a minister of the Crown refers to the Agency." This means that the scope of the NSIRA's remit would mirror that of the NSICOP. Finally, the NSIRA would be mandated not only to examine the lawfulness of national security and intelligence activities but also their reasonableness and necessity, thus creating an additional mechanism to trigger legislative and regulatory change.

Bill C-59 would also create an Intelligence Commissioner, a retired judge who would be mandated to examine the reasonableness of conclusions leading to ministerial authorizations for certain types of CSE activities and ministerial determinations regarding CSIS's collection, retention, querying and exploitation of datasets. Unlike the NSIRA, which would be a review body, the Intelligence Commissioner would have an oversight role, putting a stop to or amending planned activities before they happen.

---

158 Appointing the NSICOP secretariat executive director at this level raises some interesting questions. Not only would he or she out-rank all current executive branch watchdogs, but also the current National Security and Intelligence Advisor to the Prime Minister, who operates without a statutory basis. However, if Bill C-59, An Act respecting national security matters, which was introduced in the House of Commons on 20 June 2017, is enacted, SIRC and OCSEC would be replaced with a new expert review body, the National Security and Intelligence Review Agency. This new expert review agency would be led by a deputy minister and, would therefore be equal in rank to the NSICOP secretariat's executive director.

159 See Government of Canada, "Policy Actions Taken Since Budget 2016: Table A1.4," in "Annex 1 – Details of Economic and Fiscal Projections," *Fall 2016 Economic Statement*, 1 November 2016.

160 See Liberal Party of Canada, "Keeping Canadians Safe: Bill C-51," *Real Change: A New Plan for a Strong Middle Class*, October 2015, p. 53.

161 Bill C-59, An Act respecting national security matters, 1st Session, 42nd Parliament.

At the same time, Bill C-59 would grant significant new powers to Canada's intelligence agencies. For example, the CSIS Act would be amended to create a regime enabling CSIS to collect and use datasets on Canadians, so long as these datasets were "relevant" to the performance of CSIS duties. These amendments to the CSIS Act appear to respond to a 2016 Federal Court decision in which CSIS was reprimanded for having failed in its duty of candour to the Court regarding its practice of collecting and retaining metadata on Canadians not under investigation.[162]

CSE would also gain significant new powers. Under Bill C-59's proposed enabling mandate, the Communications Security Establishment Act, CSE will be permitted to engage in "active cyber operations" targeting foreign individuals, states, organizations or terrorist groups. CSE would also be empowered to provide technical and operational support to offensive cyber operations conducted in the context of military missions. Heretofore, Canada's military has not been permitted to engage in cyber operations of this nature.

Finally, CSE would also be authorized to provide advice and services to protect critical information infrastructure, including infrastructure owned and operated by the private sector and systems and networks used by parliamentarians and the federal courts.

---

162 See Federal Court, *2016 FC 1105*.

NEW ZEALAND

A. Overview of intelligence agencies

New Zealand has two intelligence and security agencies. The New Zealand Security Intelligence Service (NZSIS) specialises in human intelligence activities. The Government Communications Security Bureau (GCSB) specialises in signals intelligence and information assurance and cybersecurity activities.[163]

The functions of each agency are:[164]

- to collect and analyse intelligence in accordance with the Government's priorities;
- to provide any intelligence collected and analysis of it to the Minister responsible for the agency (the responsible Minister), the Chief Executive of the Department of the Prime Minister and Cabinet and any other persons (whether in New Zealand or overseas) authorised by the responsible Minister;
- to provide protective security services, advice and assistance to public authorities and other authorised persons (whether in New Zealand or overseas);
- to provide, in the case of the GCSB, information assurance and cybersecurity activities to public authorities and other authorised persons (whether in New Zealand or overseas), and to do everything necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government;
- to co-operate with the other intelligence and security agency, and to co-operate with, and provide advice and assistance to, the New Zealand Police and the New Zealand Defence Force;
- to co-operate with, and provide advice and assistance to, any entity that is responding to an imminent threat to the life or safety of:
  - any person in New Zealand;
  - any New Zealand citizen or permanent resident who is overseas;
  - any person in an area in respect of which New Zealand has search and rescue responsibilities under international law;
  - any person outside the territorial jurisdiction of any country.

The agencies must act in accordance with New Zealand law and in a manner that facilitates democratic oversight.[165]

In addition to the NZSIS and the GCSB, the third core agency of the New Zealand Intelligence Community is the National Assessments Bureau within the Department of the Prime Minister and Cabinet. The New Zealand Defence Force also has intelligence capabilities and a range of other government departments and agencies, notably New Zealand Police, the New Zealand Customs Service and Immigration New Zealand, have intelligence units.[166]

163 Intelligence and Security Act 2017, s.7, 8

164 Ibid, s.10-14

165 Ibid, s.17

166 New Zealand Intelligence Community, About us

B. Recent developments

The Intelligence and Security Act 2017 received Royal Assent on 28 March 2017. The Act, which replaces the four acts that previously applied to the intelligence and security agencies and their oversight bodies, implements the Government's response to the recent independent review of intelligence and security.[167]

An amendment to the New Zealand Security Intelligence Committee Act 1996 in 2013 introduced a requirement for a review of the intelligence and security agencies to be carried out every five to seven years.[168] The report of the first periodic review to be undertaken was published in February 2016.[169] Among the review's terms of reference was a requirement to determine whether the current oversight arrangements provided sufficient safeguards at an operational, judicial and political level to ensure the agencies acted lawfully and maintained public confidence.[170]

The review proposed that the intelligence and security agencies, their oversight bodies and potentially also intelligence assessment should be covered by a single piece of legislation. The legislation would include a new, comprehensive authorisation regime requiring some level of authorisation for all of the agencies' intelligence and security activities that involve gathering information about individuals or organisations, proportionate to the level of intrusion involved. It would also make some changes to facilitate greater oversight of the agencies and accountability for their activities.[171]

Among the review's recommendations relating to oversight were:[172]

- the agencies should be integrated within the public sector; they should be subject to the State Sector Act 1988, with any appropriate exceptions and exemptions;
- higher levels of scrutiny should apply to authorisations of agency activities that are more intrusive or target New Zealanders;
- the Inspector-General of Intelligence and Security (IGIS) should be appointed by the Governor-General on the recommendation of the House of Representatives, rather than on the Prime Minister's recommendation;
- the Office of the IGIS should be funded through an appropriation separate from that of the agencies;
- the functions and powers of the IGIS should be enhanced:
  - the category of people able to make a complaint should be broadened to include non-New Zealanders;
  - review of authorisations should not just relate to procedural matters but should include a comprehensive look behind the face of the authorisation;
  - the restriction on inquiring into operationally sensitive matters should be removed;

---

167 New Zealand Intelligence and Security Bill 2016. The four acts are: New Zealand Security Intelligence Service Act 1969; Government Communications Security Bureau Act 2003; Inspector-General of Intelligence and Security Act 1996; Intelligence and Security Committee Act 1996

168 Intelligence and Security Committee Amendment Act 2013, s.9

169 Sir Michael Cullen, Dame Patsy Reddy, Intelligence and security in a free society: report of the first independent review of intelligence and security in New Zealand, 2016

170 Ibid, p. 1

171 Ibid, p. 3

172 Ibid, p. 5-11

- the maximum size of the Intelligence and Security Committee should be increased to allow for greater flexibility in representation;
- the Committee should be able to elect its own chairperson, who would not necessarily be the Prime Minister;
- the Committee should be able to request, but not require, the IGIS to carry out an inquiry, including into operationally sensitive matters.

The Intelligence and Security Act 2017 adopted most, but not all, of the review's recommendations.[173]

Some sections of the Act came into force on 1 April 2017. The remainder of the Act came into force on 28 September 2017.[174]

C. Oversight summary

The intelligence and security agencies operate within a framework of executive, parliamentary, independent and judicial oversight. The Prime Minister, as Minister for National Security and Intelligence, is responsible for leading the national security system. The responsible Minister for each agency exercises ministerial oversight within the framework set by the Prime Minister.[175] A responsible Minister has sole responsibility for issuing some intelligence warrants and joint responsibility with a Commissioner of Intelligence Warrants, who is a former judge, for issuing others. Parliamentary scrutiny of the agencies' policies, administration and expenditure is undertaken by the Intelligence and Security Committee (ISC). The IGIS provides independent oversight of the agencies to ensure that they act with propriety and operate lawfully and effectively.

The NZSIS and the GCSB are departments of State.[176] Their Directors-General are appointed, have their performance reviewed, and may be dismissed by the State Services Commissioner in accordance with the State Sector Act 1988.[177] Each agency must present to its responsible Minister an annual report containing the information required of departments by the Public Finance Act 1989 and the additional information on its activities required by the Intelligence and Security Act 2017. The Minister must give a copy of the report to the ISC, and also present a copy, from which some information may be excluded, to Parliament. The report as presented to Parliament must be published on the agency's internet site.[178]

D. Parliamentary oversight

1. Intelligence and Security Committee

The Intelligence and Security Committee was established by the Intelligence and Security Committee Act 1996. Previously parliamentary scrutiny of the intelligence and security agencies had been undertaken by the Government Administration select committee.[179] The intention in establishing a statutory committee was to increase parliamentary oversight of the agencies while remaining sensitive to

---

173 New Zealand Intelligence and Security Bill 2016

174 Intelligence and Security Act 2017, s.2

175. National Security and Intelligence role created, 6 Oct. 2014

176. Intelligence and Security Act 2017, s.7, 8

177. State Sector Act 1988, s.35, 39, 43

178. Intelligence and Security Act 2017, s.221; Public Finance Act 1989, s.45

179 Standing Orders of the House of Representatives, 1992, S.O.345

considerations of national security.[180] Parliament has retained its power to inquire into the agencies, but it is the House's practice to make a sessional order for each Parliament that no select committee can examine an intelligence and security agency.[181]

The Intelligence and Security Act 2017 increases the interaction between the ISC and the IGIS. The ISC is now able to request the IGIS to conduct an inquiry into the agencies' compliance with the law or the propriety of their activities. It also now considers and discusses with the IGIS his or her annual report.[182]

a. Functions

The functions of the ISC are:

- to examine the intelligence and security agencies' policies, administration and expenditure;
- to receive and consider the agencies' annual reports;
- to conduct, following receipt of each agency's annual report, an annual review of the agency for the immediately preceding financial year;
- to consider any bill, petition or other matter in relation to an agency, referred to it by the House;
- to request the IGIS to conduct an inquiry into:
  - any matter relating to an agency's compliance with New Zealand law, including human rights law;
  - the propriety of particular activities of an agency;
- to consider any matter, which is not directly related to an agency's activities, that is referred to it by the Prime Minister because of the matter's intelligence or security implications;
- to consider and discuss with the IGIS his or her annual report.

The ISC's functions do not include:

- inquiring into any matter within the jurisdiction of the IGIS;
- inquiring into any matter that is operationally sensitive, including any matter that relates to intelligence collection and production methods, or sources of information;
- inquiring into complaints by individuals concerning the activities of an agency that are capable of being resolved under any other enactment.

A review of the intelligence and security agencies must be conducted every five to seven years. Before the Prime Minister appoints the reviewers or specifies the terms of reference he or she must consult the ISC. On completion of their report the reviewers must provide it to the ISC which, having considered the report, and excluded any information that cannot be disclosed, will present it to the House.

---

180 Intelligence and Security Agencies Bill, as reported from the Committee on the Intelligence and Security Agencies Bill, p. ii, 1996

181 House of Representatives, Sessional and other orders of continuing effect, Fifty-first Parliament (as at 21 October 2015); David McGee, Parliamentary practice in New Zealand, 4th ed., edited by Mary Harris and David Wilson, Oratia Books, 2017, p. 505.

182 Sections 192-205, section 223 and Schedule 3, clauses 17-26, in particular, of the Intelligence and Security Act 2017 apply to the Intelligence and Security Committee

b. Powers and performance of functions

The Director-General of an intelligence and security agency must appear before the ISC if requested by it to do so. The ISC may request any other person to attend and give evidence before it, or to produce any document or other information that is relevant to its proceedings.

Anyone asked by the ISC to disclose to it any document or other information in his or her possession must either do so, or inform the ISC that the document or information cannot be disclosed because the Director-General of the relevant agency considers it to be sensitive information, as defined by the Intelligence and Security Act 2017. The disclosure of sensitive information is not precluded in cases where the Director-General of the relevant agency considers disclosure to be safe. Sensitive documents or information must be disclosed to the ISC if the Prime Minister considers that disclosure is desirable in the public interest.

The ISC's proceedings are proceedings in Parliament for the purposes of Article 9 of the Bill of Rights 1688 and the Parliamentary Privilege Act 2014. The ISC's meetings must be convened by the chairperson. Proceedings must be conducted in accordance with the rules and practice of the House of Representatives. The ISC meets in private unless it is conducting an annual financial review, or unless it unanimously resolves otherwise.

The ISC must, having regard generally to security requirements, present an annual report on its activities to Parliament. The House may require the ISC to provide it with a copy of any or all records, including reports, evidence and advice to the ISC, that are held by the ISC in relation to the performance of the first four of its functions as set out above. Before providing a copy of any record to the House, the ISC must remove any information that it is restricted from disclosing to the House.

The ISC must not disclose in a report to Parliament:

- any information that, if publicly disclosed, would be likely to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence
    - by the government of any other country or any agency of such a government;
    - by an international organisation;
- any information that, if publicly disclosed, would be likely to endanger the safety of any person;
- any sensitive information disclosed to the ISC.

Unless it considers that there are compelling reasons in the public interest to do so, the ISC must not disclose in a report to Parliament:

- the identity of any person who is or has been an officer, employee or agent of an intelligence and security agency, other than the Director-General, or any information from which the identity of such a person could reasonably be inferred;
- any information that, if publicly disclosed, would be likely:
    - to prejudice an agency's continued performance of its functions;
    - to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand.

c. Composition and appointment

The ISC must comprise between five and seven members, the number to be determined by the Prime Minister in consultation with the Leader of the Opposition. The membership of the ISC must comprise:

- the Prime Minister;
- the Leader of the Opposition;
- members of Parliament nominated by the Leader of the Opposition, with the agreement of the Prime Minister, after consultation with the leader of each party that is not in government or in coalition with a Government party;
- members of Parliament nominated by the Prime Minister after consultation with the leader of each party in government.

If the ISC has five members, one member must be nominated by the Leader of the Opposition and two by the Prime Minister. If it has six or seven members, two members must be nominated by the Leader of the Opposition and the balance by the Prime Minister. In making their nominations the Leader of the Opposition and the Prime Minister must have regard to security requirements and the proportional representation of political parties in Parliament. When performing the ISC's functions, a member of the ISC acts in his or her official capacity as a member of Parliament.

The names of nominees must be presented by the Prime Minister to the House for its endorsement. If the House declines to endorse a nomination, the Prime Minister must present the name of another member, nominated by the Leader of the Opposition or the Prime Minister as the case requires, for endorsement.

The ISC is chaired by the Prime Minister, or another member of the ISC from time to time appointed by the Prime Minister.

d. Resourcing

The ISC is assisted in the conduct of its business by officers appointed by the Chief Executive of the Department of the Prime Minister and Cabinet with the ISC's concurrence.

E. Independent oversight

1. Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security is an independent statutory office. It is not subject to general direction from a Minister responsible for an intelligence and security agency, the Prime Minister or other ministers on how its responsibilities should be carried out. The IGIS oversees the NZSIS and the GCSB. The exercise by other agencies, e.g. the National Assessments Bureau, the intelligence services of the New Zealand Defence Force, and the intelligence units of Immigration New Zealand, the New Zealand Customs Service and the New Zealand Police, of their intelligence and security functions does not fall within the IGIS's jurisdiction.[183]

---

183 Office of the Inspector-General of Intelligence and Security, Annual report for the year ended 30 June 2016, p. 3, 4

The office of Inspector-General of Intelligence and Security was established by the Inspector-General of Intelligence and Security Act 1996. The new office replaced the office of Commissioner of Security Appeals, whose function had been to inquire into complaints regarding the NZSIS. The jurisdiction of the new office was extended to cover the GCSB and the conduct of inquiries and reviews became part of its functions. Until 2013 the office was required to be held by a former High Court judge, who carried out the role on a part-time basis.[184]

Changes were made in 2013 to strengthen the IGIS's role. Provision was made for the appointment of a Deputy Inspector-General of Intelligence and Security and staffing was increased. An advisory panel was established to provide advice to the IGIS, who no longer had to be a former judge.[185] The Intelligence and Security Act 2017 removes the restriction on inquiries by the IGIS into operationally sensitive matters and clarifies that he or she may review warrants on substantive as well as procedural grounds.[186]

a. Functions

The functions of the IGIS are:

- to conduct, at the request of the responsible Minister, or the ISC, or on the IGIS's own initiative, an inquiry into:
  - any matter relating to an intelligence and security agency's compliance with New Zealand law, including human rights law;
  - any matter where it appears that a New Zealand person has been or may be adversely affected by an act, omission, practice, policy or procedure of an agency;
- to conduct, at the request of the Prime Minister, the responsible Minister, or the ISC, or on the IGIS's own initiative, an inquiry into:
  - the propriety of particular activities of an agency;
- to deal with complaints about an agency made by:
  - a New Zealand person;
  - an employee, or former employee, of an agency, if all established internal remedies have been exhausted or the Director-General of the relevant agency agrees in writing;
  - the Speaker of the House of Representatives on behalf of one or more members of Parliament;
- to conduct reviews, at least annually, and unscheduled audits of the effectiveness and appropriateness of:
  - each agency's procedures for ensuring compliance with the Intelligence and Security Act 2017 in relation to the issue and execution of an authorisation;
  - each agency's compliance systems for operational activities;
- to conduct, on the IGIS's own initiative, a review of any activity carried out by an agency in performance of its function to co-operate with an entity that is responding to an imminent threat to life or safety;

---

184 Ibid, p. 1, 3, 4; Inspector-General of Intelligence and Security, Annual report 1997, p. 2

185 Office of the Inspector-General of Intelligence and Security, Annual report for the year ended 30 June 2014, p. 9

186 Sections 157-191, section 222 and Schedule 3, clauses 6-12, in particular, of the Intelligence and Security Act 2017 apply to the Inspector-General of Intelligence and Security

- to conduct a review in relation to either or both the issue of an authorisation and the carrying out of an authorised activity;
- to conduct reviews in relation to permissions granted to permit access to restricted information, and in relation to approvals to obtain business records from telecommunications network operators and financial service providers;
- to prepare, publish, and undertake an annual work programme.

b. Powers and performance of functions

In undertaking an inquiry, the IGIS has the power:

- to summon and examine on oath any person whom the IGIS considers is able to give relevant information;
- to require any person to provide any information, and any documents or things in the possession of or under the control of that person, that the IGIS considers may be relevant;
- to enter, at any reasonable time and after giving prior notice to the agency's Director-General, any premises or place occupied or used by an intelligence and security agency.

In conducting any inquiry or review, the IGIS must take into account any relevant ministerial policy statement providing guidance to the agency, and the extent to which the agency has had regard to that statement.

On completion of an inquiry, the IGIS prepares a report containing his or her conclusions and recommendations. If the inquiry concerned a complaint, the report may include recommendations for redressing the complaint, including the payment of compensation.

The IGIS must send the report to both the responsible Minister and the Director-General of the agency to which the inquiry relates. The report must also be sent to the Prime Minister, if the inquiry was conducted at the Prime Minister's request, or to the ISC, if the inquiry was conducted at its request.

The IGIS may also send a report of an inquiry to the ISC if:

- the inquiry was conducted on the IGIS's own initiative, or at the request of the responsible Minister, and the responsible Minister agrees;
- the inquiry was conducted at the request of the Prime Minister, and the Prime Minister agrees.

The responsible Minister must provide his or her response to the report to the IGIS and to the Director-General of the agency concerned. If the inquiry was conducted at the request of the ISC, the Minister must also provide the response to the ISC, and may do so if the inquiry was not conducted at the ISC's request.

In the case of an inquiry conducted in relation to a complaint, the IGIS must advise the complainant of his or her conclusions in terms that will not prejudice New Zealand's security or defence, or the international relations of the Government.

A report of an inquiry must also be published on the IGIS's internet site. Restrictions apply to the disclosure of certain information.

The IGIS must report annually to each responsible Minister and to the Prime Minister on his or her operations. The Prime Minister must present the report to Parliament, together with a statement as to whether any matter has been excluded from it. The Prime Minister must also present the Leader of the Opposition with a copy of the report as it was received from the IGIS. The IGIS must publish the report, as presented to Parliament, on the internet. The IGIS may at any time, with the agreement of the Prime Minister, report either generally or in respect of any particular matter to the ISC.

c. Appointment

The IGIS is appointed by the Governor-General on the recommendation of the House of Representatives. Before a recommendation may be made, the Prime Minister must consult the ISC about the proposed appointment and advise the House on the outcome of the consultation. The IGIS is appointed for a term of up to five years, and may be reappointed for a further term of up to three years.

The IGIS may be removed or suspended from office by the Governor-General, on an address from the House of Representatives, for incapacity, bankruptcy, neglect of duty, misconduct, or failure to hold the appropriate security clearance.

d. Resourcing

As at June 2016, the Office of the IGIS comprised the Inspector-General, the Deputy Inspector-General and six staff, including four investigating officers.[187]

The total budgeted expenditure for 2015/2016 was $1,498,000, approximately one per cent of the budgeted estimates for the NZSIS and the GCSB.[188]

F. Judicial oversight

1. Commissioners of Intelligence Warrants

Applications for the issue of an intelligence warrant must be made by the Director-General of the agency concerned to the authorising Minister, who is the agency's responsible Minister, in the case of a Type 2 warrant, and to the authorising Minister and a Commissioner of Intelligence Warrants in the case of a Type 1 warrant.[189]

A Type 1 warrant authorises an agency to carry out an otherwise unlawful activity for the purpose of collecting information about, or to do any other thing directly in relation to, a New Zealand citizen or permanent resident. A Type 2 warrant authorises an agency to carry out an otherwise unlawful activity for the purpose of collecting information, or to do any other thing, in circumstances where a Type 1 warrant is not required.

---

187 IGIS, Annual report, 2016, p. 4

188 Ibid, p. 32

189 Sections 52-84, in particular, of the Intelligence and Security Act 2017 apply to intelligence warrants

Up to three Commissioners of Intelligence Warrants, one of whom is the Chief Commissioner, are appointed by the Governor-General on the recommendation of the Prime Minister. Before making a recommendation, the Prime Minister must have consulted the Leader of the Opposition about the proposed appointment. A Commissioner of Intelligence Warrants must have previously held office as a judge of the High Court.[190]

The Commissioners' functions are:

- to advise, and to consider and deliberate with, the responsible Minister on applications for Type 1 intelligence warrants;
- to issue Type 1 warrants jointly with the Minister;
- to consider with the Minister applications for permission to access restricted information, i.e. driver's licence photographs and information relating to tax, an adoption and tertiary students' national student numbers;
- to consider with the Minister applications for approval to obtain business records from telecommunications network operators and financial service providers;
- to conduct a review when notified by the Director-General of the GCSB that a significant network security risk relating to public telecommunications networks exists or may arise;
- to conduct reviews of ministerial decisions to refuse to issue, or to cancel or retain possession of, a New Zealand passport or travel document.

An authorising Minister may, if satisfied that a situation is urgent and it is necessary to do so, issue a Type 1 warrant without a Commissioner's involvement. Such a warrant will expire after 48 hours unless an application has been made for a warrant via the normal procedures and the authorising Minister and a Commissioner confirm the urgent intelligence warrant. On issuing an urgent intelligence warrant, the authorising Minister must immediately notify the Chief Commissioner of Intelligence Warrants, who may revoke the warrant at any time up to the end of the 48 hour expiry period.

190 Sections 112-117 and Schedule 3, clauses 1-5, in particular, of the Intelligence and Security Act 2017 apply to Commissioners of Intelligence Warrants

UNITED KINGDOM

A. Overview of intelligence agencies

The United Kingdom has three intelligence and security services, collectively known as the Agencies:[191]

- The Secret Intelligence Service (SIS, often called MI6),[192] which collects secret foreign intelligence;
- The Security Service (often called MI5),[193] which is responsible for protecting the UK against covertly organised threats to national security; and
- Government Communications Headquarters (GCHQ),[194] which gathers intelligence through the interception of communications.

In addition to the dedicated intelligence agencies, other elements of the UK's national intelligence machinery are contained within specific government departments:[195]

- Defence Intelligence, an integral part of the Ministry of Defence, provides intelligence products, assessments and advice to guide decisions on policy and the commitment of the armed forces; to inform defence research and equipment; and to support military operations.
- The National Security Secretariat, based at the Cabinet Office supports the National Security Council (NSC), providing coordination on security and intelligence issues of strategic importance across government. The NSC is the main forum for the collective discussion of the government's objectives for national security. The Prime Minister is advised by the head of the NSC secretariat, the National Security Adviser.
- The Joint Intelligence Committee (JIC), which is supported by the Joint Intelligence Organisation, is also part of the Cabinet Office. The JIC assesses raw intelligence gathered by the agencies and presents it to ministers to enable policy making.
- The Office of Security and Counter-Terrorism is a unit within the Home Office.
- The Joint Terrorism Analysis Centre (JTAC) is an organisation comprised of representatives from 16 government departments and agencies, housed at MI5's headquarters. JTAC analyses and assesses all intelligence relating to international terrorism. It sets threat levels and issues warning of threats and other terrorist-related subjects, as well as producing in-depth reports on trends, terrorist networks and capabilities. It brings together information from the police and government departments and agencies so that it is analysed and processed on a shared basis.

B. Oversight summary

Within government, the Prime Minister has overall responsibility for security matters. The Home Secretary has specific responsibility for the Security Service; the Foreign and Commonwealth Secretary for SIS and GCHQ; and the Defence Secretary for the Defence Intelligence staff. To the extent that the ministers responsible for the various intelligence services are accountable to Parliament, there has always been some degree of parliamentary oversight of the Agencies.

---

191 These three agencies are referred to as the "intelligence agencies" in legislation, for example, s 263 of the *Investigatory Powers Act 2016*

192 *Intelligence Services Act 1994*, s1

193 *Security Service Act 1989*, s 1

194 *Intelligence Services Act 1994*, s3

195 Further information is available at Gov.uk and Mi5.gov.uk [links accessed 28 March 2017]

The day-to-day operations of the Agencies are overseen by their respective Heads, each of which has a statutory duty to provide annual reports to the Prime Minister and respective Secretary of State.

The Agencies' accounts are subject to audit by the National Audit Office. They are also shown to the Chair of the Public Accounts Committee. The accounts are not published, for reasons of national security. However, an annual Financial Statement is published covering the Single Intelligence Account, the funding vehicle for the Agencies.[196]

The *Intelligence Services Act 1994* (ISA) put the SIS and GCHQ on a statutory footing and established the Intelligence and Security Committee (ISC). The members of the ISC are nominated by the Prime Minister and appointed by Parliament, to which the ISC reports. The ISC's function is to examine the expenditure, administration, policy and operations of the UK's three main intelligence and security agencies. To this end its members take evidence from Cabinet Ministers and senior officials which is used to formulate committee reports. ISC members are subject to section 1(1)(b) of the *Official Secrets Act 1989* and have access to highly classified material in carrying out their duties.[197]

The *Justice and Security Act 2013* reformed the ISC making it a Committee of Parliament. It gave it greater powers and widened its remit. Originally set up to cover MI5, MI6 and GCHQ, the ISC now also takes an interest in the work of Defence Intelligence and the JIC, as well as law enforcement agencies (police and Customs & Excise).

In addition to general Ministerial responsibility for the Agencies, the executive plays a specific role in the grant of warrants for activities such as interception and equipment interference.[198] It is argued that this is necessary because Ministers are accountable, both to Parliament and to the public, for their decisions, and because the grant of warrants involves the exercise of political judgement in sensitive matters of national security and foreign policy.

The Investigatory Powers Commissioner (IPC) provides independent oversight of the use of intrusive powers by the Agencies. The Commissioner makes an annual report to the Prime Minister, which is then published and laid before Parliament, subject to necessary redactions.[199]

Finally, complaints of unlawful use of covert techniques by public authorities are investigated and determined by the Investigatory Powers Tribunal (IPT). The tribunal was established in October 2000 under the *Regulation of Investigatory Powers Act 2000* (RIPA). It provides a right of redress for anyone who believes they have been a victim of unlawful action under RIPA or wider human rights infringements in breach of the *Human Rights Act 1998*.

---

196 See *Security and Intelligence Agencies: Financial Statement 2015-16*, HC 363, July 2016

197 Section 1(1)(b) makes unauthorised disclosure of classified information an offence.

198 This is currently provided for by the *Regulation of Investigatory Powers Act 2000* and the *Intelligence Services Act 1994*. The recently enacted *Investigatory Powers Act 2016* will reform the procedure, introducing a so-called "double lock" whereby the relevant Secretary of State will approve the warrant, but this will be subject to review by a Judicial Commissioner, before the warrant comes into effect.

199 Further information is available from the website of the Investigatory Powers Commissioner's Office.

C. Recent developments

The *Investigatory Powers Act 2016* consolidated, rationalised, and in certain respects extended, the use of investigatory powers by the Agencies, the police, and other law enforcement bodies.[200] When fully in force, it will make a number of significant changes to oversight mechanisms, including:

- Introducing judicial scrutiny to the grant of warrants;
- Overhauling the independent oversight regime, to that of a single Investigatory Powers Commissioner responsible for the use of investigatory powers by the agencies; and
- Creating a right of appeal from the Investigatory Powers Tribunal

D. Parliamentary oversight

1. The Intelligence and Security Committee

a. Functions

The ISC is tasked with overseeing the expenditure, administration, policy and operations of the three intelligence agencies. It may also examine or oversee other intelligence and security matters, as set out in memoranda of understanding agreed between the Prime Minister and the ISC.

The ISC is only able to consider operational matters where:

- they do not relate to ongoing operations and it is in the national interest;
- requested to do so by the Prime Minister; or
- consideration is limited to information voluntarily provided by the Agencies or a government department.

b. Powers and performance of functions

Schedule 1 of the JSA sets out details of the ISC's powers with respect to matters such as access to information. The ISC may ask the heads of any of the three Agencies to disclose information, and they must make it available, or inform the ISC that it cannot be disclosed because the Secretary of State has vetoed disclosure. The same applies to requests for information from Government departments.

The Secretary of State may only veto disclosure of information on two grounds:

- that it is sensitive and should not be disclosed to the ISC in the interests of national security; or
- that it is information of such a nature that, if the Secretary of State were requested to produce it before a Departmental Select Committee of the House of Commons, the Secretary of State would consider (on grounds not limited to national security) it proper not to do so. In making this decision, the Minister must have regard to government guidance concerning the provision of evidence by civil servants to Select Committees.[201]

This represented a change from the previous position, under which the heads of the Agencies were able to decline to disclose information because it was deemed to be sensitive.

---

200 For further information on the background to the IPA, see the following House of Commons Library Briefing Papers: CBP 7371 *Draft investigatory Powers Bill*, 19 November 2015; CBP 7518 *Investigatory Powers Bill*, 11 March 2016; CBP 7578 *Investigatory Powers Bill: Committee Stage Report*, 2 June 2016; CBP 7746 *Investigatory Powers Bill: Lords amendments*, 28 October 2016.

201 Cabinet Office, *Giving evidence to select committees: guidance for civil servants*, October 2014

Information is defined as sensitive under paragraph 5 of Schedule 1 of the JSA if:

- it might identify or provide details of a source of information, other assistance, or operational methods of the Agencies or other parts of the intelligence apparatus;
- it includes information about current or future operations;
- it includes information provided by another country, where the Government of that country does not consent to disclosure.

Evidence provided by witnesses to the ISC may not be used in civil, disciplinary or criminal proceedings, unless it was provided in bad faith.

The ISC is required to make an annual report to Parliament on the discharge of its functions. It is also able to make any other reports that it considers appropriate.

The Agencies are able to request that sensitive material is redacted from reports if publication would damage their work, for example by revealing targets, methods, sources or operational capabilities.

c. Composition and appointment

Members of the ISC are appointed by their respective Houses of Parliament (the House of Commons or the House of Lords), following nomination by the Prime Minister, as set out in section 1 of the JSA.

The current members of the ISC are listed on the website.

The Committee Chair is elected by the Members. The current chair, Dominic Grieve QC, is a former Attorney General.

Members hold their position on the ISC for the duration of the Parliament during which they were appointed. They can be removed by a resolution of the House by which they were appointed, or if they cease to be an MP, or they become a Minister. A member may also resign.

d. Resourcing

Since the JSA made the ISC a "Committee of Parliament", primary responsibility for resourcing rests with Parliament. However, an amendment to the JSA made provision for supplementary funding to be met by the Government. Paragraph 3 of Schedule 1 provides that a Minister of the Crown may:

- make payments to either House of Parliament relating to any expenditure incurred by the ISC; or
- provide staff, accommodation or other resources, either directly to the ISC or via Parliament.

The 2015-2016 annual report explained that the ISC is currently supported by four core staff; six staff working on a particular inquiry;[202] and a part-time investigator. The ISC's core budget is agreed with the Foreign Secretary on behalf of the National Security Council and is set at £1.3m. This excludes security, IT, telecoms, report publication, accommodation, utilities and centrally-provided corporate services. These are currently provided by the National Security Secretariat and the Cabinet Office.[203]

---

202 The Detainee Inquiry, looking at the role of the Agencies in relation to detainee treatment and rendition. It was agreed when this inquiry was established that it would be funded by Government.

203 Intelligence and Security Committee of Parliament, *Annual Report 2015-2016*, HC 444, July 2016

E. Independent oversight

The *Investigatory Powers Act 2016* (IPA) created the new role of Investigatory Powers Commissioner (IPC) to replace the previous independent oversight regime, comprised of the Intelligence Services Commissioner, the Interception of Communications Commissioner, and the Surveillance Commissioner. Lord Justice Fulford was recently appointed as the first IPC for a three-year term.[204]

The IPC, along with a number of judicial commissioners, are appointed by the Prime Minister, following recommendation by the Lord Chancellor; the Lord Chief Justice of England and Wales; the Lord President of the Court of Session; and the Lord Chief Justice of Northern Ireland. The Prime Minister must also consult the Scottish Ministers.

They will be required to keep under review, by way of audit, inspection and investigation, the exercise by public authorities of various statutory functions, including those relating to:[205]

- the interception of communications;
- the acquisition or retention of communications data;
- equipment interference;
- the acquisition, retention and use of bulk personal datasets.

Under section 230 the IPC may also be directed by the Prime Minister to review any other functions of the Agencies.

The IPC will be required to report annually to the Prime Minister. The IPA sets out further detail of what the report must cover, including:

- statistics on the use of investigatory powers;
- information about the results or impact of such use;
- information about the operation of safeguards contained in the Act in relation to items subject to legal privilege, confidential journalistic material and sources of journalistic material;
- information about the use of specific categories of warrant.

Section 235 provides that any "relevant person" must provide a judicial commissioner with documents, information and assistance, as required for carrying out any investigation, inspection or audit. A "relevant person" includes any employee of a public authority and a telecommunications operator or postal operator who is subject to a requirement imposed by the Act.

Funding, staff and facilities for the IPC are provided for by section 238. Funding is determined by the Secretary of State in consultation with the IPC. The Treasury must approve the number of staff. The judicial commissioners' salary and expenses will be determined by the Treasury.

---

204 *Investigatory Powers Commissioner appointed: Lord Justice Fulford*, Press release, Prime Minister's Office, 3 March 2017.

205 Section 229.

F. Executive oversight

1. Warrantry

Ministers are responsible for determining applications to carry out certain activities by the agencies. These include:

- warrants under section 5 of the ISA, which provides that the relevant Secretary of State may issue a warrant for "interference with property or with wireless telegraphy" following an application from one of the intelligence agencies. The action specified in the warrant must be necessary and proportionate to what the warrant seeks to achieve.
- authorisations under section 7 of the ISA, which provides that the Secretary of State may give authorisation for action on the part of MI6 and GCHQ for any act outside of the British Isles which would otherwise attract (criminal or civil) liability within the jurisdiction.
- interception warrants under section 5 of RIPA, which provides that the Secretary of State may issue a warrant on certain specific grounds where it is necessary and proportionate.

2. The Wilson Doctrine

Under a convention known as the "Wilson Doctrine", intelligence agencies will not normally intercept the communications of an MP.

In 2015 the Investigatory Powers Tribunal gave judgment in a case brought by Caroline Lucas MP and Baroness Jones of Moulsecoombe, arising from the Snowden leaks, on the status, meaning and effect of the Wilson Doctrine.[206]

The Tribunal concluded that the Agencies must comply with their own Guidance on the doctrine, which was disclosed for the first time during the proceedings. This makes clear that particular care must be taken to consider whether the interception is necessary and proportionate, and requires that the advice be sought of a legal adviser, the head of the warrantry section and a senior policy officer. The Director General must also be informed. Before deciding whether to issue a warrant, the Secretary of State must consult the Prime Minister, via the Cabinet Secretary.[207]

The Guidance also states that the Wilson doctrine does not apply to the interception of the communications of a Member of a devolved administration.

Section 26 of the IPA would place the requirement for the Prime Minister's approval on a statutory footing. It would also make clear that it applies in relation to members of the Scottish Parliament, the National Assembly for Wales, the Northern Ireland Assembly and UK members of the European Parliament.

G. Judicial oversight

1. Warrantry

When the relevant provisions come into force, the IPA will introduce a new layer of judicial scrutiny to the process of granting warrants to the Agencies.

---

206 [2015] UKIPTrib 14_79-CH

207 Para 11 of the judgement

At present, the relevant Secretary of State is solely responsible for granting warrants, as described above. Under the new procedure, the warrant will not come into force until it has been reviewed by a judicial commissioner.

The new procedure will apply in relation to the following warrants:

- Interception warrants,[208] including:
  - targeted interception warrants, authorising the targeted interception of communications;
  - targeted examination warrants, authorising the targeted examination of the content of communications obtained in bulk; and
  - mutual assistance warrants, authorising requests for, or the provision of, mutual assistance in the execution of a warrant involving the authorities of another jurisdiction.
- equipment interference[209] warrants, including:
  - targeted equipment interference warrants; and
  - targeted examination warrants, which operate in the same way as targeted examination warrants for interception.
- bulk interception warrants,[210] authorising the interception of overseas-related communications in bulk (on a non-targeted basis);
- bulk acquisition warrants,[211] authorising access to communications data in bulk;
- bulk equipment interference,[212] authorising interference with equipment in bulk for the purpose of obtaining overseas-related communications, data or information;
- bulk personal dataset warrants,[213] authorising the retention and examination of bulk personal datasets.[214]

Judicial commissioners are also required to approve decisions to renew or modify these types of warrant.

Judicial commissioners will be appointed as members of the office of the IPC. They will have to hold or have held high judicial office and will subject the Secretary of State's decision to a review, on the same principles as would be applied in an application for judicial review.

---

208 Section 15

209 Section 99. Equipment interference warrants permit interference with equipment for the purposes of obtaining communications or certain data

210 Section 136

211 Section 158

212 Section 176

213 Sections 204 and 205

214 Bulk personal datasets are defined as sets of information including personal data relating to multiple individuals, the majority of whom are not of interest to the intelligence services

These changes provoked considerable controversy during the Bill's passage through Parliament. In particular, the following issues arose during debate:[215]

- Whether political or judicial authorisation is most appropriate in this context. Some of those engaged in the debate felt that the task of issuing warrants is one best suited to independent judges, who are accustomed to weighing up the kind of factors relevant to such decisions, and would ensure that the process is seen to be impartial. It was acknowledged that ministers should have a role to play in issuing warrants in cases with a significant foreign policy dimension, involving more overtly political considerations. Others argued that judges are ill suited to weighing up considerations of national security when reaching decisions on such matters, and that it was important to maintain political accountability to Parliament through the involvement of ministers.
- The appropriate degree of scrutiny by judicial commissioners. The IPA requires that judicial commissioners review the minister's decision, applying the same standards as would apply in a judicial review. There was much debate as to what this would require in practice. Some argued that judicial review would only require consideration of the formal process by which the decision had been arrived at, and that this degree of scrutiny was insufficient. Others argued that judicial review standards would permit consideration of the "full merits" of the decision, and that the test was thus sufficient. Amendments were made to the Bill to ensure that it was clear that, in reviewing a minister's decision, a judicial commissioner would review the necessity and proportionality of the warrant with sufficient care to comply with the duties imposed by section 2 of the Act to protect individuals' privacy.
- The impartiality of the judicial commissioners. Questions were raised concerning the role of the Prime Minister in appointing and removing judicial commissioners, and of whether this might impact on their actual or perceived independence. Another potential conflict of interests was identified in the duality of the judicial commissioners' role in directly approving warrants, and in providing a general oversight and auditing function with respect to the exercise of the powers subject to the warranty procedure.

2. Investigatory Powers Tribunal

The Investigatory Powers Tribunal (IPT) was created by RIPA and given the power to investigate complaints against public bodies' use of investigatory powers.[216]

The IPT's procedures mean that much of its work is conducted in secret, and it is argued that this is necessary in order to ensure the trust and cooperation of the agencies.

However, it has been criticised for being excessively secretive, and procedurally unfair.

In an attempt to address some of these criticisms, the IPA created a right of appeal on a point of law from the IPT, either to the Court of Appeal in England and Wales or the Court of Session in Scotland.

Leave to appeal must be granted, either by the IPT or the appellate court, on the basis that it would raise an important point of principle or practice, or there is some other compelling reason.

This provision is yet to come into force and at present there is no domestic route of appeal from a decision of the IPT. As a result, claimants must pursue appeals to the European Court of Human Rights.

---

215 For background information on the passage of the Bill through Parliament, see the following House of Commons Library Briefing Papers: CBP 7371 *Draft investigatory Powers Bill*, 19 November 2015; CBP 7518 *Investigatory Powers Bill*, 11 March 2016; CBP 7578 *Investigatory Powers Bill: Committee Stage Report*, 2 June 2016; CBP 7746 *Investigatory Powers Bill: Lords amendments*, 28 October 2016

216 Section 65 of the *Regulation of Investigatory Powers Act 2000* sets out the Tribunal's jurisdiction.

H. Cooperation

At present there are a number of mechanisms for cooperation between the different oversight bodies. For example, the Investigatory Powers Commissioner's Office has a duty to give the IPT any assistance that it requires in connection with the investigation, consideration or determination of any matter. This may include the Commissioner's opinion on anything the IPT has to decide, meaning that it can take advantage of the Commissioner's expertise when reaching a decision.[217]

The IPA introduced provisions aimed at further facilitating cooperation:

- Section 230 provides that the ISC can request that the Prime Minister make a direction to the IPC to oversee a new area of activity.
- Under section 231, the IPC is required to inform individuals of serious errors concerning them in the use of investigatory powers, provided it is in the public interest. The individual concerned must also be informed of their right to bring a claim in the IPT, and be provided with the details necessary to bring such a claim.
- Section 236 concerns a situation in which the ISC uncovers an issue that merits further investigation but which is outside its remit, and therefore refers it to the IPC. The IPC is required to subsequently inform the ISC as to whether any further action is to be taken.

---

217 Section 232, *Investigatory Powers Act 2016.*

COMPARATIVE ANALYSIS

Except where otherwise specified, this section of the paper is based on the information provided about the Australian, Canadian, New Zealand and UK arrangements in the preceding sections.

As noted previously, the Congressional Research Service was unable to participate in the preparation of this paper. Accordingly, the paper does not include a specific section on the US, but information on US arrangements has been included in this section based on research conducted by Cat Barker and Samantha Godec.

A. The 'intelligence community'

There are some notable similarities between the intelligence communities of the Five Eyes countries in terms of jurisdiction, function, and discipline.

- All five countries have **signals intelligence** agencies.
- Each has an agency (or agencies) mandated to collect **security intelligence**.
- Each has some form of dedicated **military intelligence** component.
- All countries have specialized agencies or capabilities devoted to **geospatial intelligence**.
- Each country has an office or agency responsible for **all-source analysis** drawing on intelligence from across the whole government.

Nevertheless, there are differences as to which agencies are considered to comprise the intelligence community.

- The **Australian** Intelligence Community currently comprises six specific agencies spanning defence, signals, foreign, geospatial and security intelligence, and a broader national assessments agency.[218]
- **Canada** does not identify an intelligence community distinct from a broader national security community, of which key elements are security, signals and defence intelligence, as well as a national law enforcement agency. Canada does not have a dedicated agency to collect foreign intelligence abroad using human sources (HUMINT).
- In **New Zealand**, three agencies form the core of the intelligence community (security, signals intelligence, and national assessments). Like Canada, New Zealand does not have a dedicated HUMINT foreign intelligence service.
- In the **UK**, there are three core agencies responsible for security intelligence, foreign intelligence, and signals intelligence that form part of the broader 'national intelligence machinery', which includes Defence Intelligence and the Joint Intelligence Committee.
- The **US** Intelligence Community is comprised of 17 military and civilian intelligence-related entities, including defence, signals, security and foreign intelligence, as well as energy, drugs, diplomatic and financial intelligence.[219]

---

218. As noted earlier in this paper, a 2017 review concluded that a more appropriate frame of reference would be a 'National Intelligence Community' comprising the six AIC agencies, ACIC, AUSTRAC, and parts of the AFP and the DIBP.

219 'Members of the IC', Office of the Director of National Intelligence website. See also A Daugherty Miles, *Defense primer: national and defense intelligence*, CRS in Focus, IF10525, Congressional Research Service (CRS), 5 December 2016.

Some of the differences between intelligence communities simply reflect differences in the nature or scope of intelligence collection and analysis. Others reflect the way different nations have chosen to define or characterise their intelligence communities.

B. Oversight mechanisms

Although development was staggered, the oversight mechanisms of the intelligence agencies in each of the Five Eyes countries have converged in a number of ways.

Firstly, the jurisdiction and mandate of almost all the intelligence agencies are now largely governed by statute, which has paved the way for the establishment of oversight mechanisms.

Secondly, whilst intelligence agencies were initially overseen predominantly by the Executive, each country has gradually developed non-Executive oversight mechanisms. Broadly speaking, the majority have developed at least some if not all of the following mechanisms in addition to Executive oversight:

- Specialised parliamentary or congressional committees
- Inspectors-General or Independent Commissioners
- Judicial oversight
- Independent reviewers of national security legislation.

C. Jurisdictional scope of the key oversight mechanisms

Differences between countries in relation to which agencies are taken to be part of the intelligence community have implications for oversight. By way of example:

- Entities that, in the US, would be treated as part of the intelligence community and therefore come within the intelligence oversight framework, fall outside that framework in other countries by virtue of a more narrowly defined intelligence community.
- The parliamentary and independent oversight mechanisms for intelligence agencies in Australia and NZ are very similar, but because Australia defines its intelligence community more broadly than does NZ, those mechanisms apply across a greater portion of the national security apparatus in Australia than they do in NZ.

The key parliamentary/congressional committees and independent oversight bodies also differ in whether their mandate is based around specific agencies or specific activities. There are potential benefits and risks associated with each approach. Basing a mandate around specific activities means that it automatically keeps pace if additional agencies become involved in those activities, but might mean that the oversight body cannot look deeply at the way an agency operates more broadly. Basing a mandate around specific agencies allows the oversight body to scrutinise the full range of those agencies' operations, but can also mean that jurisdiction to examine an issue that extends beyond those agencies is limited. **Table 1** below compares the jurisdiction of the key bodies.

Table 1: Agencies/elements within the jurisdiction of key oversight bodies[220]

	Parliamentary/congressional	Independent
Australia	PJCIS: all AIC agencies (and AFP terrorism functions)	IGIS: all AIC agencies
Canada	NSICOP: will cover activities relating to national security or intelligence	CSIS, CSE and RCMP
New Zealand	ISC: NZSIS and GCSB	IGIS: NZSIS and GCSB
United Kingdom	ISC: main focus is MI5, MI6 and GCHQ; other government activities relating to intelligence and security as agreed in an MOU with the Prime Minister	IPC: particular statutory functions; may be directed by the Prime Minister to review other functions of the Agencies
United States	Congress oversees all USIC agencies[221]	Inspectors-General, PCLOB and PIAB: all USIC agencies[222]

A related issue is whether the key bodies overseeing the intelligence agencies have the jurisdiction to look more broadly at intelligence related matters that extend beyond those core agencies. This is a key issue given the increasing cooperation between the intelligence agencies and the broader national security community, and increased sharing and use of intelligence across governments. Can these bodies examine, for example, the use of security intelligence by an agency outside the 'intelligence community', such as one involved in border protection functions?

Table 2 below compares the extent to which the key bodies in each country are able to examine intelligence related matters across their respective national governments. There is some scope for at least one of the key intelligence oversight mechanisms in each country to examine broader intelligence and security matters, but in most instances there are also clear limits to that power. Further, the parliamentary/congressional committees and independent bodies typically perform different types of oversight, so if only one of them has jurisdiction to look at matters beyond the core intelligence community, the ability to properly examine all such issues remains constrained.

220. A glossary is provided at pages 7–8 of this paper.

221. LE Halchin and FM Kaiser, *Congressional oversight of intelligence: current structure and alternatives*, CRS Report for Congress, RL32525, CRS, 14 May 2012; ZK Goldman, 'The emergence of intelligence governance', in ZK Goldman and SJ Rascoff, eds, *Global intelligence oversight: governing security in the Twenty-First Century*, Oxford University Press, New York, 2016, pp. 207–234.

222. W Ginsberg and M Greene, *Federal Inspectors General: history, characteristics and recent Congressional actions*, CRS Report, R43814, CRS, 8 December 2014; US Government Accountability Office (GAO), *Inspectors General: reporting on independence, effectiveness, and expertise*, GAO, September 2011; Goldman, 'The emergence of intelligence governance', op. cit.

Table 2: Ability of key oversight bodies to examine intelligence related matters[223]

	Parliamentary/congressional	Independent
Australia	PJCIS: limited to matters relating to AIC agencies (and certain AFP functions)	IGIS: may only inquire into an intelligence or security matter relating to another agency or department at the request of the Prime Minister
Canada	NSICOP: jurisdiction based on activities relating to national security or intelligence instead of specific agencies, will mean broader issues may be examined	SIRC, OCSEC, CRCC: each mandated to perform an agency-specific review function. At the time of publication, a bill that would consolidate SIRC and OCSEC into a single review agency (NSIRA) that would also handle CRCC national security-related complaints was before parliament.
New Zealand	ISC: may inquire into an intelligence or security matter not directly related to the activities of NZSIS or GCSB on referral from the Prime Minister	IGIS: limited to matters relating to the NZSIS or GCSB
United Kingdom	ISC: may examine other government activities relating to intelligence and security as agreed in an MOU with the Prime Minister	IPC: jurisdiction is based on specific statutory functions of agencies; while the functions include those of intelligence and some other agencies, the IPC's functions do not include examining broader issues
United States	Congress has broad jurisdiction to examine matters relating to intelligence[224]	PIAB and the IG of the Intelligence Community have broad jurisdiction; PCLOB focuses on privacy and civil liberties.[225]

D. Executive oversight

Oversight of intelligence agencies traditionally sits within the executive branch of government, with responsibility falling to the relevant ministers and ultimately the Prime Minister or President. This is the case for all five countries. In all jurisdictions there are various executive review bodies with 'before the event' and 'after the event' oversight responsibilities. In addition to executive review bodies, in Australia, New Zealand and the UK, the responsible Ministers exercise executive oversight in respect of certain types of warrants and authorisations.

In **Australia**, responsibility for the intelligence agencies rests with the Attorney-General, Ministers for Foreign Affairs and Defence, and ultimately the Prime Minister. Ministers are responsible for authorising the use of certain powers, including searching premises; interception of communications; installation of surveillance devices; access to data on computers; and collection of intelligence on Australian citizens by ASIS, AGO or ASD.

223. A glossary is provided at pages 7–8 of this paper.

224. Halchin and Kaiser, *Congressional oversight of intelligence: current structure and alternatives*, op. cit.; Goldman, 'The emergence of intelligence governance', op. cit.

225. Goldman, 'The emergence of intelligence governance', op. cit.; Privacy and Civil Liberties Oversight Board (PCLOB), 'About the Board', PCLOB website; Office of the Inspector General of the Intelligence Community, 'What we do', Office of the Director of National Intelligence website.

In **Canada**, the Ministers for Public Safety and National Defence, and ultimately the Prime Minister, are responsible for national security issues. The Prime Minister chairs the Cabinet Committee on Intelligence and Emergency Management. Beyond ministerial responsibility, oversight of intelligence agencies is largely implemented by two main executive review bodies, which are restricted to making findings and recommendations.[226] SIRC reviews the activities of CSIS *ex post facto*. SIRC is composed of members of different political parties but is tasked by, and reports to, ministers. CSE is reviewed by the CSE Commissioner, a retired or part-time judge, who can also be tasked by and reports to ministers. In order to collect foreign intelligence and engage in cyber defence activities, CSE operates under ministerial authorizations.

In **New Zealand**, the Prime Minister, as Minister for National Security and Intelligence, is responsible for leading the national security system. The Minister responsible for each intelligence and security agency exercises ministerial oversight within the framework set by the Prime Minister. They have sole responsibility for issuing some warrants and joint responsibility, with the Commissioner of Intelligence Warrants, for issuing others.

In the **UK**, the Prime Minister has overall responsibility for national security matters. The Home Secretary is responsible for MI5, the Foreign and Commonwealth Secretary is responsible for MI6, and the Defence Secretary is responsible for the Defence Intelligence staff. The relevant Ministers also have responsibility for approving warrants or authorisations for various activities including: property or equipment interference; actions of MI6 or GCHQ outside of the British Isles which would otherwise attract criminal or civil liability; and interception warrants. The interception of the communications of Members of Parliament requires the approval of the Prime Minister.

In the **US**, the President has overall responsibility for national security matters, though responsibility for specific components of the USIC is spread across several members of Cabinet (including the Secretaries of State, Defense and Homeland Security), and two Cabinet-level officials (the Directors of National Intelligence and the Central Intelligence Agency).[227] There are several key executive branch mechanisms for overseeing the intelligence community within the Executive Office of the President (EOP) augmented by a large network of agency Inspectors General and legal counsels. Within the EOP, the President's Intelligence Advisory Board (PIAB) and the President's Privacy and Civil Liberties Oversight Board (PCLOB) serve the president in an advisory capacity.[228] Independent commissions, whether appointed by the President (e.g., Weapons of Mass Destruction Commission) or mandated by Congress (e.g., 9/11 Commission) may also play an important role in oversight of the intelligence community.[229]

In each jurisdiction, the distribution of responsibilities across different portfolios means that while the head of government has overall responsibility for national security matters, no one minister is responsible for all of the agencies and components of the intelligence apparatus.

---

226 K. Roach, 'Review and Oversight of Intelligence in Canada: Expanding Accountability Gaps', in Z. Goldman and S. Rascoff (ed.s), Global Intelligence Oversight: Governing Security in the Twenty First Century, OUP, 2016, p.196

227 James Baker, "Intelligence Oversight," *Harvard Journal on Legislation*, Vol. 45, (2008): 199-208, pp. 202-203. See also Bretton G. Sciaroni, "Theory and Practice of Executive Branch Intelligence Oversight," *Harvard Journal of Law and Public Policy*, vol. 12 (1989): 397-432, p. 397.

228 Mark Lowenthal, *Intelligence: From Secrets to Policy*, 6th ed. (Washington D.C.: Sage, CQ Press, 2015), p. 279. See also Executive Order 13462, *President's Intelligence Advisory Board and Intelligence Oversight Board*, signed by President George H.W. Bush, February 29, 2008, at https://www.hsdl.org/?view&did=483878.

229 James Baker, "Intelligence Oversight," *Harvard Journal on Legislation*, Vol. 45, (2008): 199-208, p. 205.

E. Parliamentary or congressional oversight

Each of the Five Eyes countries, with the notable exception of Canada, has established one or more parliamentary or congressional committees specifically to scrutinise the intelligence agencies. The first of the countries to establish separate committees focused solely on intelligence-related activities was the **US**, with the establishment of the Senate Select Committee on Intelligence (SSCI) and House Permanent Select Committee on Intelligence (HPSCI) in 1976 and 1977 respectively, by way of resolution.[230] The SSCI and HPSCI were established to better integrate (not replace) the interests, responsibilities, and depth of intelligence-related expertise of all the intelligence-related standing committees and to respond to the perceptions of widespread abuse by certain intelligence agencies.[231] Following the Iran-Contra scandal of the 1980's, congressional oversight was strengthened under the Intelligence Authorization Act of 1991 to ensure that Congress be kept 'fully and currently informed' of intelligence activities.[232]

Australia, New Zealand and the UK all established similar committees by way of statute. **Australia** established the Parliamentary Joint Committee on ASIO in 1988. The committee's formation followed legislative reforms in 1986 to establish the committee and the IGIS.[233] When he first announced the establishment of the committee, the then Prime Minister noted the "relevant overseas experience of parliamentary scrutiny of intelligence and security agencies" as evidence that such committees could operate effectively.[234] The remit of the Committee was expanded in 2002 and 2005, and since 2005 it has overseen all six agencies comprising the intelligence community.

The US experience also influenced **Canada**, but it repeatedly rejected the idea of strengthening the role of parliamentarians in scrutinizing intelligence activities. Instead, Canada subsumed intelligence oversight within the broader remits of Standing Committees. Bill C-22, when it enters into force, will establish the first committee of parliamentarians to review intelligence issues, but this committee will be an executive rather than parliamentary body.

In the **UK**, oversight by Parliamentarians was established under the Intelligence Services Act 1994 in the form of the Intelligence and Security Committee. The powers and remit of the ISC were later expanded under the Justice and Security Act 2013. Scholars have pointed to the potential influence of the European Court of Human Rights, and the impetus to avoid adverse judgments,[235] as well as the influence of parliamentary oversight bodies which had already been established in the US and Australia.[236]

---

230 The SSCI was created first by Senate Resolution 400: *A resolution to establish a Standing Committee of the Senate on Intelligence Activities*, 94th Cong., 2nd sess., S.Res. 400, May 19, 1976. The following year, House Resolution 658 (H. Res. 658) created the HPSCI: *A resolution to amend the Rules of the House of Representatives and establish a Permanent Select Committee on Intelligence,* 95th Cong., 1st sess., July 14, 1977.

231 Frank Smist, *Congress Oversees the Intelligence Community*, 2nd ed. (Knoxville: U. of Tennessee Press, 1994).

232 R. Morgan, 'Oversight Through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Activities', in Z. Goldman and S. Rascoff (ed.s), Global Intelligence Oversight: Governing Security in the Twenty First Century, OUP, 2016, p.63

233 The Bills establishing the committee and the IGIS were introduced together in May 1986.

234 R Hawke, 'Report and Ministerial statement: Royal Commission on Australia's Security and Intelligence Agencies', House of Representatives, *Debates*, 22 May 1986, pp. 2885–2892.

235 J. Moran and C. Walker, 'Intelligence Powers and Accountability in the UK', in Z. Goldman and S. Rascoff (ed.s), Global Intelligence Oversight: Governing Security in the Twenty First Century, OUP, 2016

236 R. Morgan, 'Oversight Through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Activities',p.61

New Zealand established the Intelligence and Security Committee in 1996. An important consideration in the establishment of both the Committee and the IGIS was the desirability of closer conformity with accountability practice and procedure in the UK, Australia and Canada in relation to their intelligence and security agencies.[237]

1. Mandates

Although each country, with the exception of Canada, has established a parliamentary or congressional committee, the mandates of these committees differ.

In the **US**, while each of the relevant committees has some limits on what they may examine (for example, there is a distinction drawn between military and other forms of intelligence), there are no official limits on what these committees, taken collectively, may inquire into in terms of the intelligence-related activities of the US Government.

The mandate of the **UK**'s ISC, whilst not as far-reaching as the US committees, permits the review of policies, administration and expenditure of the intelligence agencies as well as operational activities in certain circumstances. The ISC may only consider operational activities when requested to do so by the Prime Minister; where the operations are no longer ongoing; or where information is disclosed voluntarily.

Neither the **New Zealand** ISC nor the **Australian** PJCIS is permitted to review operational matters. They are charged with examining the administration and expenditure of the agencies (and in the case of the ISC, also their policies), and other matters referred by a house of Parliament or minister (in New Zealand, the Prime Minister; in Australia, a minister responsible for an intelligence agency). The Australian PJCIS may not inquire into individual complaints about the activities of an intelligence agency. The New Zealand ISC may only inquire into complaints by individuals concerning the activities of an agency where they are not capable of being resolved under any other enactment.

In **Canada**, the NSICOP will have powers of review in relation to policy, administration and expenditure of the intelligence agencies, emulating the powers of the ISC in New Zealand. Similarly to the UK, the NSICOP will also have the power to review operations as long as the operations are not ongoing, or where the appropriate Minister determines that the operational review would not be injurious to national security. However, the NSICOP will be a committee of parliamentarians (as opposed to a parliamentary committee) and would therefore remain part of the Executive.

2. Powers

a. Initiating inquiries

The parliamentary and congressional committees may initiate their own inquiries or investigations into:

- in the **US** and **UK**, any matter within the committee's jurisdiction;
- in **New Zealand**, the policies, administration and expenditure of the intelligence and security agencies;
- in **Australia**, the administration and expenditure of the intelligence agencies; and
- in **Canada** the NSICOP will be able to initiate its own inquiries into any matter within its mandate (subject to the limitation relating to ongoing operations noted above).

237 Intelligence and Security Agencies Bill, as reported from the Committee on the Intelligence and Security Agencies Bill, p. ii, 1996

The matters that the Australian and New Zealand committees may examine upon referral from a minister or the Prime Minister respectively, or from a House of Parliament, are broader than the matters they may inquire into of their own accord.

While it may not undertake such an inquiry itself, the New Zealand ISC may request that the NZ IGIS conduct an inquiry into any matter relating to an agency's compliance with the law, or the propriety of its activities. A similar power has been recommended for the Australian PJCIS.

b. Obtaining information

While the mandates of the committees differ, the powers the committees have to examine matters within their mandate are broadly equivalent.

The **US** President must ensure that the congressional committees are "fully and currently informed" of intelligence activities and "promptly" notified of collection and covert action programs, and any illegal intelligence activities.[238] The committees may call officials to testify at hearings and require that information be provided.

In **Australia**, **New Zealand** and the **UK**, the committees have similar powers to request briefings or appearances from the heads of the intelligence agencies, as well as any other person required to give evidence or produce documents. However, in all jurisdictions there are limits to the information that may be requested or compelled under these powers in order to protect sensitive operational information, as further outlined below.

c. Disclosure

There are limitations placed on the committees' access to sensitive information. In **Australia**, the PJCIS must not require a person or body to disclose to the committee operationally sensitive information or information that would or might prejudice Australia's national security or the conduct of Australia's foreign relations. Ministers may also issue certificates preventing the disclosure of operationally sensitive information to the PJCIS. In **New Zealand**, the heads of the agencies can refuse to disclose sensitive information. However, the Prime Minister can override the refusal of an agency head to disclose information if it is in the public interest to do so. In the **UK**, the position is slightly different: heads of agencies can only avoid disclosure to the ISC if a request for disclosure is vetoed by the Secretary of State. This veto power can only be exercised if the information is sensitive and should not be disclosed in the interests of national security, or if it is not proper to do so in accordance with the relevant guidance. In the **US**, disclosure depends on a number of factors such as the sensitivity of the issue and operational necessities. For example, 'Gang of Eight' notifications refer to issues so sensitive that only eight Members of Congress are notified.[239]

238 50 U.S.C. §§ 3091-3093. Section 3092 governs oversight of intelligence activities that are not covert actions and Section 3093 governs oversight of covert actions.

239 Mark Lowenthal, *Intelligence: From Secrets to Policy*, 6th ed. (Washington D.C.: Sage, CQ Press, 2015), p. 298. The *Gang of Eight* consists of the leaders of each of the two political parties from both the Senate and the House of Representatives (Speaker of the House and the House Minority Leader and the Senate Majority and Minority Leaders) along with the chairs (majority) and ranking Members (minority) of the HPSCI and the SSCI.

F. Independent oversight

Each jurisdiction has some form of independent oversight. In **Australia** and **New Zealand**, this function is carried out by an Inspector-General of Intelligence and Security (IGIS). In the **UK**, this function will be carried out by the newly appointed Investigatory Powers Commissioner (IPC). In Canada, the executive relies upon three expert review bodies: SIRC, CRCC and OCSEC. If Bill C-59 is passed, this would effectively consolidate the OCSEC and SIRC into a single body, the NSIRA.

The **US** has a government-wide system of inspectors-general (IGs), which includes IGs that oversee specific intelligence agencies and an IG of the Intelligence Community with cross-agency jurisdiction.[240] It also has two boards that serve the President in an advisory capacity: the President's Intelligence Advisory Board (PIAB) and the Privacy and Civil Liberties Oversight Board (PCLOB).[241]

1. Appointment

The **Australian** and **New Zealand** IGISs are appointed by the Governor-General.[242] In contrast, the **UK**'s IPC is appointed by the Prime Minister, and the **US**'s PCLOB and PIAB members are appointed by the President. There are several methods by which IGs are appointed in the US. The IG of the Intelligence Community is appointed by the President with the advice and consent of the Senate, as are many of the IGs overseeing individual agencies or components.[243]

The **Canadian** SIRC, CRCC and Communications Security Establishment Commissioner are each appointed by the Governor in Council.[244]

2. Functions

The IGISs in **Australia** and **New Zealand** share a similar mandate, which differs from that of the IPC in the UK. The IGISs are responsible for reviewing the operational activities of the intelligence agencies to ensure legal compliance and propriety. In order to carry out their mandates, they are empowered to conduct inquiries into certain matters and to carry out inspections. Inquiries may be conducted at the request of the responsible minister, the Prime Minister, or on their own accord. In New Zealand, the ISC can also request inquiries. The IGISs have the powers to summon and examine persons, compel documents, and enter agency premises. Given the relatively strict limitations on parliamentary oversight in Australia and New Zealand, the IGISs play an important role in holding the agencies to account.

The role of the **UK** IPC differs from that of the IGISs in Australia and New Zealand. The IPC is mandated to keep under review certain statutory *functions*, as opposed to a broad power to review the general *activities* of intelligence agencies (with the exception of review of other functions of the Agencies if directed by the Prime Minister). Specifically, the IPC may audit, inspect and investigate the interception of communications; the acquisition and retention of communications data; equipment interference; and

---

240. Ginsberg and Greene, *Federal Inspectors General: history, characteristics and recent Congressional actions*, op. cit.; GAO, *Inspectors General: reporting on independence, effectiveness, and expertise*, op. cit.

241. Goldman, 'The emergence of intelligence governance', op. cit

242. In Australia, the Prime Minister recommends an appointee after consulting the Leader of the Opposition. In New Zealand, Parliament recommends an appointee.

243. Ginsberg and Greene, *Federal Inspectors General: history, characteristics and recent Congressional actions*, op. cit., pp. 3–5; GAO, *Inspectors General: reporting on independence, effectiveness, and expertise*, op. cit., pp. 21–24.

244 In Canada, the heads of the SIRC, OCSEC and CRCC are all Cabinet appointees. The Canadian Prime Minister consults Parliament only with respect to the SIRC appointment.

the acquisition, retention and use of bulk personal datasets. These powers of review are in addition to the IPC's powers to authorise certain types of warrants, resulting in a hybrid body which both approves warrants *before the event* and reviews certain types of activity *after the fact*.

In **Canada**, the expert review bodies are mandated to investigate complaints and examine the lawfulness of the activities of Canada's intelligence and national security agencies.

In the **US**, IGs for specific agencies and the Inspector General of the Intelligence Community may conduct audits of, and investigations into, the programs and operations of agencies they oversee. The PIAB oversees the US intelligence community's compliance with applicable laws, Executive Orders and Presidential Directives, while the PCLOB is tasked with ensuring 'that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties'.[245] Both Boards sit within the executive branch but employ external experts to ensure a degree of independence.[246]

In addition, both **Australia** and the **UK** have established independent legislation monitors—the Independent National Security Legislation Monitor and the Independent Reviewer of Terrorism Legislation respectively. In both jurisdictions, the independent monitors are empowered to review the operation and effectiveness of national security legislation, as opposed to the agencies themselves. However, in performing their roles, they examine the way that agencies apply those laws and may recommend changes to laws, processes and oversight arrangements.[247]

G. Judicial oversight

Traditionally, the judiciary has exercised deference on national security issues. Judicial oversight of intelligence agencies remains limited and divergent amongst the five nations.

In **Australia**, the judiciary has little involvement in the authorisation of the exercise of powers, most of which rests with ministers. Decisions made under laws governing the intelligence agencies are excluded from the statutory framework for judicial review of executive decisions, but individuals have some scope to apply for judicial review of the legality of actions taken by intelligence officers. The Security Division of the Administrative Appeals Tribunal can undertake merits reviews of most types of adverse security assessments issued by ASIO (which are relied on in a range of administrative decisions, such as passport cancellation) in closed session.

In **Canada**, specially designated judges in the Federal Court approve warrants requested by CSIS to conduct electronic and other forms of surveillance. For the limited purposes of threat disruption, judges may also approve warrants where CSIS wishes to violate Canadian laws or limit Charter rights within

245 PCLOB, 'About the Board', op. cit.

246 Z. Goldman, 'The Emergence of Intelligence Governance', in Z. Goldman and S. Rascoff (ed.s), Global Intelligence Oversight: Governing Security in the Twenty First Century, OUP, 2016, p.226

247 The Independent National Security Legislation Monitor is even given a specific function of assessing 'whether Australia's counter-terrorism or national security legislation is being used for matters unrelated to terrorism and national security': INSLM Act, paragraph 6(1)(d). The UK Independent Reviewer of Terrorism Legislation has a statutory powers to review the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006 (section 36 of the 2006 Act); to review the operation of the Terrorism Prevention and Investigation Measures Act 2011 (section 20 of that Act); to review the Terrorist Asset-Freezing etc. Act 2010 (Part 1) (section 31 of that Act); to report on the operation of three other statutes, in whole or in part: the Anti-Terrorism Crime and Security Act 2001, the Counter-Terrorism Act 2008 and the Counter-Terrorism and Security Act 2015 (section 44 of the Counter-Terrorism and Security Act 2015).The Independent Reviewer may at the request of Ministers or on his own initiative conduct reviews and produce reports on specific issues.

Canada or abroad.[248] There is no judicial oversight of CSE, Canada's signals intelligence agency, which does not require warrants to conduct its activities. However, if Bill C-59 is passed, certain proposed CSE ministerial authorizations will be subject to the approval of a newly created Intelligence Commissioner who must be a retired judge of a superior court.

In **New Zealand** a Commissioner of Intelligence Warrants, who must be a former High Court judge, has joint responsibility with the authorising Minister to issue Type 1 warrants, which authorise an agency to carry out otherwise unlawful activity in relation to a New Zealand citizen or permanent resident. Responsibility for the issue of Type 2 warrants, which authorise otherwise unlawful activity that does not relate to New Zealand citizens or permanent residents, lies solely with the authorising Minister and does not require the involvement of a Commissioner.

In the UK and the US, specific courts have been established to deal with intelligence-related matters, although their mandates are distinct. In the **UK**, the Investigatory Powers Tribunal (IPT) hears complaints of unlawful use of covert techniques by public authorities and provides a right of redress for victims of unlawful action, with a right of appeal on a point of law (although this right of appeal was not in force at the date of publication). The **US** Foreign Intelligence Surveillance Court not only approves warrants for intelligence-gathering, but oversees entire intelligence programmes and grants court orders for conducting foreign intelligence investigations, including electronic surveillance and physical searches.[249]

1. Recent cases

Despite the limited judicial oversight of intelligence agencies, there have been some recent court cases holding intelligence agencies to account, particularly in relation to intelligence-sharing. Since 2013, the Canadian Federal Court has twice held that CSIS had failed in its duty of candour when it did not inform the Court that it would rely upon assistance from its Five Eyes partners in executing surveillance orders, and when it failed to inform the Court for a decade that it was retaining metadata collected on individuals who were not the target of a warrant.[250] Similarly, in the UK, the IPT held that intelligence-sharing between the UK and US contravened the European Convention on Human Rights due to the lack of public clarity regarding the legal framework for such intelligence-sharing.[251] Further, the Court of Justice of the European Union (CJEU) has found that, under the Safe Harbour Agreement between the EU and the US, US agencies were accessing data beyond that which is permitted by the EU data privacy rules.[252] The sharing of intelligence is therefore a matter which is subject to judicial scrutiny.

Data retention powers have also been subject to recent judicial scrutiny. In the UK, the High Court recently held that the UK's emergency data retention legislation, the Data Retention and Investigatory Powers Act 2014, violated EU data privacy rules in large part due to inadequacies in the oversight regime created by the legislation.[253]

---

248 K. Roach, 'Review and Oversight of Intelligence in Canada: Expanding Accountability Gaps', in Z. Goldman and S. Rascoff (ed.s), Global Intelligence Oversight: Governing Security in the Twenty First Century, OUP, 2016, p. 193

249 Frederic Manget, "Intelligence and the Rise of Judicial Intervention: Another System of Oversight," *Studies in Intelligence*, vol. 39, no. 5 (CIA's Center for the Study of Intelligence, 1996): 43-50, p. 47.

250 See *X (Re), 2013 FC 1275* and *2016 FC 1105*, respectively.

251 *Liberty v Secretary of State for the FCO and Others*, UKIPT 13-77-H

252 *Schrems v Data Protection Commissioner*, 6 October 2015, Case C-362/14

253 *Davis and Others v Secretary of State for the Home Department,* EWHC 2092 (Admin) 2015. Upon appeal to the Court of Appeal, referral was made to the CJEU, which held that the data retention power exceeds the limit of what is strictly necessary and cannot be considered to be justified, within a democratic society. The matter is referred back to the Court of Appeal and judgment is pending.

H. Budget information

Each of the countries examined makes some information available about the budget allocations to intelligence agencies, but none makes public the separate allocations for all agencies.

Australia's national budget papers include agency-specific allocations for ASIO, ASIS and ONA (though it appears that not all funding is included, at least for ASIO and ASIS). The allocations for the three agencies in the Defence portfolio are included in the broader budget for the Department of Defence.

Canada and **New Zealand** are similar to Australia in that budgets are made public for the CSIS, CSE and RCMP (in the case of Canada) and NZSIS and GCSB (in the case of New Zealand), with other intelligence-related funding included in budgets for broader portfolios but not disaggregated.

The **UK** Government releases a Single Intelligence Account that outlines the total funding across MI5, MI6 and GCHQ (though GCHQ also receives funding under the National Cyber Security Programme).[254] Other intelligence-related funding is included in the broader budget for the Ministry of Defence.

The **US** Government publishes the total budgets allocated to the two major components of its intelligence budget—the National Intelligence Program and the Military Intelligence Program. However, some intelligence funding falls outside those programs.[255]

CONCLUSION

There will always be a tension in democratic societies between the need for intelligence agencies to operate largely in secret, and the need for those agencies to be held accountable for their actions. The frameworks developed by the five countries considered in this paper represent the compromises reached between these two imperatives.

This research paper highlights the differences in the way that each country has chosen to conduct oversight of the intelligence community. What might work well in one country may not necessarily be consistent with the institutions and norms of another. Instead, the oversight frameworks reflect each nation's political structure, history, and culture, and therefore differ in some of the particulars. However, each country has developed a framework that includes a system of checks and balances that spans the various branches of government, and which aims to ensure that agencies are accountable for both their administration and expenditure and the legality and propriety of their activities.

The intelligence communities have evolved to meet new challenges as they arise, and will continue to do so. It will be important for the oversight arrangements to keep pace with such changes, and there may well be lessons that the countries considered in this paper can learn from one another as they each continue to review and strengthen their oversight mechanisms.

---

254 'Security and intelligence agencies financial statement 2015 to 2016', UK Government website; 'GCHQ funding and financial controls', GCHQ website.

255 'U.S. intelligence community budget', Office of the Director of National Intelligence website. See also A Daugherty Miles, *Intelligence Community Spending: Trends and Issues*, CRS Report, R44381, CRS, 8 November 2016; A Daugherty Miles, *Intelligence Community Programs, Management, and Enduring Issues*, CRS Report, R44681, 8 November 2016.