1

Introduction

1.1 There are six intelligence agencies in Australia that comprise the Australian Intelligence Community (AIC):

- Australian Security Intelligence Organisation (ASIO),
- Australian Secret Intelligence Service (ASIS),
- Australian Geospatial-Intelligence Organisation (AGO)—formerly Defence Imagery and Geospatial Organisation (DIGO),[1]
- Defence Intelligence Organisation (DIO),
- Australian Signals Directorate (ASD)—formerly Defence Signals Directorate (DSD), and
- Office of National Assessments (ONA).

1.2 Together, AGO, DIO and ASD are known as the Defence Intelligence Agencies (DIAs) and with the Defence Security Authority,[2] comprise the Intelligence and Security Group of the Department of Defence.

1.3 The AIC operates within a strict oversight and accountability framework, which balances the need for public accountability with the need for agency operations and other sensitive information held within agencies to remain classified to protect Australia's national security.

1.4 Within this oversight framework, the intelligence agencies have limited *public* reporting responsibilities because of the need to protect certain

---

1 The change of name for DIGO/AGO and DSD/ASD had been implemented during the reporting period but had not yet been formalised in legislation. The Committee uses the terms AGO and ASD throughout this report. The National Security Legislation Amendment Bill (No.1) 2014, which received Royal Assent on 2 October 2014, gave legislative effect to the name changes.

2 The Defence Security Authority is responsible for supporting Defence to protect its business from unacceptable security risks and for providing security clearances for individuals in Defence, the defence industry and most government departments. It does not fall within the oversight of this Committee.

information about the agencies' work. ASIO is the only intelligence agency that produces an annual unclassified report to Parliament.[3]

1.5 Notwithstanding the need to keep certain information confidential, there are several levels of oversight to ensure that intelligence agencies are held accountable to the Australian Government, to the Parliament and through it to the Australian public. This oversight includes:

- the Inspector-General of Intelligence and Security (IGIS), who provides independent assurance that the AIC agencies conduct their activities within the law, behave with propriety and comply with ministerial guidelines and directives,[4] and
- parliamentary oversight, including oversight of administration and expenditure by the Parliamentary Joint Committee on Intelligence and Security.

Role of the Committee

1.6 The Committee was established pursuant to section 28 of the *Intelligence Services Act 2001* (the IS Act). Its functions include an obligation to review the administration and expenditure of each of the intelligence agencies, including their annual financial statements.[5]

1.7 This important oversight role is carried out in circumstances where the transparency and public accountability of the intelligence agencies must be balanced with the need to protect national security.

1.8 The Committee is privy to detailed, largely classified, information about the administration and expenditure of agencies. Each agency provides information on its administration and expenditure to the Committee in the form of written submissions, by appearing to give evidence in private (classified) hearings, and by providing private briefings to the Committee, at its request. Much of the evidence received by the Committee must remain confidential, due to its classified nature.

1.9 The Committee does not consider that its role in these reviews extends to advising what level of resources is appropriate for each agency to maintain to protect Australians from risks to its national security. Similarly, the Committee has no role in determining what the national

3 See ASIO, *Submission 6.1*, p. 36.

4 See <www.igis.gov.au>.

5 See section 29 of the IS Act.

security priorities should be,[6] nor how these priorities may be met with existing resources.

1.10 Rather, the Committee has responsibility to analyse the evidence put before it and report to the Parliament (and through it, to the Australian community) on any changes to administration and expenditure, or any other issues which the Committee identifies, that may affect the agency's ability to continue to meet its objectives.

Conduct of the inquiry

1.11 The Committee commenced its inquiry on 25 September 2014.

1.12 Submissions were sought and received from the six intelligence agencies, the Auditor-General for Australia and the IGIS. A list of submissions is at Appendix A.

1.13 The majority of submissions received were classified by the respective agencies. Accordingly, these submissions have not been authorised for publication and are not publicly available. Unclassified excerpts from these submissions are used in the report.

1.14 Unclassified submissions from ASIO, the Department of Defence, IGIS and ONA are also available on the Committee's website.

1.15 Private (classified) hearings were held on 19, 25 and 26 March 2015. Representatives of the six intelligence agencies and the IGIS appeared before the Committee. A list of the private hearings and witnesses who appeared before the Committee is at Appendix B.

1.16 Administration of the intelligence agencies is discussed in Chapter 2.

1.17 The expenditure and financial position of the intelligence agencies are discussed in Chapter 3.

The security environment in 2013–14

1.18 ASIO updated the Committee on the security environment in 2013–14 and the outlook for the years ahead, noting that Australia's security 'faces a broad array of challenges at an intensity not seen since the end of the Cold War'.[7]

---

6 Reviewing the intelligence gathering and assessment priorities of agencies is expressly prohibited under paragraph 29(3)(a) of the IS Act.

7 ASIO, *Submission 6.1*, p. 8.

1.19 ASIO outlined security challenges in the following key areas:

- terrorism,
- espionage and clandestine foreign interference,
- the cyber threat, and
- border integrity.[8]

1.20 ASIO particularly highlighted a worsening situation with regard to terrorism, identifying the conflict in Syria and Iraq as a 'major challenge', with the principal terrorist threat coming from

> Australian Islamist extremists who subscribe to the distorted narrative that Australia is at war with Islam, and that the use of violence to support their ideology is not only legitimate but necessary.[9]

1.21 The submission stated that

> [t]he terrorist threat from Islamist extremists is increasingly serious and significant, and future prospects in the Middle-East, Africa, South-East Asia and the West are concerning. This worsening situation has direct ramifications for Australians and Australian interests and will have generational impact globally. An emerging challenge is an increasing number of individuals who reject Australia's democratic system and act to spread discontent within it.[10]

1.22 ASIO also highlighted the 'significant' scale and breadth of espionage against Australia:

> The risk to Government information—as well as the information shared by our closest international partners—is significant and carries serious implications for our national sovereignty and prosperity and our reputation with international partners. Beyond the threat to Government business, Australia's commercial, economic, and research and development activities are being targeted, representing a risk to future economic prosperity.[11]

1.23 Investigations conducted over the reporting period had increased ASIO's understanding of the threat from clandestine activity by foreign powers. ASIO advised that it was working closely with business, government and key intelligence partners to counter that threat. However, the submission also noted that

8 ASIO, *Submission 6.1*, pp. 8–9.
9 ASIO, *Submission 6.1*, p. 8.
10 ASIO, *Submission 6.1*, p. 8.
11 ASIO, *Submission 6.1*, p. 8.

> continued unauthorised disclosures of sensitive information during the reporting period have highlighted the threat posed by self-motivated malicious insiders … [who] are a constant source of potential harm to Australia's national interests.[12]

1.24 In particular, ASIO noted that the damage caused by unauthorised disclosures by the former US National Security Agency contractor, Edward Snowden, was 'expected to be felt for many years'.[13]

1.25 Cyber threats increased in 2013–14, with the range, scale and sophistication of cyber espionage by state actors also continuing to increase.[14]

1.26 Regarding border integrity, ASIO noted that while the number of 'illegal maritime arrivals' had declined significantly since July 2013, 'maritime people smuggling continues to be a threat to Australia's border integrity and security'.[15]

1.27 Providing an outlook for the security environment, ASIO advised that:

- the conflict in Syria and Iraq would remain a significant challenge over the next 12 months and well beyond,
- an increasing number of extremists who have fought in Syria and Iraq may attempt to return to their home countries—these people 'will likely return strongly radicalised with an increased capability',
- the security environment in south and central Asia and in Africa would continue to deteriorate, with areas in these regions continuing to provide 'safe havens for al-Qa'ida and its affiliates and environments conducive to radicalisation, training and potentially, plotting against the West',
- lone actors would 'present an ongoing challenge' to national security and public safety, and
- there would be persistent challenges from clandestine foreign activity targeting Australian government and business information, as well as threats from the actions of 'malicious insiders'.[16]

12 ASIO, *Submission 6.1*, p. 9.
13 ASIO, *Submission 6.1*, p. 9.
14 ASIO, *Submission 6.1*, p. 9.
15 ASIO, *Submission 6.1*, p. 9.
16 ASIO, *Submission 6.1*, p. 10.