2017 INDEPENDENT INTELLIGENCE REVIEW

June 2017

2017 INDEPENDENT INTELLIGENCE REVIEW

June 2017

COPYRIGHT STATEMENT

2017 INDEPENDENT INTELLIGENCE REVIEW

ISBN 978-1-925362-53-4 2017 Independent Intelligence Review (Hardcopy)
ISBN 978-1-925362-54-1 2017 Independent Intelligence Review (PDF)
ISBN 978-1-925362-55-8 2017 Independent Intelligence Review (HTML)

Department of the Prime Minister and Cabinet

PO Box 6500
CANBERRA ACT 2600
Tel: +61 2 6271 5111
Fax: +61 2 6271 5414
www.dpmc.gov.au

TABLE OF CONTENTS

[This page intentionally left blank]

EXECUTIVE SUMMARY

This Report sets out the conclusions we have drawn from an extensive, wide-ranging study of the Australian intelligence community conducted from November 2016 to June 2017. We engaged intensively with the leaders of Australia's intelligence agencies. We also met with Ministers and Parliamentarians, with present and former members of the Australian and allied intelligence communities, and with senior officers of the operational and policy agencies that represent the primary customers of the intelligence agencies. Our Report draws heavily on the insights we derived from these meetings (which numbered over 150) and from our detailed analysis of the 34 Submissions we received from agencies and departments as well as the wider community.

It is clear to us that the Australian intelligence agencies are highly capable and staffed by skilled officers of great integrity. They have performed strongly since the most recent review of the intelligence community in 2011, particularly in the areas of counter-terrorism, support to military operations and assistance in addressing the issue of people smuggling. Our agencies have a strong positive culture of accountability under law and to responsible Ministers. Individually, the agencies feature world-class tradecraft and very high levels of professionalism. They are held in high regard by their international partner agencies.

A central theme of this Report is to provide a pathway to take those areas of individual agency excellence to an even higher level of collective performance through strengthening integration across Australia's national intelligence enterprise. The aim is to turn highly capable agencies into a world-class intelligence community.

In our view, progress towards this objective will require changes to the co-ordinating structures of our intelligence community, new funding mechanisms to address capability gaps, the streamlining of some current legislative arrangements, and measures to further strengthen the state of trust between the intelligence agencies and the Australian community of which they are part. This Report addresses each of these priorities.

Our national intelligence community is facing imposing challenges that, in our view, will intensify over the coming decade. Some of these challenges derive from new forms of rivalry and competition among states, the threat posed by extremism with global reach, particularly Islamist terrorism, and

the implications of accelerating technological change for Australia's national security outlook. Other challenges reflect the changing nature of twenty-first century intelligence, and especially the new frontiers of data-rich intelligence and the risks to comparative technical advantages.

These forces of change are challenging the structures in place for co-ordinating the activities of our intelligence agencies. Those structures were established some decades ago on the basis of principles set out in the landmark Royal Commissions into the intelligence agencies conducted by Mr Justice Hope in the mid to late 1970s and early 1980s. The clear dividing lines he highlighted – between foreign and security intelligence, intelligence and law enforcement, intelligence collection and assessment, and intelligence assessment and policy formulation – continue to provide the foundations of Australia's intelligence community. We assess those delineations have broad enduring relevance. They capture, in particular, the essential requirements for a relationship of trust between government and the wider community in Australia about the legitimate uses of intelligence, and therefore the legal framework within which the agencies need to operate. At the same time, Australia's future security environment will demand greater levels of collaboration across traditional dividing lines and more cross-over points.

The intelligence co-ordination arrangements recommended by Mr Justice Hope have undergone only minor change over the past 40 years. In our view, they need to reflect the contemporary and future challenges that our intelligence agencies face as a result of transforming geopolitical, economic, societal and technological changes.

We consider there are important conclusions Australia can draw from the recent experiences of our most important intelligence partners. All our Five Eyes partners have a single point of co-ordination for their intelligence communities. Australia's co-ordination arrangements are not as clear. The United States and the United Kingdom, in particular, have taken practical steps to build synergies among their agencies in response to the demands of twenty-first century intelligence. Australia is doing the same in particular areas but it needs to do much more. It is notable that both the United States and the United Kingdom took steps after the attacks of 11 September 2001 and 7 July 2005 respectively to strengthen the co-ordination and integration of their intelligence communities. They have continued to do so in the intervening period and the result in both countries is strong, strategic-level management of intelligence as a national

enterprise built on the specific attributes of individual agencies. This has enhanced both effectiveness and efficiency, even against the tragic backdrop of terrorist attacks over recent years.

We strongly recommend that Australia learn from these experiences of our Five Eyes partners. We have not recommended that Australia simply replicate the measures our allies have taken, but rather we have sought to apply the principles to the Australian context in a way that is consistent with the Australian system of Ministerial responsibility and the statutory powers of agencies.

With an annual budget approaching $2 billion and about 7,000 staff spread across 10 agencies, it is clear to us that on size alone the Australian Government's intelligence activities supporting national security are now a major enterprise. They would benefit from being managed as such.

Our major recommendation is that an Office of National Intelligence (ONI) be established in the Prime Minister's portfolio. This Office would be headed by a Director-General who would be the Prime Minister's principal adviser on matters relating to the national intelligence community. The Director-General would not be empowered to direct the specific activities of agencies, but should be able to direct the co-ordination of the national intelligence community to ensure there are appropriately integrated strategies across the suite of agency capabilities.

ONI would be responsible for enterprise-level management of the national intelligence community, leading the development and implementation of national intelligence priorities, undertaking systematic and rigorous evaluation of the performance of the agencies, implementing strategic workforce planning and facilitating joint capability planning including for the development of an environment for enhanced data sharing and collaborative analysis. ONI would subsume the Office of National Assessments and undertake the intelligence assessment function in an expanded way that includes greater contestability and more extensive engagement with external expertise.

The theme of establishing strong, enterprise-level management of the national intelligence community to complement the strengths of individual agencies runs through our recommendations. It is particularly evident in our recommendations for new funding arrangements. A key recommendation we make in this context is to establish a Joint Capability Fund. This Fund would support technological innovation and the development of

shared capabilities designed to be used across the different agencies of the national intelligence community. A further recommendation is to complement the Joint Capability Fund with a comprehensive, forward looking Intelligence Capability Investment Plan. This Plan would enable government to make better-informed decisions on the inevitable capability trade-offs that will be needed in future years, and to provide agencies with a greater degree of certainty about their future budgetary outlook to assist forward planning.

The theme of stronger integration also informs our recommendations on changes to the legislative framework in which the agencies operate, many of which are designed to create more cross-over points between agencies and to allow the full suite of Australia's intelligence capabilities to be used more readily in support of national intelligence priorities.

In addition to the establishment of ONI, we also recommend a significant change to the structure of the intelligence community in regard to the Australian Signals Directorate (ASD). This is presently within the Department of Defence, with the Director reporting to the Minister for Defence through a Deputy Secretary and the Secretary of the Department. Given its increased national responsibilities especially in relation to cyber security and also mindful of the critical operational capabilities it provides to the Australian Defence Force (ADF), we recommend that ASD become a statutory authority within the Defence portfolio. We also recommend that ASD's priority role of supporting ADF capabilities be clearly reaffirmed and strengthened in new legislation. We further recommend that ASD's legislative mandate be amended to explicitly recognise its national responsibilities for cyber security, including the provision of advice to the private sector, and that it take formal responsibility for the Australian Cyber Security Centre.

Our Report addresses current arrangements for oversight and accountability of the intelligence community. We consider that those arrangements are appropriately rigorous. They constitute a well-structured set of arrangements that provide independent assurance about the legality and propriety of intelligence operations and the management of resources. But the demands in this area are growing due to the increase in the size of the national intelligence community and the greater powers it has been given to address contemporary threats. Accordingly, we recommend that the remit of both the Inspector-General of Intelligence and Security (IGIS) and the Parliamentary Joint Committee on Intelligence

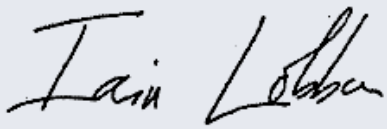
and Security be expanded to cover the ten agencies which we consider now properly constitute the national intelligence community. We also recommend a significant strengthening of the Office of the IGIS through a substantial increase to its authorised staffing level. We further recommend an expanded set of functions for the Parliamentary Joint Committee.

In this Report, we have sought to identify likely strategic trends over the coming decade, to identify the issues they pose for our intelligence agencies and to make recommendations designed to address them. Those trends and issues will continue to evolve over coming years, and responses to them need to be kept under review.

We consider that Australia is well served by its intelligence agencies. But the challenges they face are significant and over coming years their capabilities, as well as the effectiveness of our intelligence community as a whole, will be significantly tested. The changes we recommend in this Report are designed to ensure that Australia is as well placed as it possibly can be to meet those challenges.

Michael L'Estrange AO
(Reviewer)

Stephen Merchant PSM
(Reviewer)



Sir Iain Lobban KCMG, CB
(Adviser)

[This page intentionally left blank]

CONTEXT OF THE REVIEW

On 7 November 2016 the Prime Minister, the Hon Malcolm Turnbull MP, announced that we would conduct the 2017 Independent Intelligence Review (the Review). The Prime Minister's full press release can be found at Appendix 1.

The Review's **Terms of Reference** are:

> The 2017 independent review of the Australian Intelligence Community (AIC) will prepare findings and recommendations on the AIC and related issues below in a classified report for the Government, along with an unclassified version of that report.
>
> The review will be completed in the first half of 2017 and will focus on the Office of National Assessments, the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, the Australian Signals Directorate, the Defence Intelligence Organisation and the Australian Geospatial-Intelligence Organisation.
>
> It will also examine the relationship and engagement between those agencies and the members of the broader National Intelligence Community, including the Australian Federal Police, the Department of Immigration and Border Protection, the Australian Criminal Intelligence Commission, and the Australian Transaction Reports and Analysis Centre.
>
> The review will consider, among other things:
>
> - how the key aspects of our security environment and the nature of security threats have changed in recent times, including as a result of technological advancements, and how they are likely to change further over the coming ten years or so
> - how effectively the AIC serves (and is positioned to serve) Australian national interests and the needs of Australian policy makers
> - whether the AIC is structured appropriately, including in ensuring effective co-ordination and contestability
> - whether the AIC is resourced appropriately, including to ensure the right balance of resources across the AIC and that agency resources are properly matched against national security priorities, and the impact of the efficiency dividend
> - whether legislative changes are needed, including to the *Intelligence Services Act 2001*

- whether capability gaps, including technological, are emerging and how these might be met, noting potential efficiencies and that any new proposals would need to be consistent with the Government's overall fiscal strategy
- the effectiveness of current oversight and evaluation arrangements
- the development path of overseas intelligence partners and lessons for Australia

The Department of the Prime Minister and Cabinet will establish a secretariat for the review and provide logistics support to the review as required.

The review team will have full access to all material applicable to its examination. Relevant departments and agencies are to co-operate fully with the review and provide any requested assistance. Ministers will also be asked to meet with and assist the review team.

CONSULTATION

The Review wrote to and met with relevant intelligence agencies, Ministers, members of the Opposition, government departments, and a wide range of people with informed views on intelligence matters generally and Australia's intelligence agencies in particular. The Review also met with the Inspector-General of Intelligence and Security, the Parliamentary Joint Committee on Intelligence and Security, and with Five Eyes intelligence agencies and colleagues in New Zealand, Canada, the United States and United Kingdom.

In addition, the Review called for and received a range of Submissions, including from members of the community.

A list of the people consulted and Submissions received as part of the Review is at Appendix 2.

SUMMARY OF RECOMMENDATIONS

STRUCTURE/ARCHITECTURE

Recommendation 1: An Office of National Intelligence (ONI) be established as a statutory authority within the Prime Minister's portfolio, and that:

a) ONI be led by a Director-General (DG ONI) and this appointment be at departmental Secretary level;

b) DG ONI be the head of the National Intelligence Community (NIC) as well as the Prime Minister's principal adviser on intelligence community issues, with the role including advice on the appointment of senior NIC office-holders and succession planning;

c) DG ONI be a member of the Secretaries Committee on National Security;

d) without directing the specific activities of agencies, DG ONI be able to direct the co-ordination of the NIC to ensure there are appropriately integrated strategies across the suite of NIC capabilities;

e) DG ONI chair an expanded National Intelligence Co-ordination Committee and that its membership include the Chief of the Defence Force or their representative;

f) DG ONI chair a new Intelligence Integration Board;

g) DG ONI's roles and responsibilities be supported by a new legislative mandate which would include the provision of statutory independence for the position of DG ONI; and

h) DG ONI be accountable to the Prime Minister and the National Security Committee of Cabinet for the performance of the NIC generally, and agencies in particular, in relation to National Intelligence Priorities and the provision of relevant input to Ministerial and Cabinet decision-making.

(paragraphs 4.18 to 4.28)

Recommendation 2: The Office of National Intelligence (ONI) encompass two main areas of responsibility led by Deputy Directors-General (at the Senior Executive Service Band 3 level) responsible for Intelligence Enterprise Management (including intelligence integration) and Assessments, and that:

a) the Director-General ONI (DG ONI) be given the authority and

responsibility for advising government on intelligence collection and assessment priorities, and allocating responsibility for intelligence collection across the intelligence agencies;

b) DG ONI report to the Prime Minister and the National Security Committee of Cabinet on a regular basis to provide a holistic view of performance against priorities and to make recommendations on ways of closing intelligence gaps, making choices among relative priorities, and in consultation with the heads of relevant intelligence and policy agencies ensuring the appropriate mix of coverage;

c) DG ONI have responsibility for new arrangements for agency evaluation that are appropriately rigorous across specific mandates, that are similar to the Functional and Efficiency Reviews currently led by the Department of Finance, that are conducted by senior ONI and Department of Finance staff supplemented as appropriate by competent experienced external reviewers, and that make practical assessments of progress in relation to prioritisation, effectiveness, resource allocation, capability development and co-ordination; and

d) DG ONI provide the Prime Minister with a written personal overview every two weeks on key issues for the intelligence agencies, and that this overview be supplemented by meetings with the Prime Minister every two weeks.

(paragraphs 4.29 to 4.38)

Recommendation 3: Integration in areas of high intelligence focus be improved by:

a) establishing a dedicated Office of National Intelligence (ONI) position to facilitate closer co-ordination, evaluation and integration across national counter-terrorism intelligence activities as a whole;

b) the Australian Cyber Security Centre (ACSC) operating as part of the Australian Signals Directorate (ASD), and that:

i) staff from other agencies be seconded to the ACSC but also retain their existing organisational authorities and ability to access data, information and capabilities from their home organisations;

ii) a Head of the ACSC be appointed as the single focus of accountability to the Government for cyber security, and provide a six-monthly report

to Cabinet on proposed cyber security priorities, progress in implementing them and emerging cyber issues;

iii) one Minister have primary responsibility for the ACSC and cyber security under arrangements to be determined by the Prime Minister, noting that the authorities under which ASD would continue to operate would derive from the Minister for Defence (as currently required by section 3A of the *Intelligence Services Act 2001)*;

iv) an Intelligence Co-ordinator for Cyber Security be appointed to more effectively meet and manage the growing expectations of the ACSC, particularly in safeguarding the security of government networks, responding to incidents, and providing the intelligence to support policy and international engagement;

v) governance of the ACSC be provided by the current Cyber Security Board chaired by the Secretary of the Department of the Prime Minister and Cabinet, and in addition to its existing membership the Board also include Director-General ONI and CEO-level representatives of critical national infrastructure sectors including telecommunications, health care, financial institutions, other services, energy, water and ports;

vi) ASD's legislative mandate specify its role as the national information and cyber security authority, including functions to combat cyber crime and to provide advice to the private sector on cyber security matters; and

vii) ACSC's cyber hotline for Government agencies and the private sector operate 24 hours a day, 7 days a week, and a 24/7 capability to manage public messaging and policy advice in relation to rapidly emerging cyber events also be established.

(paragraphs 4.39 to 4.56)

Recommendation 4: The Office of National Intelligence (ONI) be responsible for leading and co-ordinating data management and ICT connectivity initiatives across the National Intelligence Community, and that the Open Source Centre be integrated into ONI's Intelligence Enterprise Management role and enhanced as a centre of expertise for open source collection, analysis, tradecraft and training.

(paragraphs 4.57 to 4.61)

Recommendation 5: Current Office of National Assessments analyst numbers be increased by at least 50 per cent to support the Office of National Intelligence's (ONI) intelligence assessment role, and that:

a) ONI be responsible for preparing a morning Daily Brief for the Prime Minister on intelligence issues of significance;

b) an ONI Assessment Consultation Board be established, chaired by the Director-General ONI and consisting of senior leaders from ONI, other intelligence agencies and relevant policy departments as well as individuals from business, non-government organisations, universities and think-tanks who can add relevant perspectives to intelligence assessment matters; and

c) ONI develop a more intensive and substantive program of interaction with experts outside of government to inform assessments.

(paragraphs 4.62 to 4.69)

Recommendation 6: The Australian Signals Directorate (ASD) be made a statutory authority within the Defence portfolio reporting directly to the Minister for Defence, and that:

a) the Head of ASD be appointed at a level of seniority equivalent to the Directors-General of the Australian Security Intelligence Organisation and the Australian Secret Intelligence Service;

b) the existing organisational arrangements that integrate the support to military operations capability within ASD be reaffirmed and strengthened;

c) a senior military officer be appointed as the principal ASD Deputy Director at a rank commensurate with the responsibilities and accountabilities of the role; and

d) a dedicated joint ASD–Defence team be established to manage ASD's transition to a statutory authority, drawing on relevant expertise within and outside of government, and reporting to the National Security Committee of Cabinet.

(paragraphs 4.70 to 4.80)

CAPABILITY AND FUNDING

Recommendation 7: A Joint Capability Fund administered by the Office of National Intelligence be established to support the development of shared capabilities, with the total amount in the Fund being equivalent to the Efficiency Dividend levied on the intelligence agencies.

(paragraphs 5.29 to 5.42)

Recommendation 8: Changes be made to the application of the Efficiency Dividend to the intelligence agencies as follows:

a) the Efficiency Dividend be applied to 100 per cent of Australian Signals Directorate (ASD) funding with effect two years after ASD's establishment as a statutory authority; and

b) the Efficiency Dividend be applied to 100 per cent of the funding of the Office of National Intelligence (ONI) with effect two years after ONI's establishment as a statutory authority.

(paragraphs 5.38 to 5.39)

Recommendation 9: An Intelligence Capability Investment Plan (ICIP) be established that identifies the major capability projects that agencies seek agreement to commence over the period of the Forward Estimates, and that the Director-General of the Office of National Intelligence prepare the ICIP annually for consideration by the National Security Committee of Cabinet, noting that:

a) The ICIP should also be presented in conjunction with a comprehensive overview of the National Intelligence Community's (NIC) existing funding and commitments.

b) The ICIP should include the projects which the Australian Signals Directorate (ASD) has in Defence's Integrated Investment Program (DIIP), and that the associated funding be transferred from the Defence budget to ASD after it transitions to a statutory authority. The current phases of ASD's DIIP funding should continue to be administered by the Department of Defence, and over time, later phases of existing projects, as well as their replacements and future projects, should move into the ICIP.

c) The ICIP, in its first iteration, be presented to government with options for overall funding envelopes based on NIC funding and indexed at 1.5 and 3 per cent real growth per year, with effect from 2018–19.

(paragraphs 5.43 to 5.54)

Recommendation 10: Proposals for new funding for important long-term intelligence capability initiatives be assessed against agreed principles, including:

a) additional funding should be focused primarily on Australia's own intelligence needs;

b) the likely return on investment should be specified; and

c) funding should be phased over time and subject to periodic review against objectives.

(paragraphs 5.26 to 5.27)

Recommendation 11: The Office of National Intelligence be responsible for developing and overseeing the implementation of a strategic approach to the development of the National Intelligence Community workforce as part of its intelligence enterprise management responsibilities.

(paragraphs 5.5 to 5.12)

Recommendation 12: The Australian Security Intelligence Organisation receive additional resourcing to allow it to second staff to the Australian Government Security Vetting Agency (AGSVA) as soon as possible, and that the situation with AGSVA Top Secret (Positive Vetting) clearances be reviewed in early 2018 to allow time for the current remediation program to have effect. If processing times still exceed six months, alternative options for Top Secret (Positive Vetting) clearances should be explored.

(paragraphs 5.13 to 5.14)

Recommendation 13: Data analytics and ICT connectivity, including the establishment of an intelligence community computing environment in which technical barriers to collaboration are minimised, be one of the highest priorities of a more structured approach to technological change and for the funding of joint capabilities.

(paragraphs 5.15 to 5.19)

Recommendation 14: The Office of National Intelligence lead a more structured approach to the National Intelligence Community's responses to technological change, with a high priority given to:

a) establishing a National Intelligence Community Science and Technology Advisory Board;

b) creating a National Intelligence Community Innovation Fund to support the development of prototypes for transitioning research outcomes into operational systems; and

c) supporting a National Intelligence Community Innovation Hub to facilitate ways in which government, industry and academia could come together to address capability needs and solutions and create new linkages.

(paragraphs 5.20 to 5.25)

LEGISLATION

Recommendation 15: A comprehensive review of the Acts governing Australia's intelligence community be undertaken to ensure agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians. This review should be carried out by an eminent and suitably qualified individual or number of individuals, supported by a small team of security and intelligence law experts with operational knowledge of the workings of the intelligence community.

(paragraphs 6.7 to 6.19)

Recommendation 16: Amendments to the Ministerial authorisation (MA) regime in the *Intelligence Services Act 2001* (ISA) and associated processes be made to address practical difficulties arising from implementation of the regime. Such amendments, to be pursued in advance of the comprehensive review recommended above, would include:

a) Introducing a class-based MA regime to enable ISA agencies to produce intelligence on a class of Australian persons involved with proscribed terrorist organisations. The class authorisation should be issued by the responsible Minister with the agreement of the Attorney-General and overseen by the Inspector-General of Intelligence and Security (IGIS). Class authorisations should last for a maximum period of six months but could be renewed. ISA agencies should maintain a current list of the Australians on whom they are seeking to produce intelligence on under the authorisation, outlining the justification for their continued coverage. Agencies should have to report to the responsible Minister within six months of the original authorisation.

b) Introducing a class-based MA regime to enable ISA agencies to undertake activities to produce intelligence on Australian persons when the agencies are operating in support of the Australian Defence Force (ADF). This regime would be subject to the same oversight requirements

as recommended above in relation to class authorisations for Australian persons involved with proscribed terrorist organisations.

c) Introducing a requirement for all ISA agencies to seek an MA for activities likely to have a direct effect on an Australian person.

d) Requiring ISA agencies to obtain MAs only for activities involving the use of covert collection capabilities by including a definition of 'producing intelligence' in the ISA. For the Australian Secret Intelligence Service, Ministerial authorisation should continue to be required for tasking an agent or network of agents to produce intelligence on an Australian person or class of Australian person overseas, or when requesting an international partner to do likewise. We also recommend amending the definition of 'intelligence information' in the ISA.

e) Permitting an ISA agency to act immediately and without an MA in situations where it is reasonable to believe that an Australian person consents to the ISA agency producing intelligence on that person. In these circumstances, the ISA agency should be required to notify the responsible Minister and the IGIS as soon as possible and at a maximum, within 48 hours. In situations involving a threat to security, the Minister responsible for the Australian Security Intelligence Organisation (ASIO) should also be advised.

f) Providing that when an MA involves a threat to security, the Minister responsible for the ISA agency first consider the case prepared by their own agency in consultation with ASIO. If the Minister agrees with the arguments presented by the ISA agency, the Minister should then consult with and obtain the agreement of the Attorney-General before issuing the authorisation.

(paragraphs 6.30 to 6.51)

Recommendation 17: Regular briefings be held involving the 'Agency Heads' (as defined by the *Intelligence Services Act 2001*), their responsible Ministers, and the Attorney-General and Director-General of Security, on intelligence collection activities overseas which, if compromised, could impact on Australia's foreign policy or international relations.

(paragraphs 6.52 to 6.53)

Recommendation 18: The co-operation provisions in Divisions 2 and 3 of Part 3 of the *Intelligence Services Act 2001* (ISA) be streamlined to enhance co-operation amongst agencies. These changes, also to be pursued in advance of the comprehensive review recommended above, would include:

a) clarifying that two ISA agencies co-operating with one another can act jointly under a single Ministerial authorisation from the relevant Ministers; and

b) extending the co-operation regime for activities undertaken in relation to the Australian Security Intelligence Organisation to all ISA agencies and to activities undertaken both within and outside Australia.

(paragraphs 6.54 to 6.62)

Recommendation 19: The Director-General of the Australian Secret Intelligence Service (ASIS) be able to authorise activities under Schedule 2 of the *Intelligence Services Act 2001* concerning the use of weapons and self-defence techniques by ASIS staff members and persons co-operating with ASIS. In addition to the existing requirement in relation to notifying the Inspector-General of Intelligence and Security, the Director-General should also be required to notify the Minister responsible for ASIS of any new authorisations or changes to existing authorisations on a monthly basis.

(paragraphs 6.63 to 6.67)

Recommendation 20: Existing consultation arrangements for the development of legislative reform proposals be strengthened to ensure legislative amendments are coherent and progressed in a timely manner.

(paragraphs 6.68 to 6.74)

OVERSIGHT

Recommendation 21: The oversight role of the Parliamentary Joint Committee on Intelligence and Security and the Inspector-General of Intelligence and Security be expanded to apply to all ten agencies within the National Intelligence Community, with oversight of the Australian Federal Police, the Department of Immigration and Border Protection, and the Australian Criminal Intelligence Commission limited to their intelligence functions, and with current oversight arrangements in relation to the Office of National Assessments applied to the Office of National Intelligence.

(paragraphs 7.19 to 7.22)

Recommendation 22: The Office of the Inspector-General of Intelligence and Security be allocated additional resources to enable it to sustain a full-time staff of around 50.

(paragraphs 7.23 to 7.27)

Recommendation 23: The role of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) be expanded by amending relevant legislation to include:

a) a provision enabling the PJCIS to request the Inspector-General of Intelligence and Security (IGIS) conduct an inquiry into the legality and propriety of particular operational activities of the National Intelligence Community (NIC) agencies, and to provide a report to the PJCIS, Prime Minister and the responsible Minister;

b) a provision enabling the PJCIS to review proposed reforms to counter-terrorism and national security legislation, and to review all such expiring legislation;

c) provisions allowing the PJCIS to initiate its own inquiries into the administration and expenditure of the ten intelligence agencies of the NIC as well as proposed or existing provisions in counter-terrorism and national security law, and to review all such expiring legislation;

d) provisions enabling the PJCIS to request a briefing from the Independent National Security Legislation Monitor (the Monitor), to ask the Monitor to provide the PJCIS with a report on matters referred by the PJCIS, and for the Monitor to provide the PJCIS with the outcome of the Monitor's inquiries into existing legislation at the same time as the Monitor provides such reports to the responsible Minister; and

e) a requirement for the PJCIS to be regularly briefed by the Director-General of the Office of National Intelligence, and separately by the IGIS.

(paragraphs 7.28 to 7.47)

CHAPTER 1: AUSTRALIA'S NATIONAL SECURITY ENVIRONMENT

1.1 This Chapter addresses the first of the Review's Terms of Reference on "*how the key aspects of our security environment and the nature of security threats have changed in recent times, including as a result of technological advancements, and how they are likely to change further over the coming ten years or so.*"

THE STRATEGIC ENVIRONMENT

1.2 The current international environment is one in which powerful forces of change are re-shaping concepts of security, recalibrating interactions among states and people as well as between individual states and their citizens, and enhancing the asymmetrical capabilities of non-state actors. These forces of international change are framing our foreign policy and national security interests. They are also reverberating domestically in Australia – creating new challenges for Australia in pursuit of our global and regional interests, influencing perceptions of the role of our intelligence agencies and creating new requirements for more effective co-operation between the Australian public and private sectors on national security issues.

1.3 This pace of change has made the context in which Australia protects and advances its security interests more complex, less predictable and more volatile than in the past. In our view, that pace of change is set to intensify with the major influences on Australia's national security outlook over the coming decade coalescing around three key focal points: fundamental changes in the international system, extremism with global reach and the security and societal consequences of accelerating technological change.

Fundamental Changes in the International System

1.4 The international environment is characterised by transforming economic, political, security, technological and societal change. The trend in the global balance of wealth and power is favouring China and India. The Western ascendancy in international institutions and values that characterised the second half of the twentieth century, and the early years of the twenty-first century, is eroding. The geopolitical consequences of economic globalisation are creating new centres of power and encouraging new strategic ambitions among many

states. There are increasing complexities, particularly in the Indo-Pacific region, generated by enhanced economic interdependence and rising geopolitical rivalry. The global strategic influence of the United States has declined in relative terms and that trajectory is set to continue. The rise of China and India continues. Russia seeks to reassert its influence. Japan's international role is evolving and growing. And, over the longer term, the influence of emerging regional powers, including potentially Indonesia, is set to grow.

1.5 These profound changes in the distribution of wealth and power have far-reaching implications, not only internationally but also domestically. They are challenging aspects of Australia's comparative advantages, increasing the interest that foreign intelligence agencies are showing in Australia, reinforcing the need to guard against the potential for foreign interference in Australia's commercial practices, political institutions and democratic processes, and generating foreign investment proposals that can raise sensitive issues for government.

1.6 In addition to these trends, technological disruption (particularly in information technology) as well as slow and uneven economic growth within and among states and regions are contributing to enhanced nationalism, populism and economic parochialism in many countries. This is exacerbating a growing sense of insecurity and alienation. Technology is changing the way in which economies work and societies evolve, making the intersection of economics, politics and security more difficult to manage. Economic development challenges, demographic trends, climate change pressures, resource security concerns (particularly in relation to food, water and energy), irregular people movements, and intrastate and regional conflicts are also contributing to heightened tensions and instabilities that are affecting nations' perceptions of their security.

1.7 In this environment, power politics remains important in the rivalry and competition among states, and there are signs that it will become more accentuated over coming years. Espionage and counter-espionage have always been realities in the power politics of the modern international system. That remains the case and it will intensify and evolve in unpredictable ways. Furthermore, ideological rivalry is re-emerging and instability in key theatres is increasing. The use and especially the threat of force is evolving as more states develop and utilise overt, covert and proxy capabilities to pursue their strategic objectives, and as access to advanced destructive capabilities increases and diversifies.

1.8 The international security environment is also being changed by the asymmetrical influence and capacities of non-state actors – whether they be agents of terrorism, international crime or malicious cyber activity. This growth of destabilising and violent non-state capabilities is often being facilitated by failed, failing and rogue states. In turn, that is resulting in military interventions to stabilise situations and deny sanctuary to extremists.

1.9 Australia's national security outlook over the coming decade will be affected by all these developments. In particular, its contours will be shaped by new dimensions of rivalry and ambition among states, by the destabilising role of non-state actors as well as by changes in international institutions and the shifting balance of power and influence within them. Moreover, assumptions that have long underpinned Australia's security and foreign policy, including those in relation to the strength of the rules-based component of the global order, will be more uncertain.

1.10 In this environment, Australia's ability to protect and advance its security interests will depend critically on how well it understands the complex forces of change that are evolving. It will also depend on how effectively it addresses the challenges and utilises the opportunities they present. Australia's intelligence agencies have a vitally important role to play in achieving these outcomes.

Extremism with Global Reach

1.11 Australia's national security circumstances have been re-shaped by the realities of extremism with global reach.

1.12 Economic globalisation over recent decades has dramatically accelerated the international movement of people, goods, money and ideas. This phenomenon has had a remarkably positive and empowering impact on states and individuals. It has been vital in bringing more people out of poverty more quickly than at any other time in history. This greater freedom of international movement and sense of global connectedness has been enabled through communications, financial and physical networks. But these transforming influences have also had a negative impact through their facilitation of the illegal and destabilising transfer of goods, money, weapons and people. This has broadened the potential for extremism, sectarian fundamentalism, radicalisation and terrorism to take root and have their destructive impact. It has also raised expectations, especially among Australians living and working abroad, that their government will protect them from such dangers or support them if those dangers directly affect them.

1.13 Extremism with global reach has important consequences for Australian society. It accentuates the urgency and constancy of the need to counter terrorist influences and ambitions in Australia.

1.14 In our view, extremism with global reach will continue and diversify over the coming decade. Fundamentalist advocacy of violence in the name of religion will continue to inspire attacks, especially from Islamist terrorist organisations. Radicalisation and terrorist acts will continue to be enabled by increasingly internationalised networks and encrypted communications. The prominence and power of individual groups such as the Islamic State of Iraq and the Levant (ISIL) may wane but many of the forces of deep alienation, ruthless hostility and ideologies of violence that have brought these groups to prominence will remain. Individuals inspired by ISIL will outlive any demise of the organisation. Al-Qaida and its affiliates will remain a threat. Those groups and other splinter organisations that may emerge will aim to give effect to ambitions for mass casualty attacks and random violence. Such groups will continue to draw on local grievances to support their regional and global agendas.

1.15 These realities of Australia's national security environment will continue as a vital focus for the work of the intelligence agencies over the coming decade and beyond. Particular challenges will emerge and others will evolve. These will include the activities and networks of Australian 'foreign fighters' involved in international extremist and terrorist causes, the rise of 'lone wolf' assaults and the scope for low-technology terrorism attacks often facilitated online. The time taken between radicalisation and terrorist attack is shortening, further challenging intelligence agencies' detection and response capabilities.

1.16 In our view, the terrorist and extremist threats to Australia and Australian interests will continue to grow in scale and complexity. Detecting and countering such threats will be increasingly challenging for our intelligence and law enforcement agencies. The greater numbers of Australians travelling and living overseas, as well as the international movement of radicalised individuals, will magnify the security threats Australia faces.

The Security Consequences of Accelerating Technological Change

1.17 The economic, security and societal changes we are witnessing in the international system, including the emergence of extremism with global reach, are enabled to a large extent by the accelerating pace of disruptive innovation across a wide range of technologies.

1.18 One of the most worrying aspects of technological change is the way it is helping to place enormously destructive capabilities within easier reach of rogue states and non-state actors. This trend is not reversible and it will lead to an even more threatening international environment than now exists. The threat is most immediately manifest in North Korea which is making steady progress towards a capability that could put an increasing number of countries, including the United States mainland and Australian territory, within reach of its missiles. This emboldens North Korea to believe it can act aggressively towards regional countries in the hope of coercing them. In addition, extremist groups will have access to the type of destructive capabilities that were previously the preserve of nation states with an advanced scientific and industrial base. Intelligence will have a unique and crucial role to play in relation to these issues. Governments will rightly want insights, assessments and operational detail to inform responses.

1.19 The proliferation of weapon systems, including those with indiscriminate mass-destructive impact, is being facilitated by technological advances. Improvements in 3D printing, biotechnology and other dual-use technologies make it easier to manufacture weapons of high lethality from raw materials that are less amenable to international trade restrictions.

1.20 Advances in technology are also enhancing the accuracy and lethality of precision weapons with direct implications for the conduct of warfare and for the importance of the support for military operations that needs to be provided by intelligence agencies. The proliferation of precision weapons will see more nations with the capability, and the temptation, to undertake 'surgical' strikes.

1.21 Advances in communication technologies will continue to add to international volatility, complicating the task of intelligence agencies trying to anticipate and track developments. The use of social media to help mobilise mass protests or invoke international intervention is now a well-learned tactic of those seeking to challenge the established order. The ability to move money at speed and in large quantities will also remain a potential source of instability in the international system, and enable extremists to help affiliates build capability and conduct operations. The use of the internet to proselytise extremist ideology and groom potential attackers will continue to help extremists achieve global reach.

1.22 More generally, the cyber domain will likely feature even more prominently than it currently does in attempts to undermine economies, societies and national governments. It offers a relatively inexpensive but potentially effective way of achieving a wide range of effects – from influencing political processes to disrupting financial systems and key aspects of national infrastructure. And it can enable espionage to be conducted at scale and speed, and with a high degree of deniability if done professionally. Countries, non-state actors and international criminal networks will continue to test the possibilities in cyber, resulting in a new array of national security challenges. This acceleration of cyber technologies creates opportunities as well as challenges for Australia's intelligence agencies.

1.23 New technologies are also transforming the security dimensions of space-based activities. Access to space and to space-derived information is becoming increasingly commercialised and is declining significantly in cost, making many intelligence, surveillance and reconnaissance capabilities more attainable for a greater number of countries and non-state actors. Again, this represents both a challenge and an opportunity for Australia.

1.24 The rise of big data and associated advanced analytic techniques are transforming the way private and public sector organisations operate. Big data has also increased the risks and consequences of security breaches. The unauthorised disclosures of Wikileaks and Edward Snowden, in particular, over recent years have compromised capabilities, endangered the lives of individuals and inhibited co-operation with commercial organisations.

CONCLUSION

1.25 Australia's security environment and the nature of the security threats Australia faces are a product of changes in the balance of wealth and power in the international system, new dimensions of the interaction between economic globalisation and geopolitical power politics (particularly in our own region), the asymmetrical influence of non-state actors, including extremists, and the implications of technological advances for Australian, regional and global security. These changing contours of the international security outlook have created new demands on intelligence processes as well as new expectations of them on the part of national governments and communities. For Australia's intelligence agencies, in particular, the forces of strategic change are broadening their responsibilities, diversifying

their operational priorities and creating new requirements for a more integrated focus. In the next Chapter, we focus on these and other consequences for intelligence processes resulting from Australia's changing national security outlook.

[This page intentionally left blank]

CHAPTER 2: IMPLICATIONS OF THE NATIONAL SECURITY OUTLOOK FOR AUSTRALIA'S INTELLIGENCE AGENCIES

2.1 This Chapter assesses the consequences of Australia's changing national security outlook in terms of the challenges and opportunities facing Australia's intelligence agencies.

THE ONGOING RELEVANCE OF INTELLIGENCE AND ITS LIMITATIONS

2.2 The value-adding potential of intelligence processes and products to government decision-making has sometimes been questioned, particularly by those who are concerned by its lack of transparency or sceptical of its worth. Such critiques are likely to continue, particularly in circumstances in which information is more publicly accessible, secrets are harder to keep and issues of accountability of intelligence agencies are often prominent.

2.3 Our view is that, in a context of rapid and systemic international change, the input of high-quality intelligence to particular government decision-making processes and to support the Australian Defence Force (ADF) will remain indispensable. Furthermore, the factors shaping Australia's national security environment over the coming decade and beyond are reinforcing and further diversifying the role of Australia's intelligence agencies. The rising potential for destabilising actions by states and non-state actors is putting a premium on current and strategic intelligence of the highest order to assist Australian decision makers in the choices they make.

2.4 It is also increasing the focus that Australia's intelligence agencies need to bring to the consequences of such international instability for domestic security within Australia, including effective counter-espionage strategies. In addition, the spread of increasingly lethal armed capabilities to more states and non-state actors is broadening the range of operations in which the ADF may be involved, and the contingencies for which it needs to plan, thereby accentuating the importance of the support to military operations and planning that Australia's intelligence agencies need to provide.

2.5 Secret intelligence is needed to combat secretive adversaries.[1] Australia and like-minded countries increasingly confront critical issues of security consequence that are opaque. Access to others' secrets is therefore needed to safeguard legitimate strategic interests. Those issues of opaque security consequence include the assertive ambitions and offensive capabilities of other states, the disruptive potential of non-state actors (particularly terrorists) and the destabilising applications of new technologies. Intelligence can provide hard evidence about the often harsh realities of how the world works, how states and other actors pursue their goals, and what those goals are.

2.6 Judicious and timely decision-making will continue to require the contextual awareness, the information about others' capabilities and intentions, and the insights into immediate and potential threats to the security of the state and its citizens that good intelligence can provide. Australia's intelligence agencies will therefore continue to have a vital role in supporting decision-making by identifying trends and patterns as well as discontinuities, providing early warning, highlighting risks and opportunities, identifying and on occasions disrupting threats to national interests, assisting law enforcement and supporting military operations. This role is complemented by timely and insightful diplomatic reporting.

2.7 In the context of the economic, security, technological and societal change that is transforming relations among states and people in unpredictable ways, an effective Australian intelligence capability is a vital ongoing national asset and an indispensable source of comparative advantage, now and into the future. But the limitations of intelligence also need to be clearly recognised.

2.8 Secret intelligence has no special status simply because it is acquired by secret means. Moreover, because it often deals with reasonable probabilities and not absolute certainties, intelligence rarely provides clear-cut guarantees about the future. Nor is it appropriate for intelligence agencies to recommend policy directions to government. Through its 'opportunity analysis', however, intelligence can clarify for government the net costs and advantages among a range of potential policy approaches. The primary purpose of intelligence remains to provide value-adding contextual insights and actionable information, thereby reducing the uncertainty in which government decisions are ultimately made and, where appropriate, contributing to the

1 See Sir Roderic Braithwaite, '*Defending British Spies: The Uses and Abuses of Intelligence*', Address to the Royal Institute of International Affairs, Chatham House, 5 December 2003.

implementation of those decisions. In fulfilling that purpose, intelligence often illuminates the foundations on which good policy can be built.

2.9 The challenges facing Australia's intelligence agencies, and the expectations of them, can pull in opposite directions. The scope for intelligence targets to become more opaque and unyielding (through deception, denial, encryption and other means) is increasing. The complexities involved in sifting and connecting exponentially increasing amounts of data have become more formidable. The pace of technological change is creating mounting pressures on the budgets and specialist skills base of intelligence agencies. The investments required in intelligence capabilities are growing dramatically, and returns on those investments in terms of value-adding intelligence that advances Australian national interests to the extent envisaged cannot be guaranteed.

2.10 At the same time, in an information-rich world, the expectations of Ministers and other intelligence users in government have also increased in terms of what intelligence agencies can, and should, provide to inform decision-making. This is despite the fact that, although some of the issues that intelligence agencies address are 'puzzles' (to which answers exist), others are 'mysteries' (on which, at best, insights are more relevant than answers).[2] Mostly, the role of intelligence is not to predict the future but to explain the forces at work in particular situations and thus to help government influence developments.

2.11 These and other limitations are inherent in the nature of intelligence. They need to be acknowledged within the wider context of the ongoing relevance, and sometimes the unique value, of the intelligence input to government decision-making.

Australia's Changing National Security Environment and the Operational Context for Australia's Intelligence Agencies

2.12 The changes in Australia's current and evolving national security environment have had, and will continue to have, important consequences for the work of Australia's intelligence agencies. At one level, they have been a catalyst in deepening and broadening the scope of the activities undertaken by the intelligence agencies in fundamentally important ways. Australian agencies are now focused on protecting and advancing Australian national interests through identifying and countering threats that are intensifying and diversifying,

2 See Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information,* Cambridge University Press, 2003, pp.11–13.

and through identifying and exploiting opportunities that are emerging to advance those interests. They do so through modern means of collecting and assessing intelligence material, advising government and the wider community appropriately, and assisting in the implementation of government national security policies when authorised to do so.

2.13 The changing nature of Australia's national security environment has broadened the range of activities of Australia's intelligence agencies. Those activities include the modern parameters of human intelligence, signals intelligence as well as geospatial intelligence. They are focused on the motives and capabilities of states but also those of destabilising non-state actors. They encompass support for the planning and conduct of military operations, including information on the weapons systems and defence technologies of potential adversaries or of those countries developing, manufacturing and exporting such capabilities. They include illuminating and countering espionage and foreign interference against Australia.

2.14 The work of Australia's intelligence agencies also relates to support for law enforcement actions and prosecutions, and for border security operations. It covers foreign investment, financial intelligence (including evasion of sanctions, countering money-laundering and terrorism-financing) as well as intelligence on current and emerging crime threats and criminal justice issues. It also covers a range of other responsibilities, including personnel security assessments, visa security checks and protective security advice.

2.15 At another level, Australia's changing national security circumstances and outlook have also provided a new context for the legacy of the landmark Royal Commissions into the Australian intelligence and security agencies conducted by Mr Justice Hope in 1974–77 and 1983–84.

2.16 The Hope Royal Commissions were the most formative and enduring influences in the history of the Australian Intelligence Community (AIC).[3] They highlighted a core challenge for any democratic society of managing, in changing circumstances of security risk, the balance between the right of a community to public safety backed by coercive powers of the state, and the right of individuals in that community to their freedom and privacy. The Hope Royal Commissions defined the roles and responsibilities of the intelligence agencies directly in the context of Australia's national interests, the requirements of the government of the

3 The AIC currently consists of the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Office of National Assessments, the Defence Intelligence Organisation, the Australian Signals Directorate, and the Australian Geospatial-Intelligence Organisation.

day and the rights of individual Australians. They established the principle of proportionality in relation to the actions of agencies. They specified clear lines of responsibility for Ministers as well as new and appropriately high benchmarks for propriety, accountability under law and oversight of the activities of Australia's intelligence agencies. Furthermore, they established the centrality of clearly identified national intelligence priorities and the critical role of effective co-ordination in pursuing them.

2.17 The Hope Royal Commissions also established operational principles that shaped the evolution of Australia's intelligence agencies over succeeding decades. Those principles were based on what Mr Justice Hope saw as vital distinctions between foreign and security intelligence, between intelligence collection and assessment, between human intelligence and signals intelligence, between intelligence assessments and policy determination, and between security intelligence and law enforcement.

2.18 Many of the broad responsibilities, accountabilities and operational principles of the AIC continue to reflect the outcomes of the Hope Royal Commissions. The result has been that the effectiveness and standing of the intelligence agencies have been greatly strengthened. In our view, it is important that this influence continues. It is also important that the indispensable legacy of the Hope Royal Commissions be refreshed to reflect the contemporary Australian national security outlook and a structural and operational environment for Australia's intelligence agencies that differs in important respects to that which prevailed at the time of the Royal Commissions, and that are also different in some aspects to the context in which more recent reviews of the AIC were conducted.[4]

2.19 Current structural arrangements in relation to Australia's intelligence agencies are different in some respects to those that existed at the time of the Hope Royal Commissions. There are new agencies such as the Australian Transaction Reports and Analysis Centre. And there are other agencies such as the Australian Geospatial-Intelligence Organisation, the Australian Criminal Intelligence Commission, the Australian Federal Police and the Department of Immigration and Border Protection which have evolved from earlier organisations and/or in which the range of intelligence functions has significantly expanded.

4 For example, Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies,* 2004; and Robert Cornall and Rufus Black, *Independent Review of the Intelligence Community,* 2011.

2.20 The more influential force of change since the time of the Hope Royal Commissions has been the nature of Australia's national security environment which we outlined in Chapter 1. Together with societal change, this has re-shaped the operating environment for Australia's intelligence agencies in important ways.

Foreign and Security Intelligence

2.21 Some of the old lines of demarcation between foreign and security intelligence have become more porous. Economic globalisation, applications of new technologies and the rising influence of non-state actors have been important influences in that process. With more extensive and direct involvement of some Australians in international terrorist and extremist causes, and with greater scope for external covert interference in Australia generally, domestic and foreign sources of security threat have become less mutually exclusive. Security threats to Australians, in Australia and overseas, have increased and diversified as a result.

2.22 This blurring of some of the demarcations between foreign and security intelligence needs to be seen in perspective. Foreign and security intelligence continue to retain important distinguishing characteristics in terms of their operational context as well as Ministerial and legal accountability. We do not, therefore, see any logic or net advantage in a merging of responsibilities for foreign and security intelligence, for example in bringing the Australian Security Intelligence Organisation (ASIO) and the Australian Secret Intelligence Service together in a single organisation. Furthermore, the traditional distinction between foreign and security intelligence underpinned an emphasis on the special rights to privacy and civil liberties of Australian persons in the Hope Royal Commissions. That underpinning continues to be important and the privileging of Australian persons in the mandates of particular Australian intelligence agencies and in Australian law remains strong.

2.23 For all these elements of continuity, there are also forces of change at work. In particular, we consider that the changing nature of the interaction between foreign and security intelligence created by globalising influences, technological change and the destabilising capabilities of non-state actors calls for new synergies among intelligence agencies, more effective co-ordination of their priorities and purposes, and streamlining of some of the arrangements that currently shape their operations. These trends in foreign and security intelligence have resulted in changes in the way the agencies of Five Eyes partners operate,

particularly those of the United States and the United Kingdom. But in Australia progress has been more limited.

Operational and Strategic Intelligence

2.24 Priorities such as support for military operations, enhancing cyber security, and countering terrorism, people-smuggling and weapons proliferation have increasingly put a premium on actionable intelligence. The balance between actionable and strategic intelligence has changed in the context of Australia's contemporary national security circumstances (particularly in relation to the impacts of extremism with global reach). For all this enhanced profile of actionable intelligence, strategic intelligence assessments, whether they be focused on short or longer-term perspectives, continue to retain their relevance in decision-making processes. Identifying changing patterns of co-operation and competition among states as well as current and emerging practical manifestations of each are critical assets in policy development. Australia's intelligence agencies have a vital and continuing role to play in that context.

2.25 The shifting balance between actionable and strategic intelligence has affected some of the traditional dividing lines between the roles of intelligence collectors and assessors. Collectors increasingly need their own analytical filters for processing and evaluating a proliferating range of actionable intelligence data, for connecting intelligence derived in different ways across different parts of the world, and for presenting collected intelligence product intelligibly to Ministers and policy agencies. Furthermore, assessment agencies are increasingly broadening their own collection of open source material. So the old labels of 'collectors' and 'assessors' are no longer as useful or as meaningful as they once were.

An Evolving Relationship Between Intelligence and Law Enforcement

2.26 The Reports of the Hope Royal Commissions articulated a clear view that the responsibilities of the intelligence agencies were different from those of law enforcement bodies, and should be kept distinct. There is an important sense in which that distinction continues to apply. We agree with the view expressed in ASIO's 2015–16 Annual Report to Parliament:

> "ASIO's role as the national security intelligence service is anticipatory and protective in nature: it is expected to identify and

act against threats before harm has occurred. This is a key difference between ASIO's work and that of law enforcement partners..."[5]

2.27 And yet, for all the continuing relevance of this distinction, our view is that the changing nature of the security threats facing Australia and the opportunities opened up by new technologies, particularly in relation to data analytics, mean that these points of interaction between Australia's intelligence agencies and law enforcement authorities are becoming more intensive. The points of interaction relate to co-operation not only among Commonwealth entities but also among relevant State and Territory bodies. They need to be managed in ways that respect the information sharing arrangements, the accountability and the obligations under law of each entity, including arrangements for managing intelligence-derived information in the conduct of legal proceedings. What is clear, however, is that many of the traditional distinctions between intelligence and law enforcement in the Australian context are less comprehensive and definitive than in the past, and that this trend towards more intensive interaction will continue.

Intelligence Assessments and Policy Priorities

2.28 The need for intelligence assessments to be independent of policy-making has been, and remains, an indispensable requirement. It was one of the key operational principles at the core of the recommendations of the Hope Royal Commissions as well as those of subsequent inquiries into Australia's intelligence agencies. It has been a principle strongly upheld in practice by those agencies themselves. And it is a principle which this Review strongly reinforces.

2.29 Unless intelligence assessments are unambiguously independent, and seen as such, their currency is demeaned and their influence is diminished. In this context, it is vital that intelligence assessments not only 'speak truth to power' when the intelligence evidence exists but also that they indicate when definitive judgments are not possible because the intelligence evidence (derived from either open or covert sources or both) is incomplete, contradictory, unreliable or inconsistent.

2.30 If the content of intelligence assessments is influenced by pre-ordained policy priorities and preferences, those assessments lose their credibility. On the other hand, if intelligence assessments are seen as disconnected from the difficult but necessary choices involved in policy-making, or from the timing of major policy decisions and direction-setting, those assessments become increasingly irrelevant.

5 ASIO Annual Report, 2015-16, p.10.

2.31 The independence of intelligence assessments from the pressures of policy priorities does not mean that they should be unrelated to the policy cycle. Intelligence products and processes should not operate in 'splendid isolation' from policy priorities. Intelligence assessments need to make judgments strictly on the balance of the evidence but their input to policy determination processes needs to be timely and relevant. Policy decision-making and intelligence assessments need to be connected, even when policy preferences and intelligence assessments do not coincide.

2.32 In our view, the independent character of intelligence assessment remains indispensable. But we also consider that intelligence assessments and the requirements of policy-making processes are closely connected. Independent intelligence assessments need to draw out from their analysis the implications for Australian policy interests. We assess that the importance of this connection between high-quality intelligence assessments and policy-making needs to be further accentuated.

New Technologies and the Frontiers of Data-Rich Intelligence

2.33 Advances in technology will continue to challenge important aspects of the way countries have traditionally conducted intelligence operations. The rapid spread of strong encryption presents a formidable challenge. It is already requiring new approaches to be adopted and will demand extensive and close collaboration among agencies to achieve the type of access that government will need from Australia's intelligence agencies.

2.34 Similarly, advances in surveillance technology and its increasingly widespread use in urban environments will increase the difficulty of conducting clandestine human intelligence operations overseas. This will be compounded by enhanced capabilities for establishing the true identity of individuals with a high degree of reliability. These realities create an increasingly formidable operational environment for intelligence agencies.

2.35 The amount of publicly available multimedia information facilitated by the internet of things, enhanced artificial intelligence, the expansion of computational power and new tools for exploiting open source information is transforming public and private sector enterprises. Intelligence agencies are no exception. They will require increasingly automated capacities to filter, translate, verify, summarise, correlate and contextualise greatly increased volumes of data. One consequence is that the demand for data analytical expertise in both the public and

private sectors will continue to grow. Another is that the realities of big data heightens risks – for governments, for the private sector and for the community generally, particularly in relation to the functioning of national infrastructure and the provision of services. The fact that advances in technology enable large amounts of information to be moved quickly and discreetly also magnifies the consequences of security breaches, especially from disaffected individuals inside the intelligence community.

2.36 In our view, the challenge of protecting the integrity, confidentiality and availability of systems and data will only become more important and more complex. Defensive and proactive technical security measures will increasingly be at the core of strategies to secure systems and data. Whether it is in relation to data analytics, encryption, decryption, data protection generally or the use of cyberspace, collaboration and co-operation between Australia's intelligence agencies and the private sector will become increasingly necessary and relevant, not least because in important specific areas private sector ICT innovation and technology application are more advanced.

CONCLUSION

2.37 Australia's evolving national security environment is fundamentally changing the way in which Australia's intelligence agencies need to operate. It is creating new imperatives for more effective integration and synergies among agencies. And it is requiring new benchmarks of agency capabilities in relation to physical security, personnel vetting, data analytics, multi-disciplinary operations, information and communications technology infrastructure, intelligence management tools for producing and disseminating intelligence product, innovation culture, effective partnerships as well as training, development and career management. This context frames our consideration in Chapter 3 of how well Australia's intelligence agencies are positioned to meet the challenges that confront them, and our recommendations for change.

CHAPTER 3: THE PERFORMANCE OF THE AUSTRALIAN INTELLIGENCE COMMUNITY (AIC)

3.1 This Chapter addresses the Review's second Term of Reference which focuses on "*how effectively the AIC serves (and is positioned to serve) Australian national interests and the needs of Australian policy makers.*"

3.2 In our assessment, Australia's intelligence agencies have effectively met many of the challenges presented by our national security circumstances. On particular issues, they have co-operated intensively and productively. They have a strong record of achievement in protecting the security of Australians and in advancing important Australian interests. In our view, however, Australia's intelligence agencies are facing a range of challenges as a result of the broadening scope of intelligence collection requirements and assessment priorities, the disruption of traditional intelligence practices by technological and other changes, the requirements of greater integration as well as the difficulties of remaining at the leading edge of capability and skills against increasingly sophisticated, opaque and asymmetric adversaries. These challenges are addressed later in this Chapter.

AREAS OF STRENGTH

3.3 Australia's intelligence assets are highly capable and effective with advanced levels of analytical, technical and operational tradecraft engaged in areas of human intelligence (HUMINT), signals intelligence (SIGINT) and geospatial intelligence (GEOINT). Australia's intelligence agencies are staffed by highly professional and dedicated officers of great integrity. The AIC is well regarded among its Five Eyes and other international partners. There is also a strong, positive culture of accountability under law within Australia's intelligence agencies.

3.4 The agencies are performing well in countering terrorism as one of the nation's highest national security priorities. Since the national terrorism threat level was raised to 'Probable' in 2014, there have been twelve major disruptions in Australia to prevent imminent attack plans. Lone actors present significant challenges for the AIC and law enforcement agencies, and other concerning terrorism risks remain. But, in terms of practical outcomes over recent times, the counter-terrorism record of the AIC and the wider national intelligence and security community is an impressive one. Australia's agencies are also working closely with partners

in neighbouring countries to counter terrorist networks in our region, including preventing attacks planned against international targets.

3.5 Australia's intelligence agencies have also performed co-operatively and with similarly impressive results in relation to the challenge of people smuggling. In addition, the AIC has performed exceptionally strongly in providing intelligence to support Australian Defence Force (ADF) operations. Intelligence has provided critical inputs into operational decision-making and force protection in Iraq, Syria and Afghanistan. Strategic intelligence assessments, including the range of Defence Intelligence Organisation (DIO) products, have helped provide contextual awareness to Australian policy makers in the deployment of forces and the development of long-term ADF military capabilities. Intelligence has not only effectively supported operational and strategic planning but has also contributed importantly to Australian peacekeeping and peace-monitoring operations, counter-piracy strategies as well as contingency planning for regional humanitarian assistance and disaster relief.

3.6 Similarly, valuable intelligence support has been provided by Australia's intelligence agencies in responses to major international incidents. The aftermath of the MH17 disaster was one such example.

3.7 Over recent years, the AIC has worked collaboratively in specific areas to deliver more focused and timely intelligence, particularly for operational decision makers. Through enhanced co-ordination initiatives and fusion centres, agencies have addressed particular areas of interaction that reflect the changing nature of Australia's national security environment. An important feature has been the growth in 'mission approaches' to tackle complex issues through whole-of-government operational and policy responses. These have included:

- the role of the Commonwealth Counter-Terrorism Co-ordinator and the functions of the Centre for Counter-Terrorism Co-ordination which are designed to ensure Australian counter-terrorism strategies at operational, policy and capability levels are effectively co-ordinated;
- the Operation Sovereign Borders Joint Agency Task Force which co-ordinates whole-of-government strategies to combat people-smuggling and the specific intelligence inputs to the work of the Disruption and Deterrence Task Group;

- the Australian Cyber Security Centre which co-locates the AIC's cyber security capabilities (including collection and assessment) with those from the broader national intelligence and law enforcement community;
- the National Threat Assessment Centre (NTAC) which is located in the Australian Security Intelligence Organisation (ASIO) and integrates a limited number of staff from agencies and policy departments; and
- on a smaller scale, collaborative structures for intelligence support to initiatives to counter the proliferation of weapons of mass destruction.

3.8 Increasingly, agencies are partnering to enhance their respective capabilities and deliver better intelligence outcomes. Co-operation among collection and operational agencies has continued to grow as a result of the mission approaches outlined above and through other collaborative projects. In intelligence assessment, the interactions of the Office of National Assessments (ONA) and DIO reinforce the importance of both contestability and collaboration through regular analytical tradecraft training and exchanges, peer review as well as the production of joint products where appropriate. Furthermore, some agencies have focused explicitly in their future strategic planning on the need for, and implications of, greater interdependence and integration of intelligence capabilities along 'mission' lines.

3.9 Australia's intelligence agencies have established increasingly effective relationships over recent years with Australian businesses and others in the non-government sector in ways that advance the national interest including through the Trusted Information Sharing Network, the broad-based engagement by NTAC and diverse bilateral agency interactions with individual private sector entities and organisations.

3.10 The AIC's international partnerships are another strength that underpins Australia's intelligence capabilities. Australia has global interests but its intelligence capabilities cannot realistically achieve genuine global coverage. Intelligence partnerships extend the reach of Australian agencies, providing access to a greater breadth and depth of information and perspectives on global developments outside our region. While our relationships with the traditional Five Eyes partners remain of critical importance for access to intelligence data, assessments and advanced capabilities, the complexity and scope of our global interests mean our intelligence relationships with some non-Five Eyes partners have

grown substantially in significance and intensity. These interactions have been crucially important in combating threats from non-state actors such as terrorists and people smugglers, and in responding to incidents such as hostage-taking and consular emergencies. Australia's own contribution and capabilities to intelligence-sharing with Five Eyes and non-Five Eyes partners is highly valued by intelligence counterparts in those countries.

CHALLENGES

3.11 While the AIC has performed effectively overall, and exceptionally well in particular areas noted above, there are a range of challenges it faces as well as opportunities for building on its impressive achievements to date.

Co-ordination

3.12 Effective co-ordination of the AIC is both necessary and desirable in the pursuit of a range of critically important objectives. These include the provision of intelligence community leadership and broad strategic direction-setting for intelligence as a national enterprise; the clear identification of national intelligence priorities in support of the policy priorities of the government of the day; effective cross-agency implementation of those priorities, maximising the efficiency of resource allocation, particularly in terms of the impact of the accelerating pace of technological change; and the robust evaluation of individual agency and broad-based AIC performance. Effective co-ordination also requires the development of relevant joint capabilities and assets across the AIC, a strategic focus on AIC workforce planning requirements, and accountability to the Prime Minister and other Ministers for the AIC's output and performance.

3.13 In our view, across all these benchmarks of effective AIC co-ordination, more can be achieved. In particular, intelligence community leadership is impeded by the absence of an appropriate explicit remit, by the nature of the current deeply 'federated' intelligence structure, and by an insufficient number of individuals with comprehensive cross-agency appreciation of the full range of Australian intelligence capabilities, activities and potential synergies.

Intelligence Priorities and Resource Management

3.14 While the current arrangements for setting and implementing National Intelligence Priorities (NIPs) provide broad guidance to Australia's intelligence agencies, the scope for agencies to reallocate resources from lower to higher priorities is very limited because of the large number

of high priorities and funding constraints. The arrangements would also benefit from greater clarity in relation to the ordering of priorities and greater precision on the extent to which there is an ongoing need for intelligence input as distinct from other forms of coverage. Many of the arrangements which oversee the prioritisation mechanisms could be made more effective.

3.15 In an overall sense, the current prioritisation and co-ordination processes are in need of some adjustment to resolve difficult but necessary prioritisation and resourcing issues. They need more authority, particularly in addressing the reality that currently important and immediate priorities are having the effect of crowding out longer-term issues.

3.16 A particular and increasingly important need will be for the collection prioritisation decisions, resource allocation priorities and capability development agenda of the larger AIC agencies to be managed in ways that are closely connected with the broader needs and potential joint capability development options of the intelligence community as a whole.

3.17 Effective co-ordination of risk management on intelligence issues is also an increasingly complex and consequential requirement, encompassing a broad set of stakeholders. We address this issue further in Chapter 6.

Evaluation

3.18 The processes for evaluating the performance of individual intelligence agencies and the AIC as a whole need to work more effectively. Our view is that the annual evaluations conducted by ONA and the Department of the Prime Minister and Cabinet (PM&C) do not accommodate the broad functions and mandates of particular agencies, and have inadequate discernible impact on prioritisation, resource allocation, capability development or overall performance. Neither ONA nor PM&C is adequately resourced in the context of their roles in evaluating individual agency and overall AIC performance. Moreover, the Submissions of several agencies to this Review reflected an assessment that current evaluation processes do not address the key challenges facing agencies.

ICT Connectivity

3.19 While ICT connectivity within the AIC works well, connectivity between the AIC and other agencies – and with policy departments – would benefit from upgrading to ensure that relevant intelligence material

is available to those who can make best use of it in the most timely way. Widespread secure desktop communications among intelligence agencies and policy counterparts is a critical requirement for closer policy–intelligence integration. Voice connectivity, in particular, facilitates timely discussions about intelligence requirements or products without necessitating face-to-face meetings.

Accountability to Government

3.20 In our view, there is scope for improvement in the ways in which the AIC as a whole accounts to the government of the day, and in particular to the National Security Committee of Cabinet, for its performance against intelligence priorities.

3.21 ONA is sometimes perceived as being responsible for co-ordination of the AIC as a whole. But ONA's actual legislated responsibilities are restricted to co-ordinating "the foreign intelligence activities that Australia engages in."[6] Its formal authority over the other agencies is therefore limited. These factors result in unrealistic expectations on ONA to co-ordinate effectively across the AIC. As the national security environment and national security structures have evolved over time, ONA's position has also changed. Increasingly, new structures and interactions have meant there are substantive areas of intelligence co-ordination activity now taking place outside of ONA's direct remit. For example, important aspects of intelligence co-ordination are currently performed by the Commonwealth Counter-Terrorism Co-ordinator, the Australian Cyber Security Centre and Operation Sovereign Borders.

3.22 Within its existing mandate, ONA is not positioned to meet the broader challenges of AIC co-ordination. Organisationally, ONA is not resourced to allocate to co-ordination tasks a sufficient number of officers with appropriate expertise, particularly given the demands on it in relation to meeting its increasingly diverse assessment responsibilities. Furthermore, the status of the Director-General of ONA is currently seen as less senior than that of leaders of some other AIC agencies. It is against this background that we put forward in Chapter 4 proposals for more effective co-ordination of Australia's intelligence agencies.

The AIC and the Broader Intelligence Community

3.23 There are six agencies that constitute the AIC: ASIO, the Australian Secret Intelligence Service (ASIS), ONA, the Australian Signals Directorate (ASD), DIO and the Australian Geospatial-Intelligence Organisation (AGO).

6 The *Office of National Assessments Act 1977* (ONA Act), s.5.

Membership of the broader 'National Intelligence Community' (NIC) also includes those parts of the Australian Federal Police (AFP) and the Department of Immigration and Border Protection (DIBP) which perform intelligence related functions, as well as the Australian Criminal Intelligence Commission (ACIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC). To be clear, we are not including the AFP and DIBP as organisational entities in the NIC but only those parts of each that are engaged in intelligence functions.

3.24 There have been important linkages established among NIC agencies and with the policy agencies through their involvement in intelligence community groupings (such as the National Intelligence Co-ordination Committee and the National Intelligence Collection Management Committee),[7] through functional co-operative arrangements (such as the Centre for Counter-Terrorism Co-ordination) and through bilateral operational and other interactions among particular agencies.

3.25 These points of connection facilitate highly effective and productive co-operation in some critical areas of national security. But they will need to be taken further as the boundaries between intelligence processes become less clear-cut and as the realities of intelligence as a national enterprise become more compelling. In this context, our view is that the 'AIC' construct will increasingly become a more artificial one as the seamless nature of national intelligence becomes more accentuated. In the Australian context, this will be evident at a number of levels.

3.26 DIBP is expanding its role in strategic, operational and tactical intelligence on issues related to border threats, including to maintain a "current and comprehensive intelligence picture on issues such as counter-terrorism, counter-proliferation and maritime people smuggling, serious and organised crime, and visa fraud."[8] We consider that the expansion of DIBP's intelligence role is logical, legitimate and necessary for the pursuit of its responsibilities, and that this role will increasingly need to be integrated into, and co-ordinated with, broader NIC functions and capabilities.

3.27 The intelligence-related work of the AFP, and its interaction with other agencies, continues to diversify and deepen. AUSTRAC's role as Australia's financial intelligence unit, with responsibility for anti-money laundering and counter-terrorism financing, is growing in significance.

7 The National Intelligence Co-ordination Committee and National Intelligence Collection Management Committee include representatives from the NIC agencies, as well as from the Departments of the Prime Minister and Cabinet, Foreign Affairs, Defence, and the Attorney-General's Department.

8 From: https://www.border.gov.au/about/careers-recruitment/intelligence.

ACIC's investigative, research and information delivery functions in relation to current and emerging crime threats and criminal justice issues is also interacting more intensively with related intelligence areas.

3.28 These realities in the broader intelligence community constitute a further dimension of the integration challenge that members of the NIC face. The linkages among them established to date will need to be significantly consolidated and expanded in a more comprehensive way. We assess that in the period ahead a frame of reference for the intelligence community that encompasses the 'AIC Six' as well as ACIC, AUSTRAC and those parts of the AFP and DIBP which perform intelligence functions will be a more realistic one than the traditional AIC construct.

Increasing Requirements

3.29 The agencies are being expected to deliver on a broadening agenda that includes intelligence collection and assessment, aspects of policy implementation, crisis and emergency responses, as well as support for ADF operations. Broadening demands on Australian agencies are also being generated by the pace of technological change (particularly in relation to big data) and by the impact of globalisation on the rapidly accelerating movement of people, goods, money, weapons and ideas across national borders. To address effectively this broadening range of expectations and requirements, the intelligence agencies will require streamlined prioritisation arrangements, enhanced co-ordination and, in some instances, increased access to resources.

ONA Intelligence Assessments

3.30 The functions of ONA include focusing on "information relating to international matters that are of political, strategic or economic significance to Australia."[9] Under its legislation, ONA is required to report in relation to "matters of current significance" and to produce assessments on matters of "national importance."[10]

3.31 ONA pursues these assessment roles responsibly and professionally. Its staff are highly skilled and deeply committed. Its reports are well-informed on an all-source basis and its judgments are subjected to robust internal review. They are held in very high regard internationally, especially among Australia's Five Eyes partners.

9 ONA Act 1977, s.5.
10 ibid.

3.32 For all ONA's attributes and achievements, however, we consider that its reporting and assessments could be more directly connected to the needs and requirements of policy-making, particularly in relation to economic issues and linkages between economic and security developments. The Hope Royal Commissions emphasised the important potential role that ONA could play in economic intelligence.[11] We share the same perspective.

3.33 ONA is being stretched in terms of its tasking and the expectations of its product. Particular pressures on it in some areas (such as the provision of current intelligence and information relevant to day-to-day policy decision-making) are impacting on its capacity to focus on other responsibilities including medium to longer-term reporting.

3.34 In addition, we assess that more contestability of ONA's assessments, including through deeper, more structured and more productive engagement with expertise outside government (in academia, think tanks and the private sector), would better enable ONA to meet the contemporary needs of government.

3.35 In our view, there is another dimension in relation to ONA product. It relates to some unrealistic expectations of what ONA can and should do. ONA is Australia's peak body for foreign intelligence assessment. Its product is the result of rigorous and careful intelligence methodology. Furthermore, at times some intelligence targets are opaque and elusive, making assessments of them highly conditional or on specific aspects simply not possible. These are realities of life for ONA, and expectations of what its intelligence assessment role can deliver need to be tempered by a clearer understanding of intelligence processes and inherent limitations related to them.

Intelligence Agencies' Workforce

3.36 Australia's intelligence agencies are facing a range of challenges relating to the recruitment, retention, career management and training of their workforces. These challenges derive partly from the rapid evolution of technology, the demand for technological expertise in the private sector and the long lead times in security clearance processes. They also reflect the pressures on staff numbers as well as work cultures, career structures and public sector remuneration practices.

11 Royal Commission on Australia's Security and Intelligence Agencies, 1984, *Report on the Office of National Assessments and the Joint Intelligence Organisation*, 3.118–3.130, pp.48–52.

3.37 These challenges are particularly demanding where highly specialised and technologically expert workforces are involved. ASD is one such organisation. ASD has experienced a net reduction in its workforce over recent years. While the *2016 Defence White Paper* has provided for significantly increased staffing numbers for Defence-intelligence related capabilities over the next decade, and for ASD in particular, the net reduction in ASD staff over recent years has presented significant challenges.

Cyber Security Issues

3.38 The Australian Cyber Security Centre (ACSC) is an important national initiative to develop synergies within government and the wider community on cyber issues. It was established in 2014, replacing the Cyber Security Operations Centre which had been operating within ASD. The ACSC brings together representatives of all of the Government's cyber security elements into a single location.

3.39 To achieve its full purpose, ACSC needs to be a more genuinely integrated organisation with clearer lines of authority and leadership. The Government's 2016 *Cyber Security Strategy* sought to strengthen the ACSC, including by arrangements to provide greater guidance on national priorities and moving it from ASIO's building to a new location that would allow for more integrated partnerships between government, business, academia and foreign partners. That move, to the Brindabella Business Park in Canberra, which is scheduled to occur in the second half of 2017, will be important in enhancing the ACSC's national cyber security role.

3.40 To enable ACSC to realise its full potential, we assess that the Head of the ACSC needs to have the authority to direct staff. Organisationally, the ACSC should have a clear set of functions and authorities that allows it to integrate all of the Government's cyber security activities in accordance with national priorities, and to provide cyber security advice and assistance to government, the private sector and the community. We make recommendations in Chapter 4 on how progress can be achieved towards these objectives.

Data Sharing and Collective Analysis

3.41 We consider that there are critical capacities in the context of data sharing and collective analysis that could be realised by more fully exploiting economies of scale, more effectively utilising integrated data

analytics and a more productive pooling of technical expertise. We address ways in which these objectives can be pursued in Chapters 4 and 5.

Science, Technology and Innovation Outreach

3.42 Within the NIC, the scope of science, technology and innovation outreach as well as industry engagement generally is also a challenge. Some important connections between expertise in agencies and capacities in the non-government sector have been established by individual agencies over recent years. But such outreach has lacked sustained investment as well as a 'whole-of-NIC' approach on priority areas in which the benefits of national science and innovation expertise to Australian intelligence can be maximised. This challenge is further addressed in Chapter 5.

CONCLUSION

3.43 This Chapter has highlighted areas of real strength and highly impressive achievements over time on the part of Australia's intelligence agencies. It has also identified some key challenges for the intelligence community. The remainder of this Report will focus on ways in which these can be addressed. This will include proposals for structural change within the NIC (Chapter 4), resourcing options to address specific challenges (Chapter 5), adjustments to the legislative framework governing the intelligence community (Chapter 6) and proposals in relation to oversight and accountability arrangements (Chapter 7).

[This page intentionally left blank]

CHAPTER 4: NEW STRUCTURAL ARRANGEMENTS FOR MANAGING THE NATIONAL INTELLIGENCE ENTERPRISE

4.1 This Chapter addresses the Review's third Term of Reference "*whether the AIC is structured appropriately, including in ensuring effective coordination and contestability.*" It also addresses the Term of Reference in relation to the "*effectiveness of evaluation arrangements*." The Chapter proposes new structural arrangements to address some of the challenges identified in Chapter 3. In particular, we propose changes aimed at providing the co-ordination and leadership required to manage Australian intelligence as a genuinely national enterprise. We also address the place of the Australian Signals Directorate (ASD) within the intelligence community given its multiple roles as a Defence signals collection agency, as the Australian Government's authority for signals intelligence, information security and assurance, and as an organisation with a lead capability role in cyber security matters.

STRUCTURE OF AUSTRALIA'S INTELLIGENCE COMMUNITY

4.2 In considering issues relating to the structure of the intelligence community, our starting point was not oriented to significant changes. Australia's intelligence community is performing very effectively overall. Its individual agencies are generally performing very capably and are able to point to an impressive set of operational outcomes and effective strategic planning in a complex and changing threat environment. Despite our starting point not being focused on structural change, we became convinced over the course of this Review that some of the challenges facing the intelligence agencies would be most effectively addressed if changes are made to its structure. These changes are needed to facilitate a genuinely national enterprise that is agile, innovative and effective in responding to the challenges of twenty-first century intelligence.

4.3 In summary, we are not recommending changes in intelligence agency structures for the sake of it. We are recommending them to promote synergies within the broader intelligence community, clearer direction-setting and prioritisation, more effective resource allocation, more productive evaluation and benchmarking, and more instances of shared capability development and joint procurement. And we are also recommending structural change in response to the evolving role of ASD.

Co-ordination and Integration – the Case for Enterprise Management

4.4 Over the past decade or more, each of Australia's Five Eyes partners has pursued greater co-ordination of, and integration among, its intelligence agencies. They have done so at differing paces and in different ways but with a shared sense of purpose.

4.5 After the 9/11 attacks, the United States established an Office of the Director of National Intelligence led by a Director (DNI) who is a Cabinet-level appointee responsible for overseeing the activities of 17 US intelligence agencies. The DNI's functions and authorities are set out in legislation. The DNI is the principal intelligence adviser to the President and has a degree of influence over the intelligence community's budget and senior appointments.

4.6 The United Kingdom has also sought to strengthen intelligence co-ordination arrangements over the past decade, particularly as a consequence of the 7/7 attacks on the London transport system in 2005. The focal point for co-ordination is the role of the UK National Security Adviser in the Cabinet Office, with intelligence co-ordination delegated to the Deputy National Security Adviser. Their role is enhanced by their management of a Single Intelligence Account which encompasses the budgets of the three largest intelligence agencies: the Security Service, the Secret Intelligence Service and the Government Communications Headquarters (GCHQ). This budgetary mechanism has been an important driver of shared capabilities across the three agencies. The momentum towards greater integration has been further reinforced by passage in 2016 of the *Investigatory Powers Act* which enhances the common legal regime applicable to the three major intelligence agencies.

4.7 New Zealand and Canada are also moving towards greater co-ordination. The New Zealand Security Intelligence Service and the Government Communications Security Bureau report to a single responsible Minister. The Department of the Prime Minister and Cabinet is responsible for the leadership, co-ordination and performance of the core New Zealand intelligence agencies.[12] And a new single Bill governing the agencies has passed through the New Zealand Parliament. The Canadian intelligence community is also promoting co-ordination of

12 Sir Michael Cullen and Dame Patsy Reddy, *Report of the First Independent Review of Intelligence and Security in New Zealand: Intelligence and Security in a Free Society,* 2016, pp.37–38. The core agencies are the New Zealand Security Intelligence Service, Government Communications Security Bureau and the National Assessments Bureau.

intelligence community activities through the role of its National Security Advisor in the Privy Council Office.

4.8 Australia is now alone among its Five Eyes partners in not having a single point of co-ordination for its intelligence community. Australia currently has high-class intelligence agencies, but for individual agencies and the intelligence community generally to be truly world-class the whole must be greater than the sum of the parts.

4.9 The structure of the intelligence community needs to reflect Australia's own governance practices, priorities and circumstances. Nonetheless, models of integration adopted by Australia's Five Eyes partners provide lessons drawn from experience in relation to modernising intelligence co-ordination arrangements. These lessons encompass the advantages of 'light-touch' rather than prescriptive co-ordination including on priorities, resourcing, mission integration, ICT connectivity and appointments. They also include the importance of seniority, intelligence experience, peer respect and a close connection to the Head of Government in any leadership role co-ordinating agencies.

4.10 There is a familiar contention in the Australian context that the smaller scale of the intelligence community, relative to counterparts in the United States and United Kingdom, and the close interaction among leaders of the intelligence agencies mitigate the need and desirability for the National Intelligence Community (NIC) to move in the same direction on integration as intelligence communities in those countries. We do not agree with such arguments. We see effective co-ordination as an indispensable requirement for twenty-first century intelligence. Current structures do not enable such co-ordination and a distinctively Australian model for it needs to be implemented in a deliberate way. We believe that more effective co-ordination of Australia's intelligence agencies will enhance the Australian system of Ministerial responsibility and the intelligence community's accountability to the Government. We also believe that enterprise-level management of Australia's national intelligence capabilities will complement the statutory responsibilities of agencies.

Options for Enterprise Management of Australia's Intelligence Agencies

4.11 We examined a number of potential options for the intelligence co-ordination function in Australia. One option would be to widen the existing remit of the Office of National Assessments (ONA) and substantially increase its resources, noting that the Hope Royal

Commission recommendations intended ONA to be at the centre of the Australian Intelligence Community (AIC). A number of Submissions to this Review argued a larger and better resourced ONA would be able to assume more meaningful priority-setting, co-ordination and evaluation, to manage the national intelligence missions more effectively, and to deliver assessments which better meet the needs of policy makers.

4.12 We set out in Chapter 3 the challenges that ONA faces in its co-ordination role. Additional resourcing alone is not a remedy. In our view, ONA's focus on its role as the peak body for foreign intelligence assessment does not give it the appropriate perspective for co-ordinating the activities of Australia's intelligence agencies within the framework of a twenty-first century national intelligence enterprise. In this context, realities have changed since the time ONA was established following the first Hope Royal Commission. As noted in Chapter 2, the processes of intelligence are more diffuse; the balance of strategic and operational intelligence has shifted; the demarcations between security and foreign intelligence have blurred in some respects; and the requirements for effective co-ordination of national intelligence have also changed.

4.13 The nature of twenty-first century intelligence that we outlined in Chapter 2 has direct consequences for the structure and operation of Australia's intelligence agencies. It calls for clear direction-setting across the broad spectrum of foreign and security intelligence, and the promotion of effective integration and synergies in support of intelligence as a national enterprise. It also calls for the provision of a single focus of accountability to the Government for the performance of the NIC as a whole.

4.14 The co-ordination that Australia's intelligence agencies require in the twenty-first century is different to that which shaped the establishment of ONA in 1977 and defined its legislative mandate. What is required into the future is an enterprise-based management of the NIC that provides leadership and a focus on integration across the full spectrum of intelligence activities.

4.15 ONA's functions and priorities are shaped primarily by its foreign intelligence assessment role and its constrained co-ordination functions in relation to foreign intelligence. ONA's foreign intelligence assessment role will continue to be indispensable. But, as an organisation, we consider that ONA is neither oriented to, nor structured for, the modern leadership role and co-ordination responsibilities that Australian intelligence in the twenty-first century requires. That role and those responsibilities call for

a new organisation specifically designed, structured and resourced for the contemporary and future challenges that the Australian national intelligence enterprise faces.

4.16 A second option we considered was to locate the intelligence co-ordination function within the Department of the Prime Minister and Cabinet (PM&C). PM&C is a policy co-ordination department. It is connected with, but not part of, the NIC. Given the ongoing importance of distinguishing policy roles and intelligence purposes, we do not consider that PM&C is the most appropriate location for co-ordination of Australia's intelligence activities.

4.17 The imperative of a national intelligence enterprise, the nature of Australia's changing national security outlook, the current challenges facing agencies (outlined in Chapter 3) and the rising expectations of Australian governments all reinforce the need for change in the co-ordination arrangements for Australian intelligence that have existed for the past four decades. We do not consider that ONA or PM&C constitutes an appropriate location for the new arrangements nor for addressing the challenges associated with facilitating a national intelligence enterprise. **We recommend that an Office of National Intelligence (ONI) be established as a statutory authority within the Prime Minister's portfolio.**

THE OFFICE OF NATIONAL INTELLIGENCE

4.18 ONI would be the principal advisory agency to the Prime Minister on intelligence matters. Its responsibilities would include producing all-source national assessments and strategic foreign intelligence assessments; clearly identifying national intelligence priorities in support of government policy-making; overseeing robust evaluations of individual agency and community performance, drawing on external expertise as required; co-ordinating proposals for the development of joint capabilities and shared services across the NIC, including through enhanced private sector engagement; presenting annually an Intelligence Capability Investment Plan for the Forward Estimates period; devising strategies for, and co-ordination of, Australia's international intelligence liaison relationships; and setting community-wide intelligence standards in areas such as security, analytic tradecraft and ICT.

4.19 ONI responsibilities would also include facilitating a strategic focus for workforce planning and training, and providing a single point of accountability to the Prime Minister and the National Security Committee

of Cabinet generally for the performance of the intelligence community, additional to the accountability of individual agencies to their responsible Ministers.

4.20 If our recommendation to establish ONI were accepted by the Government, the current roles, staff and functions of ONA would be subsumed by ONI. As has been the case with ONA, ONI's role, responsibilities and prerogatives would be set out in legislation, providing it with an explicit mandate. We acknowledge that the transition will have some complexity and will take time.

Director-General of the Office of National Intelligence

4.21 **We recommend that ONI be led by a Director-General (DG ONI) and that this appointment be at departmental Secretary level. We also recommend that DG ONI be the head of the NIC as well as the Prime Minister's principal adviser on intelligence community issues, with the role including advice on the appointment of senior NIC office-holders and succession planning. We further recommend that DG ONI be a member of the Secretaries Committee on National Security, reflecting the importance of the co-ordination and assessments functions of ONI.**

4.22 Effective and regular interaction with the Prime Minister would be critical to the authority of DG ONI. **We recommend that DG ONI provide the Prime Minister with a written personal overview every two weeks on key current and emerging issues for the intelligence agencies. We also recommend that this overview be supplemented by meetings with the Prime Minister every two weeks.**

4.23 DG ONI would not control the intelligence agencies' operational activities nor infringe on their statutory responsibilities. **We recommend that, without directing the specific activities of agencies, DG ONI be able to direct the co-ordination of the NIC to ensure there are appropriately integrated strategies across the suite of NIC capabilities**. DG ONI should be able to influence and shape the balance of resources across the intelligence community, promote shared capability development, and provide advice to the Prime Minister on intelligence-related new policy proposals and Cabinet Submissions from a whole-of-community perspective. Consistent with established Ministerial portfolio responsibilities, DG ONI would not have control over, or responsibility for, individual agency appropriations.

4.24 These arrangements in relation to DG ONI accommodate the special responsibilities of the Director-General of Security, preserve the political

impartiality of the Australian Security Intelligence Organisation (ASIO) and allow for the appropriate compartmentalisation and management of sensitive counter-espionage and foreign interference cases. There will continue to be a range of matters falling into this latter area that will require the Director-General of Security to maintain direct and exclusive contact with the Prime Minister and, where appropriate, the Leader of the Opposition.

4.25 The National Intelligence Co-ordination Committee (NICC) will have an important ongoing role in ensuring that there is a strong relationship between the intelligence community and the policy and operational agencies. To achieve that purpose, however, its membership needs to be expanded to ensure that the perspectives of the Australian Defence Force (ADF) are appropriately considered in intelligence co-ordination arrangements. This is particularly important given Defence's unique technical requirements, operational experience and organic ADF intelligence capability. **We recommend that DG ONI chair the expanded NICC and that its membership include the Chief of the Defence Force or their representative**.

4.26 To help promote enhanced integration among NIC agencies, **we also recommend that DG ONI chair a new Intelligence Integration Board**. The Board would include relevant Agency Heads as members to oversee strategic planning, staffing, resources and benchmarking in current or new areas of integration focus. In relation to current integration priorities, the Board should specifically include in its remit counter-terrorism, cyber, and data sharing and connectivity.

4.27 In accordance with the above, **we recommend that DG ONI's roles and responsibilities be supported by a new legislative mandate which would include the provision of statutory independence for the position of DG ONI**. **We also recommend that DG ONI be accountable to the Prime Minister and the National Security Committee of Cabinet for the performance of the NIC generally, and agencies in particular, in relation to the National Intelligence Priorities (NIPs) and the provision of relevant input to Ministerial and Cabinet decision-making.**

4.28 To support this accountability role, DG ONI should be responsible for new approaches to setting intelligence priorities and for more rigorous evaluation of the performance of agencies and the NIC generally.

Organisational Structure of ONI

4.29 To achieve its purposes, **we recommend that ONI encompass two main areas led by Deputy Directors-General (at the Senior Executive Service Band 3 level) for Intelligence Enterprise Management (including intelligence integration) and Assessments.** The Intelligence Enterprise Management position would be responsible for co-ordination and national intelligence priority setting (including the setting of the NIPs as well as the roles of the NICC and National Intelligence Collection Management Committee (NICMC), both of which facilitate important connections with policy departments), integration of key intelligence missions as well as NIC evaluation mechanisms. ONI's Assessments role would focus on producing national and strategic foreign assessments as well as on engagement with senior policy makers, other intelligence agencies, policy departments and areas of external expertise. Security intelligence assessments would remain the responsibility of ASIO, and the Defence Intelligence Organisation's (DIO) assessment role would remain unchanged.

ONI's National Intelligence Enterprise Management Role

4.30 ONI's National Intelligence Enterprise Management role should have a particular focus on issues of prioritisation, evaluation of the NIC and individual agency performance as well as the promotion of integration and inter-agency synergies. We envisage that this National Intelligence Enterprise Management role would require approximately 50 additional staff.

Prioritisation

4.31 In Chapter 3 we outlined the challenge of increasing demands on Australia's intelligence agencies and the implications for intelligence priority setting. In our view, the NIPs and NICMC processes need to be reformed to work more effectively. **We recommend DG ONI be given the authority and responsibility for advising government on the intelligence collection and assessment priorities, and allocating responsibility for intelligence collection across the intelligence agencies.**

4.32 In practical terms, DG ONI should recommend to Ministers (in consultation with other intelligence agencies and policy departments) a set of NIPs matched against available intelligence community resources. These priorities should be formally updated every 12 months as part of the evaluation process outlined below. Reflecting the synergies of the modern intelligence enterprise, ONI should evaluate the intelligence

agencies on the basis of their collective and individual performances against their assigned responsibilities for specific priorities.

4.33 **We recommend that DG ONI also report to the Prime Minister and the National Security Committee of Cabinet on a regular basis to provide a holistic view of performance against priorities and to make recommendations on ways of closing intelligence gaps, making choices among relative priorities, and in consultation with heads of relevant intelligence and policy agencies ensuring the appropriate mix of intelligence coverage.**

4.34 This report by DG ONI to the National Security Committee of Cabinet would assist in clarifying the Government's risk appetite, and in particular decisions that need to be made about trade-offs between the funding of urgent priorities and desirable longer-term investments in capability. Such clarification would underpin DG ONI's authority to better direct the co-ordination of intelligence efforts. To fulfil this responsibility, senior staff in ONI would need to have a good understanding of the totality of activities undertaken by the intelligence agencies.

4.35 In areas of high priority intelligence focus, we make further recommendations below on how ONI should harness and improve inter-agency synergies as part of ONI's National Intelligence Enterprise Management role.

Evaluation of Intelligence Agencies

4.36 In Chapter 3 we commented on current arrangements for evaluating the performance of individual intelligence agencies and the AIC as a whole. **We recommend that DG ONI have responsibility for new arrangements for agency and NIC evaluation that make practical assessments of progress in relation to prioritisation, effectiveness, resource allocation, capability development and co-ordination.** The new review process should be focused on assisting agencies and their staff to better perform their roles and functions. In our view, this responsibility of DG ONI for evaluation should be pursued at two levels.

4.37 The first would be an annual report by DG ONI to the Prime Minister, and subsequently to the National Security Committee of Cabinet, on the overall effectiveness of Australia's intelligence agencies in implementing the NIPs set by the Government. This report could also identify specific achievements of individual agencies as well as particular challenges that they may be encountering.

4.38 The second dimension of evaluation is focused at an agency level. **We recommend a new evaluation process for NIC agencies similar to the Functional and Efficiency Reviews currently led by the Department of Finance.** These reviews should be the responsibility of DG ONI and be conducted by senior, qualified and experienced staff from ONI and the Department of Finance supplemented as appropriate by competent external reviewers with current or past experience of working in or with intelligence agencies. Such reviews should be conducted every two years for the larger agencies (the Australian Secret Intelligence Service (ASIS), ASIO and ASD) and every three years for other intelligence agencies. The evaluation of ONI itself should be led by PM&C in conjunction with the Department of Finance. These agency evaluation reports should be provided to the National Security Committee of Cabinet.[13]

Integration and Inter-Agency Synergies

4.39 Promoting integration and synergies in areas of high priority intelligence focus would be a critically important responsibility of ONI in its National Intelligence Enterprise Management role. Those areas include counter-terrorism, cyber security as well as data sharing and connectivity. Each of these issues are, in their own right, of the highest importance to Australia. Moreover, each needs an approach that integrates the capabilities of foreign and security intelligence, intelligence and law enforcement, and an extremely close relationship between the intelligence community and policy agencies. These areas of greater intelligence integration focus are not exclusive. There will be other areas where such integration will be warranted in light of changing circumstances, and DG ONI should take the lead in identifying such areas and promoting such integration.

Counter-Terrorism Intelligence Integration

4.40 The *2015 Review of Australia's Counter-Terrorism Machinery* strengthened Australia's counter-terrorism structures by establishing the Commonwealth Counter-Terrorism Co-ordinator position to lead and co-ordinate the Commonwealth's operational and policy counter-terrorism responses in partnership with the States and Territories.

4.41 The Counter-Terrorism Co-ordinator is supported by the Centre for Counter-Terrorism Co-ordination (CCTC). The CCTC is responsible for strategic and operational co-ordination across six distinct missions: intelligence (led by ASIO), law enforcement operations (led by the

13 The Review benefited from particular insights on evaluation processes provided by Mr Frank Lewincamp.

Australian Federal Police (AFP)), offshore operations (led by ASIS), border security (led by the Department of Immigration and Border Protection), community engagement (led by the Attorney-General's Department) and international engagement (led by the Department of Foreign Affairs and Trade (DFAT)).

4.42 The intelligence mission of the CCTC sets priorities and evaluates agencies' performance against those priorities. That mission is currently focused in a particular way on the threat posed by Australian foreign fighters and radicalised individuals in Australia. Within this context, arrangements are working well.

4.43 Over recent years, the National Threat Assessment Centre (NTAC), located in ASIO, has initiated the production of documents on intelligence strategy and collection requirements for key counter-terrorism priority areas. NTAC's focus is on a broad framework of threat assessment and its business model of integrating staff from other agencies has been productive. This has enabled NTAC to access all relevant counter-terrorism intelligence to inform the priorities and operations of other NIC agencies. NTAC uses its integrated staff to reach back into their home agencies as required.

4.44 We consider there would be value in augmenting these arrangements so that a broader overview of all the activities that NIC agencies undertake in support of counter-terrorism can be achieved. This would facilitate better visibility of all relevant intelligence activities on counter-terrorism.

4.45 Moreover, we consider there is potential to enhance the broader integration and co-ordination of the Commonwealth's intelligence effort on counter-terrorism. In our view, this would be best achieved by establishing a role for ONI in the Commonwealth's counter-terrorism machinery. **We recommend that there be a senior dedicated ONI position to facilitate closer co-ordination and integration across the national counter-terrorism intelligence effort.**

4.46 ONI would be responsible for developing intelligence priorities to support the government's counter-terrorism requirements and for allocating activities in support of those priorities across NIC agencies. Furthermore, it would evaluate agencies' performance against those priorities. ONI's counter-terrorism role would encompass identifying, and assisting in the resolution of, impediments to effective collaboration. The senior ONI counter-terrorism officer would be supported by a small number of staff located in ONI. The position would report to the ONI Deputy

Director-General for Intelligence Enterprise Management and would also support the Commonwealth Counter-Terrorism Co-ordinator.

Cyber Security Integration

4.47 The 2016 *Cyber Security Strategy* provides a comprehensive blueprint for the development of Australia's cyber capabilities. Within the framework of that Strategy, the Australian Cyber Security Centre (ACSC) is a unique entity which has critical capability dependencies on ASD for its cyber security mission. In our view, a unified cyber security mission would significantly enhance the delivery of the Strategy and lead to a single point of co-ordination, accountability and public interface in relation to cyber security matters.

4.48 To achieve progress towards this goal, **we recommend that the ACSC should operate as part of ASD**. It is essential in our view that the ACSC has a seamless connection to ASD in its capacity as the national cryptologic agency which constitutes the critical mass of national expertise on cyber issues at a government level. It is also important for maintaining links with international partners which provide invaluable situational awareness and intelligence bases for incident response and policy deliberations. The United Kingdom has implemented a comparable arrangement, with GCHQ taking responsibility for the National Cyber Security Centre. In our view, such an arrangement most effectively facilitates access to diverse and sophisticated national capabilities on cyber security while making the benefits of that expertise as widely available as possible through the provision of information, assurance advice and support to government, industry, critical national infrastructure operators, businesses and individuals. As in the United Kingdom, the ACSC should have its own identity within the construct of ASD, reflecting the responsibility it should have for cyber security in Australia.

4.49 **We recommend that a Head of the ACSC be appointed as the single focus of accountability to the Government for cyber security.** Consistent with such a role for the Head of the ACSC, we consider the ACSC should integrate the cyber policy team currently located in the Office of the Cyber Security Special Adviser in PM&C. This would consolidate and clarify the lines of responsibility and authority on cyber security. **We further recommend that one Minister have primary responsibility for the ACSC and cyber security under arrangements to be determined by the Prime Minister**, **noting that the authorities under which ASD would continue to operate would derive from the Minister for Defence (as currently required by section 3A of the *Intelligence Services Act 2001* (ISA)).**

4.50 **We also recommend an Intelligence Co-ordinator for Cyber Security be appointed to meet and manage the growing expectations of the ACSC, particularly in safeguarding the security of government networks, responding to incidents and providing the intelligence to support policy and international engagement.** The ACSC Intelligence Co-ordinator for Cyber Security would be an ONI Senior Executive Service Band 2 officer and would be supported by a small number of staff, responsible for co-ordinating and integrating the ACSC's intelligence collection, analysis and operational resources to meet intelligence requirements for government's cyber security priorities. Day-to-day, the ACSC Intelligence Co-ordinator for Cyber Security would report to the Head of the ACSC, but should also be empowered by ONI's mandates in relation to visibility of agencies' cyber security activities.

4.51 **We recommend that staff from other agencies be seconded to the ACSC but also retain their existing organisational authorities and ability to access data, information and capabilities from their home organisations.** Working under the direction of the Head of the ACSC, these authorities would be exercised in accordance with the defined functions and priorities of the ACSC. The functions of the ACSC should either be reflected in a directive from the Prime Minister or legislation if necessary. The ACSC should bring together all of the Government's cyber security capabilities. Agencies, especially the Australian Criminal Intelligence Commission and AFP, should make a concerted effort to substantially strengthen their presence in the ACSC so that it is resourced with the expertise to cover the full spectrum of the national cyber security challenge, including cyber crime.

4.52 The ACSC should also include the Computer Emergency Response Team (CERT Australia) that is part of the Attorney-General's Department, noting that CERT Australia should continue to have responsibility for the Government's role in the Joint Cyber Security Centres being established in states and territories. ACSC should liaise closely with the Ambassador for Cyber Affairs. ACSC should also work in partnership with organisations outside of government and it should aim to have a significant number of representatives from the private sector. Given its national responsibilities, **we also recommend that ACSC's cyber hotline for Government agencies and the private sector should operate 24 hours a day, 7 days a week, and that a 24/7 capability to manage public messaging and policy advice in relation to rapidly emerging cyber events be established.**

4.53 **We recommend that, as part of the ACSC's role, the Head of the ACSC prepare a six-monthly report to the Cabinet proposing national cyber security priorities, evaluating progress towards them and assessing emerging cyber challenges.**

4.54 **We also recommend that the governance of the ACSC be provided by the current Cyber Security Board chaired by the Secretary of PM&C with its membership increased to include DG ONI and CEO-level representatives of critical national infrastructure sectors such as telecommunications, health care, financial institutions, other services, energy, water and ports.** Private sector members of the Board should undergo appropriate security clearances to allow frank discussions about the ACSC's capabilities.

4.55 **We recommend that ASD be given a formal legislative mandate which reflects its role as the national information and cyber security authority, including functions to combat cyber crime and to provide advice to the private sector on cyber security matters.** Broadening ASD's mandate recognises the increasing difficulty of delineating state and non-state actors in cyberspace as well as the need to be able to shift scarce operational cyber resources to areas of greatest need.

4.56 The overriding purpose of these recommendations is to establish the ACSC as the credible and authoritative voice on cyber security in Australia. The ACSC should aim to pre-empt or respond at speed to incidents and bring a new level of inclusiveness and co-operation with the private sector. It should also drive the development of a nation that is resilient against cyber threats.

Data Sharing and Inter-Agency Connectivity

4.57 In our view, the NIC would also benefit from greater co-ordination and integration of its data holdings and data tools, including a co-ordinated approach to the exploitation of open source data. As a basic principle, the NIC should be developing data tools and ICT infrastructure with a view to enabling collaborative projects and enhancing interoperability.

4.58 This approach has legislative, policy and oversight implications. It would also require significant adjustment within the work cultures of agencies to move toward a more integrated data environment.

4.59 We judge that ONI would be best placed to identify, prioritise and provide advice to government on further measures to bridge gaps in the connectivity between NIC agencies. This connectivity is not just

electronic. The NIC should also be moving toward homogenisation of systems access for staff, as well as for physical access. To enhance data sharing, connectivity and a more co-ordinated approach to open source data, **we recommend that ONI be responsible for leading and co-ordinating data management and ICT connectivity initiatives across the NIC.** We address this further in Chapter 5.

4.60 Open source material is becoming increasingly important in all aspects of intelligence. The National Intelligence Open Source Committee chaired by ONA seeks to co-ordinate the development of open source capabilities across the NIC, but in our view these efforts are hampered by the lack of a central lead or authority. While acknowledging that agencies should be able to maintain open source capabilities tailored to their own needs, some agencies also raised concerns about the risk of proliferation and duplication of open source capabilities. To address these issues, **we recommend the Open Source Centre (OSC) be integrated into ONI's National Intelligence Enterprise Management role and enhanced as a centre of expertise for open source collection, analysis, tradecraft and training.** The OSC within ONI would be responsible for a common library of analytic tools and techniques. Agencies would be able to use the common library of tools provided by the OSC to further analyse their own data holdings, as appropriate.

4.61 While agencies would need to be able to maintain tailored open source intelligence collection and analytical capabilities to suit their particular requirements, the OSC should have a remit to ensure capabilities that agencies are developing do not unnecessarily duplicate existing tools and techniques or those under development elsewhere.

ONI's Assessments Role

4.62 In Chapter 3, we identified the challenges of ONA assessments in meeting expectations related to policy-making. ONI would need to be established and operate in ways that address these challenges effectively.

4.63 ONI's assessment capability would need to have greater scale and scope, particularly in light of the geopolitical, economic and technological issues that will make Australia's strategic environment over the coming decade more complex and unpredictable. ONI should also have a greater capacity to provide assessments on foreign investment issues as well as inform the Critical Infrastructure Centre at the strategic level. Additional analytical resources would also be needed to support

ONI's recommended role as the principal advisory agency to the Prime Minister on intelligence matters, including its enhanced daily reporting responsibilities.

4.64 We would envisage that ONA's current analysts would form the core of ONI's assessment capability. In our view, however, that number of analysts would need to be significantly boosted in a new ONI structure. Given ONA's current relatively small base and ONI's expanded assessment responsibilities, **we recommend at least a 50 per cent increase in the current ONA analyst numbers to support ONI's intelligence assessment role.**

4.65 **We also recommend that, as the focal point in the provision of intelligence advice to the Prime Minister, ONI be responsible for preparing a morning Daily Brief for the Prime Minister on intelligence issues of significance.** The Brief would co-ordinate topical reporting by collection agencies and provide more detailed ONI perspectives on current and emerging issues than that currently provided by ONA in its daily reports to the Prime Minister.

4.66 Contestability is a critical input to quality intelligence assessments. In our view, this could be promoted in relation to ONI assessment products in a number of ways. Accordingly, **we recommend that an ONI Assessment Consultation Board be established, that it be chaired by DG ONI, and that it consist of senior leaders from ONI, other intelligence agencies and relevant policy departments as well as individuals from business, non-government organisations, universities and think-tanks who can add relevant perspectives to intelligence assessment matters.** The Board should meet three times a year and address issues of current and emerging intelligence priorities as well as ways in which intelligence assessments could be assisted by non-government input.

4.67 The current National Assessments Board considers National Assessments made by ONA and comprises relevant senior officers, including from PM&C, DFAT, the Department of Defence and a member of the ADF. The National Assessments Board should continue to operate in relation to ONI National Assessments in the same way as it has in relation to ONA.

4.68 **We also recommend that ONI develop a more intensive and substantive program of interaction with experts outside government to inform assessments.** Individuals with expert knowledge or deep experience in relation to current and emerging issues of importance in intelligence assessment should be identified by the ONI Assessment Consultation Board. Necessary security clearances should be processed as required.

And, where appropriate and value-adding, relevant experts should be consulted in the development of assessments and in the testing of conclusions.

4.69 In the event that there are major differences of perspective with external experts, such differences should be reflected in ONI assessments and the reasons for ONI's particular viewpoint should be clearly spelt out. More generally, ONI assessments should more often outline alternative points of view on contentious assessment issues. Explaining in more detail why ONI has arrived at a particular judgment, for example if secret intelligence has provided a decisive insight, would help policy makers to assess the weight they give to ONI judgments compared to competing views from outside the intelligence community. Over time, it would also help policy makers develop further their understanding of the role and limitations of intelligence.

THE PLACE OF ASD IN THE ARCHITECTURE OF THE INTELLIGENCE COMMUNITY

4.70 In addition to the establishment of ONI, the second major structural change we recommend in this Chapter relates to the place of ASD in the architecture of the intelligence community. ASD has evolved from a primarily Defence signals collection agency after World War II to become Australia's national signals intelligence authority conducting intelligence, military, cyber security and effects operations through the application of advanced technologies. ASD's support to ADF military operations is indispensable, and will remain so. But ASD is now a genuinely national asset, playing a much broader role than that defined by its previously exclusive Defence focus. This is highlighted in its current additional responsibilities as a national source of information assurance and cyber security. There are also strong and growing interdependencies between ASD and other intelligence agencies.

4.71 Previous intelligence reviews have examined the place of ASD. The 2004 Flood Report found that DSD (now ASD) was appropriately positioned in Defence and did not recommend any change to its place within the intelligence architecture.[14] The Report did so primarily on the basis of the importance of signals intelligence (SIGINT) support to military operations and the necessity of maintaining the closest possible links between DSD and the ADF.

14 Flood, op cit., p.136.

4.72 ASD's roles, responsibilities and interactions within government and with the non-government sector have broadened considerably since 2004. In these new circumstances, our view is ASD would be better able to fulfil its vital responsibilities to the ADF, and would more effectively carry out its broader national role, through a structure that provides it with more autonomy within the Defence portfolio. We have reached this view in light of the range of ASD's Defence support role and broader national responsibilities, the operational, workforce and other challenges that ASD faces (highlighted in Chapter 3), the role of SIGINT as a critical enabler for other intelligence agencies and ASD's evolution as an independent intelligence service.

4.73 Our main focus in relation to this issue has been on how ASD is best structured to meet the range of its ongoing and evolving support for the ADF, its expanding interactions with other intelligence agencies and its developing national cyber security responsibilities. In our view, ASD will be better placed if it remains in the Defence portfolio but if it is in a position to operate with greater independence from the Department's requirements, especially those in relation to its capacity to recruit, retain, train, develop and remunerate its specialist staff.

4.74 For ASD, the option of continuing to operate within the Department of Defence's employment framework, even with some specific exemptions, is not the most effective way forward. It would increase the risk of losing additional critical talent, skills and capabilities. ASD needs to be more in control of its own destiny.

4.75 We strongly support the maintenance of a highly interactive and mutually beneficial relationship between the ADF and ASD, especially in relation to the significant enablers that Defence provides to ASD and the provision of ADF personnel to ASD. In our assessment, the pace and intensity of ADF operations over the past decade, in particular, have resulted in shared capabilities, connections and experience becoming more firmly entrenched in the ADF and ASD.

4.76 In our view, it is neither feasible nor desirable to move ASD out of the Defence portfolio. Alternative arrangements work well with some of the Five Eyes partners. For example, ASD's UK counterpart, GCHQ, is positioned within the portfolio of the Foreign and Commonwealth Office. Nonetheless, it is clear to us that maintaining the close connection between ASD and the broader Defence Organisation in Australia is critically important in the national interest. But it is also clear to us that this relationship between the ADF and ASD can be continued and further

strengthened through a structure that gives ASD greater independence in the Defence portfolio.

4.77 Accordingly, **we recommend that ASD be made a statutory authority within the Defence portfolio reporting directly to the Minister for Defence, and that the Head of ASD be appointed at a level of seniority equivalent to the Directors-General of ASIO and ASIS.** Relevant legislative change should reaffirm and strengthen ASD's priority role to provide support to military operations for the ADF. It should also explicitly endorse its position as the national information and cyber security authority, including its role in combating cyber crime and providing advice to industry on cyber security matters.

4.78 In relation to ASD's role to support military operations, we consider the existing organisational arrangements that underpin the role should remain intact and be strengthened. Those arrangements are proven to be effective. They enable the skill-sets of ASD's military and civilian staff to be combined to optimise the benefit to the ADF. And they remove the risk of duplicating investments in core capabilities, and competing for scarce skill-sets, that would arise if the ADF were to establish its own strategic level signals intelligence branch. Furthermore, the existing arrangements ensure that cryptologic support to the ADF operates with the appropriate powers and immunities of the ISA, and that the function is subject to the oversight of the Inspector-General of Intelligence and Security and the Parliamentary Joint Committee on Intelligence and Security. Therefore, **we recommend the existing organisational arrangements that integrate the support to military operations capability within ASD be reaffirmed and strengthened.** To ensure ASD supports Defence across the range of war fighting operations and capability delivery, **we also recommend that a senior military officer be appointed as the principal ASD Deputy Director at a rank commensurate with the responsibilities and accountabilities of the role.** This officer would have access to the full suite of ASD enabling capabilities to support Defence outcomes, and would also ensure the command and welfare of ADF members seconded to ASD.

4.79 In our view, ASD's transition from being a part of the Department of Defence to a statutory authority within the Defence portfolio is necessary and desirable. It would also be complex and challenging. ASD needs to be set up for success as a statutory authority. Accordingly, **we recommend that a dedicated joint ASD–Defence team be established to manage ASD's transition to a statutory authority, drawing on relevant expertise within and outside of government. The National Security**

Committee of Cabinet should oversee the transition and receive regular reports from the transition team.

4.80 ASD as a statutory authority would need regular ongoing investment in underlying technology. Existing ASD capability projects and their associated funding should remain within Defence's Integrated Investment Program during ASD's transition to a statutory authority, with future funding requests being subject to national security decision-making processes. In our view, the transition of ASD would also present a unique opportunity to create a four-year Intelligence Capability Investment Plan (ICIP) for the NIC as a whole, which would provide government with greater certainty regarding the NIC's capability investment requirements. DG ONI would have a critical role to play in co-ordinating the ICIP consistent with the role that he or she would play in intelligence community-wide resource co-ordination. This issue is addressed in more detail in Chapter 5.

THE PLACE OF THE AUSTRALIAN GEOSPATIAL-INTELLIGENCE ORGANISATION (AGO) IN THE ARCHITECTURE OF THE INTELLIGENCE COMMUNITY

4.81 In coming to our recommendations on ASD, we were conscious that the issue of the balance between Defence and whole-of-Government responsibilities also arises in relation to AGO. However, there are strong reasons for AGO to remain an integrated component within the Department of Defence. In accordance with the recommendations of the First Principles Review of Defence, AGO is leading the establishment of a unified geospatial enterprise in Defence. Building on the successful integration of Army topographical mapping and Air Force kinetic targeting functions into AGO's predecessor organisations in the mid-1990s and mid-2000s respectively, Navy hydrographic services and Air Force aeronautical charting functions merged with AGO in 2016. AGO will also build more effective linkages with other government agencies such as Geoscience Australia and the Bureau of Meteorology.

4.82 These more recent mergers will significantly enhance AGO's ability to support its growing base of customers in Defence and across the broader national security community. Nonetheless, support to Defence will need to be carefully balanced with AGO's role in the national intelligence space. Geospatial intelligence is playing an increasingly important role in addressing national security issues, especially in relation to counter-terrorism, and close partnerships will therefore be essential going forward.

4.83 We assess that AGO will be well placed to support both its Defence and broader national security customers from its current position as an agency that is integrated into Defence. Furthermore, we are mindful of the disproportionately large administrative overheads that are often involved with smaller statutory authorities. Accordingly, we consider there should be no change to AGO's place in the architecture of the intelligence community.

[This page intentionally left blank]

CHAPTER 5: CAPABILITY AND RESOURCING FRAMEWORKS

5.1 This Chapter addresses the following two parts of the Review's Terms of Reference: "*whether capability gaps, including technological, are emerging and how these might be met, noting potential efficiencies and that any new proposals would need to be consistent with the Government's overall fiscal strategy*"; and "*whether the AIC is resourced appropriately, including to ensure the right balance of resources across the AIC and that agency resources are properly matched against national security priorities, and the impact of the efficiency dividend.*"

5.2 Chapters 1 and 2 outlined how a transforming international system, extremism with global reach and the security consequences of accelerating technological change are shaping Australia's national security environment, and increasing the expectations placed upon the intelligence community. The Submissions we received from the intelligence agencies made it clear that those increasing expectations are being felt most strongly in the diversity of issues they are now expected to address. There is a challenge for agencies to maintain an appropriate level of coverage across their broadening remit.

5.3 In this Chapter we recommend two categories of initiatives to address this challenge. In the first category, we recommend initiatives relating to specific capability issues. These aim to:

- improve the ability of the intelligence community to attract and retain its workforce;
- improve capabilities for the intelligence community to share and collaboratively analyse data;
- intensify the intelligence community's engagement with the Australian science and technology community, and with industry more generally, to facilitate innovation and the development of new capability; and
- better inform government decision-making on resourcing for issues of ongoing importance compared with more urgent priorities.

5.4 In the second category, we recommend initiatives relating to the resourcing framework for the intelligence community to:

- support the development of shared capabilities; and

- assist government in making informed decisions on trade-offs between competing priorities.

STRENGTHENING CAPABILITY

Intelligence Workforce Issues

5.5 There are diverse challenges in developing and maintaining a suitably skilled intelligence workforce staffed by appropriately qualified and highly skilled people. Potential recruits are dissuaded by a range of factors. Some are deterred by the length of time that security clearances take and by the intrusiveness of those clearances. Others are put off by salary levels. Others again judge there are more diversified careers with greater job mobility outside the intelligence community.

5.6 Recruiting and retaining people with skills in Science, Technology, Engineering and Mathematics (STEM) disciplines is particularly challenging as a result of the national shortage of skills in this area as well as competition from both the private sector and other areas of government. As data analytics become an increasingly important source of intelligence, STEM skills will be needed in a wider segment of the intelligence workforce including in assessment areas. In our view, the problem is likely to grow as demand from the private sector increases.

5.7 An intense focus on meeting the intelligence community's need for staff with advanced technical skills should be complemented by innovative programs to develop leaders within the intelligence community. Ultimately an intelligence agency (and community) will thrive when good leadership is combined with knowledgeable, skilled and highly motivated intelligence professionals. We judge the intelligence community would benefit from greater investment in the development of its current and future leaders. This should include community-wide learning and development options, but also the establishment of career pathways that allow the community to develop a future cohort of intelligence leaders. This focus should include expanding community-wide leadership development programs, identifying and managing talented leaders in the intelligence community, encouraging movement of these staff across the intelligence and policy agencies (and in some cases private industry), recognising their leadership skills as a community enabler and not just as an agency-based one, and pursuing the objective that leaders developed through such programs will reach the intelligence community's senior leadership levels.

5.8 We judge there would also be value in providing greater flexibility for members of the intelligence community to broaden their experience through employment in the policy community or non-government sector. This would help to improve considerably the flow of officers back into the intelligence community after time away. It would also give intelligence staff valuable opportunities to further their own development and diversification as intelligence professionals and leaders.

5.9 Since the *Independent Review of the Intelligence Community* in 2011 there has been considerable progress in establishing community-wide training, including in analytic skills and tradecraft. Nonetheless, there is significant scope to expand this work and leverage existing agency-based training into a wider community approach.

5.10 We also noted concerns about the need for greater diversity of the workforce in some areas of the intelligence community. This lack of diversity affects adversely the ability to attract specialist skills and the breadth of perspectives brought to bear on assessment issues.

5.11 These issues highlight the need for a strategic approach to the development of the intelligence community's workforce and for dedicated funding to support initiatives such as those noted in paragraphs 5.7 and 5.8. The approach should aim to improve the recruitment, retention and diversity of staff, ensure scarce skills are balanced appropriately across intelligence agencies, facilitate movement between agencies as well as to and from the private sector, and establish training for staff to ensure they are 'data-ready'. In particular, it should guard against the 'cannibalisation' of staff within the intelligence community in ways that degrade the capabilities of specific agencies, especially smaller ones.

5.12 **We recommend the Office of National Intelligence (ONI) be responsible for developing and overseeing the implementation of a strategic approach to the development of the National Intelligence Community (NIC) workforce as part of its intelligence enterprise management responsibilities.**

Security Clearances

5.13 The length of time taken by the Australian Government Security Vetting Agency (AGSVA) to complete Top Secret (Positive Vetting) (TS(PV)) security clearances is exacerbating the intelligence community's existing workforce challenges. At the peak of the backlog, AGSVA clearances took more than 18 months on average to process,

substantially longer than some AIC agencies that undertake their own TS(PV) clearances. As AGSVA not only processes clearances for Defence but also for a number of other agencies, including those in the wider intelligence community, the lengthy timeframes similarly have an impact on those agencies – namely the Department of Immigration and Border Protection (DIBP), the Australian Criminal Intelligence Commission (ACIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC). They also affect the Office of the Inspector-General of Intelligence and Security (IGIS).

5.14 The leadership of AGSVA is clearly aware that the time it currently takes to process a TS(PV) is unacceptably long, and is giving a high priority to a remediation program to address this. It is also of critical importance that the clearance process remains robust. We consider that it would be prudent to increase the Australian Security Intelligence Organisation's (ASIO) involvement in the clearance process, and at an earlier stage than the existing security check it undertakes. Accordingly, **we recommend that ASIO receive additional resourcing to allow it to second staff to AGSVA as soon as possible. We also recommend that the situation with AGSVA TS(PV) clearances be reviewed in early 2018 to allow time for the current remediation program to have effect. If processing times still exceed six months, alternative options for TS(PV) clearances should be explored.** The options should include decentralising the responsibility for TS(PV) clearances to individual intelligence agencies, and giving responsibility to ASIO for TS(PV) clearances for the staff of the Defence Intelligence Organisation (DIO), Australian Signals Directorate (ASD), Australian Geospatial-Intelligence Organisation (AGO), the Australian Federal Police (AFP), IGIS, DIBP, ACIC and AUSTRAC. We recognise that ASIO, the Australian Secret Intelligence Service (ASIS) and the Office of National Assessments (ONA) each have robust TS(PV) clearance processes that meet their needs. Those processes should remain unchanged.

Data Sharing and Collaborative Analysis

5.15 In our view, data analytics and connectivity are vital for the future effectiveness and efficiency of the intelligence community. Agencies are increasingly shifting from 'monitoring' narrowly defined target communications to 'mining' multiple data sets for insights, indicators and warnings, while at the same time respecting the rights to privacy of Australian persons.

5.16 International experience has shown common ICT infrastructure that facilitates the secure sharing of information and analytical resources is crucial for wider integration efforts, and also generates long-term savings for relevant agencies. A particularly instructive example has been the role of the US Director of National Intelligence in driving plans to establish a common intelligence community information technology platform. This initiative is moving the US intelligence community away from individual agency-based ICT architecture and for the first time establishing a common intelligence ICT infrastructure, further encouraging the US intelligence community towards a more enterprise-based approach.[15]

5.17 Although intelligence agencies recognise the importance and scale of the challenges, and are taking some steps to respond to and anticipate developments, stronger cross-agency approaches are required to deliver all of what will be needed. Chapter 3 outlined the value of improving secure ICT connectivity between intelligence, policy and law enforcement agencies. There are opportunities to better leverage the data holdings of individual agencies, improve connectivity between agency datasets to facilitate cross-agency collaboration, and distribute advanced analytics capabilities more evenly across agencies.

5.18 We see considerable advantage in establishing a computing environment for the intelligence community to enable sharing of data and collaborative analysis. This must be done in ways that respect the rights to privacy of Australians. In terms of improving connectivity with law enforcement agencies, proposals should take account of the National Criminal Intelligence System being piloted by the ACIC.[16]

5.19 In Chapter 4 we recommended that ONI be given responsibility for leading and co-ordinating data management and ICT connectivity initiatives across the NIC. In addition, **we recommend that data analytics and ICT connectivity, including the establishment of an intelligence community computing environment in which technical barriers to collaboration are minimised, be one of the highest priorities of a more structured approach to technological change and the funding of joint capabilities.** The development of these capabilities would need to be consistent with ONI being responsible for a central repository of open source data and a common library of open source analytic tools and techniques discussed in Chapter 4. Approaches to technological change and the funding of joint capabilities are described further in the following sections.

15 See, e.g., https://www.dni.gov/files/documents/IC%20ITE%20Fact%20Sheet.pdf.
16 See, e.g., https://www.acic.gov.au/our-services/national-criminal-intelligence-system.

Science, Technology and Innovation Strategies

5.20 Capitalising on opportunities created by scientific advances and technological change will become increasingly important for the capabilities of Australia's intelligence agencies. In this section, we focus on ways in which interaction with the broader science and technology community can secure capability advantages for Australia's intelligence agencies.

5.21 Some of the technological advantages from which Australia's intelligence agencies have benefited are being eroded by the globalisation of leading-edge technology developed outside government and commercialised internationally. While there are important areas of excellence and unique capabilities developed by Australian and other partner intelligence agencies, the rapid pace of technological change and commercialisation has diminished some of their comparative advantages.

5.22 In Chapters 1 and 2 we highlighted existing and emerging technological challenges that are most pressing for the intelligence community. They include the extraction of value from the vast and increasing volume of open source information and addressing the realities of increasingly prevalent high-quality encryption.

5.23 These challenges relate to technological developments that are relevant to the public and private sectors, though often for different reasons. Responses to these challenges are therefore being driven both within and outside government. It is critical that Australia's intelligence agencies interact as productively as possible with the broader science and technology community if they are to retain their comparative advantage in pursuit of Australian national interests.

5.24 There have been some important initiatives by agencies to enhance appropriate and productive exchanges on science and technology issues with publicly funded research agencies, academia and industry within Australia. Such outreach is useful and highly desirable, but in our view Australian intelligence interests generally would benefit significantly if this engagement was more systematic and better co-ordinated.

5.25 **We recommend a more structured approach to the NIC's responses to technological change led by ONI with a high priority given to:**

a) **establishing a National Intelligence Community Science and Technology Advisory Board;**

b) **creating a National Intelligence Community Innovation Fund to support the development of prototypes for transitioning research outcomes into operational systems; and**

c) **supporting a National Intelligence Community Innovation Hub to facilitate ways in which government, industry and academia could come together to discuss capability needs and solutions and to create new linkages.** One such way would be an annual conference focused on a particular theme, such as data analytics.

Supporting Important Long-Term Intelligence Priorities

5.26 An important issue we addressed during this Review was the challenge posed for the agencies by the need to address immediate and urgent needs such as counter-terrorism, supporting military operations and countering people smuggling while still maintaining focus on long-term issues that are of enduring importance to Australia. In our view, resourcing will need to increase for some priorities of ongoing importance. But we recognise that simply allocating more money to such priorities will not inevitably result in a commensurate improvement in intelligence outcomes. **We recommend that proposals for new funding for important long-term intelligence capability initiatives be assessed against agreed principles, including:**

- **Any additional funding should be focused primarily on Australia's own intelligence needs.** Proposals for such funding should confirm that the intelligence product to be provided through the additional funding is not duplicating information available from other sources.
- **Proposals for additional intelligence funding also need to specify the likely return on investment.** They should explain what measurable outcomes the proposed funding would achieve and the likelihood of achieving them. Objectives would need to be focused on outcomes and not simply on inputs. The funding proposal would need to specify how the additional funding would contribute (in a measurable way) to the performance of the NIC against the agreed priorities.
- **Funding should be phased over time and be subject to periodic review against objectives.** Funding proposals should provide benchmarks against which their progress could be measured, including indicators of both achievement and early warning signs of shortfalls. Outcomes of such reviews could include variations to

future funding, continuation of a lapsing program or identifying unmet needs from a terminating program. These reviews would be prepared by ONI, in consultation with relevant agencies and engaging independent external expertise as appropriate. The final report should be considered by the National Security Committee of Cabinet.

5.27 These principles are designed to balance the need for new resourcing with a greater degree of accountability and transparency on how agencies intend to use the additional resourcing to produce measurable results that advance Australia's national intelligence interests.

RESOURCING FRAMEWORKS: A NEW APPROACH

5.28 We consider that changes to the resourcing framework that applies to the intelligence agencies would assist in addressing the capability challenges we have outlined in the preceding section. We propose two initiatives – the first designed to support the development of shared capabilities and the second to assist government in making informed decisions on trade-offs between competing priorities.

A Joint Capability Fund

5.29 The enhancement of many of the capabilities addressed in the preceding section can be achieved most effectively through NIC-wide initiatives. However there is currently little incentive for individual agencies to propose such initiatives. Rather, the current funding framework attracts proposals that primarily address the needs of single agencies. This can result either in community-wide capabilities not being developed, or in capabilities being inefficiently duplicated among agencies.

5.30 Experience in the United States and the United Kingdom has shown that financial incentives for agencies to develop joint capabilities are not only highly effective but can also forge closer working relationships among agencies leading to more integrated approaches to national intelligence priorities.

5.31 **We recommend a Joint Capability Fund (JCF) for the NIC be established. The JCF would be administered by ONI.** It would only be available for developing capabilities that address the needs of more than one agency, and ideally all ten intelligence agencies that support national security. By resourcing proposals that have demonstrable benefits for multiple agencies, the JCF would also facilitate greater integration at a working level among intelligence community agencies. The JCF should

not be drawn on for proposals that only develop capability for a single agency.

5.32 The JCF should be used to finance the type of NIC cross-agency projects referred to previously in this Chapter, including:

- strategic workforce planning related to training, development and facilitating movement among the intelligence community, policy departments and the private sector;
- ICT capabilities to facilitate sharing of data and analytic capabilities;
- a National Intelligence Community Innovation Fund;
- a National Intelligence Community Innovation Hub; and
- a National Intelligence Community Science and Technology Advisory Board.

5.33 **We recommend that the total amount in the JCF be equivalent to the Efficiency Dividend levied on the intelligence agencies.** This proposal has similarities with the 2017–18 Budget 'Public Service Modernisation Fund' measures, which will invest $500 million raised by the Efficiency Dividend in initiatives to modernise, transform and enhance the productivity of the Australian Public Service.

5.34 Our recommendation that the JCF be equivalent to the Efficiency Dividend levied on the agencies obviously requires the Efficiency Dividend to continue to be applied to the intelligence community.[17] While the Efficiency Dividend constitutes a relatively small percentage of the annual budgets of intelligence agencies, its cumulative impact over a number of years has been significant.

5.35 To meet the ongoing requirements of the Efficiency Dividend, we assess that sustainable efficiencies will increasingly need to be achieved by shifting the focus from efficiencies generated within individual agencies to an approach that seeks to achieve savings across the agencies of the NIC. This approach would generate new opportunities for greater sharing of corporate services, more effectively co-ordinated procurement arrangements, standardisation of administrative processes and other initiatives.

17 The three Defence intelligence agencies operate within the separate savings disciplines imposed on the Defence Organisation and are therefore exempt from the broader government Efficiency Dividend. ONA and the Office of the IGIS have been granted an exemption since 2015–16 because of the disproportionate effect the Efficiency Dividend was having on such small agencies.

5.36 Another argument presented against the Efficiency Dividend is that its implementation has created a degree of volatility that makes it difficult for agencies to undertake forward planning. The Efficiency Dividend can be varied annually, depending on the Government's need to re-direct funding to areas of higher priority. Furthermore, one-off Efficiency Dividends are also sometimes imposed in addition to the annual Efficiency Dividend. This can occur, for example, at the mid-year updates to the Budget.

5.37 We agree that planning for the development of capabilities would benefit from greater certainty about future levels of funding. However, we do not consider the removal of the Efficiency Dividend is necessary. The desirable level of certainty in future funding requires a more substantial reform of the agencies' resourcing and capability planning framework. We address this issue in detail and make recommendations on a new approach below.

The Operation of the Joint Capability Fund

5.38 We envisage that all ten of Australia's intelligence agencies which support national security would benefit from the investments that would be made through the JCF. In our view, therefore, the principle should be that as many agencies as possible contribute through the Efficiency Dividend to the JCF. The contribution from the AFP and DIBP would only be that component of their Efficiency Dividend that relates to their intelligence functions. However, since AGO and DIO would continue to be subject to Defence's internal savings measures, we propose they should remain exempt from the Efficiency Dividend and therefore from contributing to the JCF. But, because of their roles within the wider intelligence community, they should still be able to benefit from the JCF and make proposals for its use. The Office of the IGIS would remain exempt from the Efficiency Dividend.

5.39 **We recommend the following changes to the application of the Efficiency Dividend to the intelligence agencies**:

- **The Efficiency Dividend be applied to 100 per cent of ASD's funding with effect two years after ASD's establishment as a statutory authority.** If our recommendation for ASD to be established as a statutory authority within the Defence portfolio is accepted (Chapter 4), ASD would no longer be subject to Defence's internal savings measures. In these circumstances, the Efficiency Dividend would provide an important incentive for continued efficiencies within ASD and in its operations as part of the NIC. Introducing

the Efficiency Dividend two years after ASD's establishment as a statutory authority would provide a period in which the costs of transition to a statutory authority (particularly in relation to accounting for services received from Defence such as ADF personnel, ICT infrastructure and other shared services) would be accommodated prior to the application of the Efficiency Dividend. For planning purposes only, we have anticipated the date of application of the Efficiency Dividend to ASD to be in 2020–21.

- **The Efficiency Dividend be applied to 100 per cent of ONI's funding with effect two years after ONI's establishment as a statutory authority.** ONI would be a larger organisation than the current ONA, and in our view would not warrant exemption from the Efficiency Dividend on the basis of size. As with ASD, introducing the Efficiency Dividend two years after ONI's establishment would enable the costs of establishing ONI to be finalised before applying the Efficiency Dividend. For planning purposes only, we have anticipated the date of application of the Efficiency Dividend to ONI to be in 2020–21.

5.40 Based on the assumptions above, the JCF would accumulate around $370m over the five years from 2017–18. That amount is the total amount of the Efficiency Dividend planned to be levied on the relevant intelligence agencies.

5.41 New Policy Proposals (NPPs) for committing resources from the JCF would be developed through ONI and require National Security Committee of Cabinet approval. Giving ONI responsibility for co-ordinating the proposals and administering the JCF would provide it with important influence in shaping greater integration among the intelligence agencies.

5.42 The JCF would only partially fund the future capability needs of the intelligence community. Larger projects with the potential to more closely integrate the intelligence community and produce ongoing efficiencies (for example, improved ICT connectivity) would require additional funding to that able to be provided through the JCF. Such additional funding would need to be sought through NPPs as part of the normal Budget process. The JCF could be used as a partial offset for such NPPs.

A More Strategic Approach to Future Funding – An Intelligence Capability Investment Plan

5.43 We consider that the projects proposed to be financed from the JCF should be presented to Government as part of a comprehensive plan

of investment that enables government to make well-informed decisions about the relative level of investment to meet urgent priorities while still maintaining adequate levels of capability in regard to issues of enduring importance.

5.44 Part of the challenge in securing funding for ongoing and longer-term priorities relates to the difficulty of quantifying the impact of any shortfalls. Moreover, many of the capabilities needed to address such shortfalls can take years to develop. A more strategic approach to fiscal forward planning for intelligence agencies than is supported by current budgetary processes is needed. We assess there could be improvements made in how trade-offs between the funding of urgent priorities and longer-term requirements in capability are presented to government, as well as in how the funding of such proposals is anticipated and factored into the Forward Estimates.

5.45 Recognising that intelligence is now significantly a technology-driven business requiring regular investment in new capabilities, we consider there would be great benefit from a co-ordinated approach to strategic investment planning by the intelligence community to develop effective and efficient capabilities that can serve Australia's national security requirements into the future. This would also provide the National Security Committee of Cabinet with a more holistic forecast of the future funding needs of the intelligence community than is currently available, and create a new mechanism for government approval of intelligence capability expenditure.

5.46 **We recommend an Intelligence Capability Investment Plan (ICIP) be established that identifies the major capability projects that agencies seek agreement to commence over the period of the Forward Estimates, and that the Director-General ONI (DG ONI) prepare the ICIP annually for consideration by the National Security Committee of Cabinet, noting that the ICIP should be presented in conjunction with a comprehensive overview of the NIC's existing funding and future commitments.**

5.47 An ICIP for Australia's intelligence agencies would have some parallels with Defence's Integrated Investment Program (DIIP) which aims, in part, to give government improved visibility of Defence's capability planning processes and the risks associated with projects. The DIIP recognises that periodic investment in the modernisation of capabilities and enabling elements is unavoidable and should be factored into the Budget Forward Estimates. In addition to military capabilities, the DIIP also includes

the required investments in enabling elements, such as equipment, infrastructure, ICT, science and technology, and workforce.

5.48 The ICIP would contain intelligence capability proposals (above a $20 million threshold) which are joint capability proposals, cross-portfolio proposals or standalone proposals from a single intelligence agency. Ministers would be asked to consider a preliminary outline of the business case for each new proposal which would articulate the need for it, the details of outcomes to be delivered, the projected intelligence benefit or result as well as the indicative total cost and phasing, and the associated risks. The ICIP would therefore give Ministers visibility of all major intelligence capability investments or programs that would commence within the Forward Estimates period.

5.49 In taking the ICIP forward, DG ONI would advise Ministers which proposals could or could not be funded from within the existing resources of the NIC or from the JCF. Where proposals could not be funded from existing resources or the JCF, the ICIP would give Ministers an early opportunity to indicate which proposals should be developed further as fully fledged NPPs seeking funding from the Budget. For proposals considered in this way, Ministers could also make an early judgment if the indicative funds requested should be included in the Forward Estimates for the agencies, or reflected in the Contingency Reserve. In proposing this new mechanism, our objective is to ensure that intelligence agencies are able to bring forward well-considered NPPs for approval and that Ministers are able to make an early decision on whether financial offsets would be needed for subsequent consideration.

5.50 Over time the ICIP would include proposals to address intelligence challenges, modernise agency business processes, build workforce capabilities, address requirements for new agency premises, and develop non-discretionary capabilities such as ICT and physical infrastructure upgrades that may require supplementary funds to implement.

5.51 The structural changes we proposed in Chapter 4 relating to ASD provide a useful starting point for the creation of the ICIP. In our view, the ICIP would in time include all ASD-led projects that would otherwise have been part of the DIIP. These projects would be moved from the Department of Defence to ASD as part of ASD becoming a statutory authority. Accordingly, **we recommend the ICIP should include the projects which ASD has in the DIIP, and that the associated funding be transferred from the Defence budget to ASD after it transitions to a**

statutory authority. Recognising there would need to be a period of transition, we also recommend that current phases of ASD's DIIP funding should continue to be administered by the Department of Defence, and that over time, later phases of projects, as well as their replacements and future projects, should move into the ICIP.

5.52 To impose a discipline on the presentation of the ICIP, we consider it should be developed within a defined funding envelope. We note that the projected funding for the NIC over the next five years is flat, compared to significant real growth over the last five years. In our view, a more realistic level of funding is needed to enable the NIC to address the intelligence challenges we have identified in this Chapter.

5.53 We recognise that the ICIP will develop over several years. **We recommend that, in its first iteration, the ICIP be presented to government with options for overall funding envelopes based on NIC funding and indexed at 1.5 and 3 per cent real growth per year, with effect from 2018–19.** The presentation of these options would allow the Government to make a more informed decision about trade-offs between intelligence challenges, affordable levels of funding and other priorities.

5.54 The establishment of the ICIP would also further strengthen the ability of ONI to integrate the efforts of intelligence agencies in meeting the needs and priorities of government. The experience of Australia's international partners has been that governments recognise the value of co-ordinated proposals for improved integration across an intelligence community. There is no reason for Australia to be an exception.

CONCLUSION

5.55 The JCF and ICIP proposed in this Chapter would greatly enhance co-ordinated strategic planning across the intelligence community under the leadership of the ONI. However, these two proposals will not remove the need for agencies to bring forward NPPs outside of these processes if they require additional funding to meet operational requirements that arise at short notice. Such additional funding proposals should include an explanation of why they could not be resourced through the JCF or processed through the ICIP.

CHAPTER 6: LEGISLATION

6.1 This Chapter addresses the Review's Terms of Reference in relation to *"whether legislative changes are needed, including to the Intelligence Services Act 2001."*

6.2 Australia's intelligence community is governed by a detailed legislative framework which sets out the functions, powers, immunities, administrative arrangements and oversight frameworks for the community across a number of Acts. Importantly, this framework distinguishes between the collection of intelligence by agencies inside and outside Australia.

6.3 The *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) outlines the functions and powers of, and administrative arrangements for, ASIO. Central to ASIO's role is the definition of 'security' that the Act sets out. The ASIO Act includes a detailed framework governing the collection of intelligence and gives ASIO clearly enumerated special powers to engage in conduct within Australia that would otherwise be illegal under Australian law, with protections for Australian citizens, residents and persons in Australia. The ASIO Act provides that ASIO's responsibility for security extends geographically beyond Australia and includes Australia's security obligations to other countries.

6.4 The *Intelligence Services Act 2001* (ISA) sets out the functions, immunities, administrative arrangements and Ministerial oversight frameworks for the Australian Secret Intelligence Service (ASIS), the Australian Geospatial-Intelligence Organisation (AGO) and the Australian Signals Directorate (ASD) (the ISA agencies). It also establishes the Parliamentary Joint Committee on Intelligence and Security (PJCIS). Recognising that agencies operating overseas should have greater flexibility, and that Australia lacks effective jurisdiction or control over people or events in other countries, the ISA contains broad legal authorities for ASIS, ASD and AGO to obtain intelligence about people and organisations outside Australia. The ISA also contains protections for Australians as ISA agencies do at times need to produce (duly authorised) intelligence on Australian persons to meet their responsibilities.

6.5 The *Telecommunications (Interception and Access) Act 1979* (TIA Act) includes a warrant regime that enables Commonwealth, State and Territory intelligence and law enforcement agencies to intercept communications passing over the Australian telecommunications network.

6.6 Additional legislation relevant to the intelligence community includes:

- the *Office of National Assessments Act 1977* (ONA Act) which establishes ONA as an independent assessment agency with a co-ordination and evaluation role;
- the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) which establishes the functions and powers of the IGIS, an important accountability and oversight mechanism for intelligence agencies (which is considered in Chapter 7);
- the *Crimes Act 1914* which, among other provisions, contains a uniform Commonwealth, State and Territory assumed identities framework, including assumed identities powers for ASIO and ASIS;
- the *Criminal Code Act 1995* (the Criminal Code) which, among other provisions, contains immunities for AGO, ASD and ASIS officers and agents to undertake computer-related acts outside Australia and preparatory acts inside Australia;
- the *National Security Information (Criminal and Civil Proceedings) Act 2004* which contains a range of means by which law enforcement agencies and prosecutors can seek to protect disclosure of information relating to highly sensitive capabilities in court proceedings; and
- the *Telecommunications Act 1997* which contains a range of key provisions that reflect the importance of the telecommunications network to national security.

ASSESSING CURRENT LEGISLATIVE ARRANGEMENTS

6.7 In the course of this Review, we received differing views on whether the legislative framework in which the Australian intelligence agencies operate remains appropriate to the changing security environment.

6.8 The Review heard arguments that a common legislative framework should be developed to govern the activities of Australian intelligence agencies. According to this view, a common legislative framework would provide greater clarity in functions and enable more effective co-operation and co-ordination between activities within and outside

Australia. This is the general approach taken in the United Kingdom,[18] and New Zealand has recently passed a single Act to govern the activities of its intelligence agencies.[19]

6.9 Australian intelligence legislation has been the subject of numerous amendments over many years. In our view, incremental and piecemeal reforms have lent an ad hoc character to some of the Acts. In addition, warrant thresholds across the various Acts – in particular the ASIO Act, ISA and the TIA Act – employ slightly different tests. The PJCIS has recommended the TIA Act, which it considered to be "so complex as to be opaque in a number of areas", be comprehensively reviewed.[20] Different thresholds can cause uncertainty for agencies in the performance of their responsibilities. Furthermore, frameworks to protect disclosure of sensitive capabilities in legal proceedings are coming under pressure due to increasing use of evidence derived from such capabilities.

6.10 Australia's intelligence community needs to operate under legislation containing coherent and consistent provisions that address the challenges of the contemporary threat environment. It must also retain explicit privacy protections for Australians which assist in securing ongoing public support for the powers entrusted to intelligence agencies. Such protections must be balanced with contemporary expectations of privacy.

6.11 The Submissions received by the Review and inquiries we conducted led us to conclude that a comprehensive review of the legal framework under which Australia's intelligence agencies operate would be timely. A detailed and comprehensive review and re-evaluation of the legislative framework would help to harmonise and modernise the legislation that establishes and confers powers on Australia's intelligence agencies and the major independent oversight bodies. Such a review would be a significant, complex and lengthy undertaking requiring thorough and in-depth examination, analysis and assessment of the current legislative framework and the interaction between various component Acts. In addition, consideration of the TIA Act would necessitate close

18 The common legislative framework applicable to all intrusive activities undertaken by the United Kingdom's intelligence agencies is set out in the *Regulation of Investigatory Powers Act 2000* and the *Investigatory Powers Act 2016.* The functions of the collection agencies within the United Kingdom's intelligence community are set out in the *Security Services Act 1989* (for the Security Service or MI5) and the *Intelligence Services Act 1994* (for the Secret Intelligence Service or MI6 and the Government Communications Headquarters).

19 The *Intelligence and Security Act 2017* was recently passed by the New Zealand Parliament and was given Royal Assent in March 2017. The bulk of its provisions come into force in September 2017, being six months after the date of Royal Assent.

20 PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* May 2013, p.9.

engagement with State and Territory law enforcement bodies which also exercise authority under this Act, to ensure their operational requirements are considered in making any recommendations for reform.

6.12 **We recommend a comprehensive review of the Acts governing Australia's intelligence community be undertaken to ensure agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians.** The review should be carried out by an eminent and suitably qualified individual or a number of individuals, supported by a small team of security and intelligence law experts with operational knowledge of the workings of the intelligence community. Given its key role in policy development and reform of security and intelligence law, we consider the Attorney-General's Department (AGD) is best placed to provide secretariat support to such a review.

6.13 The review should address the problems that have resulted from incremental, ad hoc changes to Australia's security and intelligence legislation. A simplified legislative framework should provide certainty about what activities agencies can undertake, the relevant thresholds to be met and the oversight mechanisms to which they are subject. It is also important that laws which intrude upon the rights of the individual are "accessible and foreseeable."[21] In other words, the legislative framework should be easily understood and accessible, and clearly state the activities that are permitted under its provisions. Enhanced transparency and access to the law will help to build public confidence in Australia's intelligence agencies. We consider these principles should guide the review we are recommending.

6.14 In addition to those fundamental principles, the review should consider the appropriate role for legislation in the context of emerging issues confronting Australia's intelligence agencies. Given the growth of bulk data, the review should look at how legislation can be used to permit the intelligence agencies to collect, share and analyse data in a flexible way while ensuring appropriate privacy protections for Australians are in place. It should also consider if it would be appropriate for legislation to codify government expectations of private sector assistance to intelligence and law enforcement activities, as is the case in the United Kingdom under the *Investigatory Powers Act 2016*, or whether this should be left to policy initiatives.

21 This principle was articulated by David Anderson QC, the Independent Reviewer of Terrorism Legislation, in his review of investigatory powers in the United Kingdom. See *A Question of Trust: Report of the Investigatory Powers Review,* June 2015.

6.15 A core issue for the review to consider would be whether Australia should adopt a common legislative framework, as has been done in the United Kingdom and New Zealand. It would be essential to consider thoroughly if such a framework, the development and implementation of which would be a complex undertaking, would offer better outcomes for intelligence agencies and the broader community than current arrangements.

6.16 In considering the merits of a common legislative framework, our view is that a starting point should be the principles articulated by Mr Justice Hope in his first Royal Commission, as noted in Chapter 2, including the distinctions between security and foreign intelligence and between intelligence and law enforcement responsibilities. The current legislative framework underpins the distinction between ASIO as a security intelligence agency with an acknowledged remit in relation to Australian persons, and the foreign intelligence agencies with a primary focus on foreign citizens and organisations overseas. Mr Justice Hope argued that the "constraints within which the domestic agency should and must work, and its obligations of propriety, are fundamentally different from those of the foreign agencies. The demarcation should not be blurred, or seen to be blurred."[22]

6.17 The proliferation of transnational issues, especially terrorism, has demanded that cross-over paths be established between the operations of the security and foreign intelligence agencies. But as we have argued previously, we consider the distinction between foreign and security intelligence has continuing relevance, and accordingly we assess it should remain an important principle underpinning Australia's security and intelligence laws. The distinction between security and foreign intelligence means that the capabilities of the foreign intelligence agencies should only be used against Australians in clearly defined circumstances and be subject to legally mandated processes. The value of this constraint was particularly important, and in our view offered assurance to government and the wider community, in the aftermath of the Snowden unauthorised disclosures.

6.18 Accepting the ongoing relevance of the distinction between foreign and security intelligence would not rule out the possibility of a single Act to govern the activities of the intelligence agencies, although it would heavily shape its provisions. The United Kingdom's common legislative framework applies to all intrusive activities undertaken by its intelligence agencies and the same requirements for obtaining approval

22 Royal Commission on Australia's Security and Intelligence Agencies (RCIS), *Third Report on Intelligence Co-ordination Machinery*, December 1976, paragraph 248.

to undertake an activity apply regardless of whether the person in question is a citizen of the United Kingdom or a citizen of another country. By contrast, New Zealand's single authorisation regime for intelligence agencies makes a distinction between the levels of authorisation required for activities concerning New Zealand citizens and permanent residents, and those which concern citizens of another country.

6.19 If the Government were to accept our recommendation for a review of the legislative framework under which Australia's intelligence agencies operate, this would be a significant and lengthy undertaking. In the interim, agencies will continue to operate under existing legislation, which we assess increasingly presents challenges for agencies in discharging their responsibilities. In this Chapter, we recommend a range of reforms that could be implemented more quickly to streamline the existing framework. We see no need for the legislative amendments to establish the Office of National Intelligence (ONI) and ASD as separate statutory agencies to await the outcomes of the more comprehensive review we are recommending.

6.20 The recommendations for reform we set out in this Chapter address what we consider to be the most important and pressing issues for reform of the current legislative framework. Our recommendations seek to facilitate the operations of intelligence agencies in the national interest, foster enhanced collaboration and co-operation among them, and provide a clear framework of assurances that the agencies will act legally, proportionately and in ways that are accountable to Ministerial authority.

THE INTELLIGENCE SERVICES ACT 2001: BACKGROUND AND FRAMEWORK

6.21 The Intelligence Services Bill 2001 set out the functions and powers of ASIS and the Defence Signals Directorate (DSD, now ASD) established a Parliamentary Committee to oversee the administration and expenditure of ASIO, ASIS and DSD, and provided limited immunities to the agencies under Australian law for activities undertaken in the proper performance of their functions.[23] The Bill implemented the findings of the 1995 Commission of Inquiry into ASIS by the Hon Gordon Samuels and Michael Codd which recommended placing ASIS on a statutory basis. DSD's functions were also specified in the Bill since, like ASIS, it had "an external focus in advancing Australia's national security, foreign relations and national economic well being."[24]

23 Revised Explanatory Memorandum to the Intelligence Services Bill 2001, p.2.
24 ibid.

6.22 The functions and Ministerial accountabilities for the Defence Imagery and Geospatial Organisation (now AGO) were included in the Intelligence Services Legislation Amendment Bill 2005 following a recommendation of the 2004 Flood Inquiry that its functions be included in legislation because of its "foreign intelligence focus."[25]

6.23 ASIS, ASD and AGO operate under the Ministerial authorisation (MA) framework which was included in the original ISA on the recommendation of the Joint Select Committee on Intelligence and Security (JSCIS) in 2001. In considering the functions of ASIS and DSD, JSCIS found that the initial draft of the Bill contained "insufficient accountability mechanisms governing the authorisation of ASIS and DSD intelligence collection concerning Australian persons or organisations overseas."[26] ASIS and DSD noted in their evidence to the Committee that, while they did not in the normal course of operations focus on Australian citizens overseas for intelligence collection, "in certain limited circumstances (i.e. a matter of national security) it could be appropriate and permissible under current practice to collect intelligence concerning an Australian citizen or organisation overseas."[27] JSCIS concluded that, even if ASIS and DSD did not focus on Australian citizens or organisations at that time, it was important to future-proof the legislation because, regardless of current practice or intentions, it was concerned with "how the legislation is interpreted and used in five, ten and twenty years time."[28] Accordingly, the Committee argued for an authorisation regime comparable with the special powers provisions in Division 2 of the ASIO Act.[29]

6.24 The MA framework introduced in 2001 provided that the responsible Minister may give an authorisation to ASIS or DSD in relation to an activity, or class of activities, specified in the authorisation for the purpose of producing intelligence on an Australian person.[30] Before issuing an authorisation, the Minister needed to be satisfied that the activities were necessary for the proper performance of the agency's functions and authorised only things reasonably necessary for the proper performance of an agency's functions. The Minister also needed to be satisfied that there were satisfactory arrangements in place to ensure acts done under the authorisation would be reasonable.[31]

25 Explanatory Memorandum to the Intelligence Services Legislation Amendment Bill 2005, pp.2–3.
26 JSCIS, *An Advisory Report on the Intelligence Services Bill 2001,* August 2001, p.49.
27 ibid., p.48.
28 ibid., pp.48–49.
29 ibid., p.48.
30 *Intelligence Services Act 2001* (ISA), section 9.
31 ibid., s 9(1).

6.25 There have been numerous amendments to the ISA since 2001 that aim to adjust its provisions to changing demands.[32] These changes have included:

- allowing a small group of Ministers to give an authorisation where emergency collection is needed and the responsible Minister is not readily available or contactable to issue an authorisation;[33]
- allowing the relevant Agency Head to issue an emergency authorisation, subject to appropriate safeguards, in circumstances where no relevant Ministers are readily available or contactable;[34]
- allowing MAs to cover classes of Australians (but only for ASIS and limited to where it is acting in support of Australian Defence Force (ADF) operations);[35]
- facilitating co-operation between agencies and with other authorities, including by providing staff;[36] and
- allowing ASIS to support ASIO in the performance of its functions, without an MA.[37]

6.26 While these changes have helped to ease some of the practical difficulties experienced, they have introduced an ad hoc character to the ISA. Furthermore, in our view the changes to the ISA constitute only a partial solution to the issues they sought to address. It is clear to us that the ISA has struggled to keep pace with changing realities in the threat environment and there are anomalies in the way it now operates that work against Australia's interests.

6.27 We considered a range of important questions in relation to the adequacy of the ISA, particularly in the context of the significant number of Australians with links to overseas extremist groups that threaten our national security.

6.28 In a general sense we consider that the current legislative framework in the ISA is appropriate. It is consistent with ASIO's leadership on counter-terrorism issues and reinforces the clear authority of the

32 Most notably, substantial amendments to the provisions of the ISA were made under the *Intelligence Services Legislation Amendment Act 2005,* the *Telecommunications Interception and Intelligence Legislation Amendment Act 2011,* the *Intelligence Services Legislation Amendment Act 2011* and the *National Security Legislation Amendment Act 2014.*
33 ISA, s 9A. Section 9A was inserted into the ISA by the *Intelligence Services Legislation Amendment Act 2005* and substantially amended by the *Counter-Terrorism Legislation Amendment Act (No. 1) 2014.*
34 ibid., s 9B. Section 9B was inserted into the ISA by the *Counter-Terrorism Legislation Amendment Act (No. 1) 2014*.
35 ibid., s 8(1)(a)(ia) and (ib).
36 ibid., ss 13 and 13A.
37 ibid., Division 3, Part 2, ss 13B–13G.

Attorney-General on such issues in regard to Australians. As both the Commonwealth's First Law Officer and the Minister responsible for ASIO, the Attorney-General's role in the authorisation process for MAs focused on a threat to security is fundamentally important. Given the Attorney's mandate for implementing the Australian Government's human rights policy agenda, international human rights law, constitutional law and privacy policy, his or her involvement helps to ensure due consideration is given to the rights, freedoms and privacy of the individual. The Attorney must also consider the security issues that arise. In that context, it is particularly important that ASIO has visibility of all intelligence operations undertaken against Australians with links to extremist groups to enable it to fulfil its counter-terrorism responsibilities. Finally, we consider nationality should remain a defining principle in the MA regime.

6.29 Within this broad context, however, we consider there are some parts of the ISA that require amendment. In the following sections we recommend a limited set of changes focused on parts of the ISA that have proved most problematic. These changes could either replace some of the ad hoc reforms noted above, or at least reduce reliance on them. The changes outlined below should apply to all ISA agencies to enhance the integrity and consistency of the Act.

MINISTERIAL AUTHORISATION REGIME

Class Authorisations – Australians Involved with Terrorist Groups

6.30 The first area of change relates to Australians involved with international terrorist groups which pose an actual or potential threat to other Australians. We consider the full capabilities of the Australian Government should be able to be used expeditiously to produce intelligence against Australians who fall into this category. We assess that, in this respect, the existing provisions of the ISA do not meet contemporary needs given both the seriousness of the threat and the number of Australians with connections to international terrorist groups.

6.31 In our view, it is important to give Ministers greater flexibility to issue MAs that cover a class of Australians whose involvement with terrorist organisations proscribed by the Attorney-General under the Criminal Code constitutes a threat to national security. The use of class authorisations would allow the ISA agencies to respond quickly to developing threats from previously unidentified individuals, a more common occurrence now with the emergence of 'lone wolf' attackers.

6.32 At present, class authorisations of this type can only be issued by the Minister for Foreign Affairs to ASIS, and only when it is supporting the ADF's operations.[38] Rather than limit class authorisations in this way, **we recommend that amendments be made to the ISA to enable ISA agencies to seek an authorisation to produce intelligence on a class of Australian persons where the class is defined by reference to involvement with proscribed terrorist organisations and irrespective of whether the intelligence activity is in support of the ADF.** We envisage that the class would extend beyond members of a proscribed terrorist organisation to those involved with such an organisation.

6.33 Such authorisations should be given by the responsible Minister. Before issuing an authorisation, the responsible Minister should obtain the agreement of the Attorney-General. **We also recommend that authorisations have effect for a maximum period of six months, but could be renewed.**

6.34 **We further recommend that agencies maintain a current list of all individuals on whom they are seeking to produce intelligence under the class authorisation.** The list should:

- include a brief explanation of the reasons the ISA agency believes the individual to be part of the class;
- be provided to ASIO to ensure it has visibility of the individuals being covered to enable it to co-ordinate counter-terrorism strategies; and
- be available for inspection and review by the IGIS, who may provide advice to the Agency Head and the responsible Minister.

6.35 **We further recommend that agencies should have to report to the responsible Minister within six months of the original authorisation providing details on the activities they have undertaken under the authorisation and attaching the current list of individuals that it has or is seeking to produce intelligence on under the class authorisation.**

Class Authorisations – Activities in Support of the ADF

6.36 As noted in the previous section, class authorisations for activities in support of the ADF can only be issued by the Minister for Foreign Affairs in respect of ASIS.[39] There are no corresponding provisions for ASD and AGO. However the ISA explicitly provides that it is a function of both agencies

38 ISA, s 8(1)(a)(ia) and (ib).
39 ibid., s 8(1)(a)(ia).

"to provide assistance to the Defence Force in support of military operations and to cooperate with the Defence Force on intelligence matters."[40] This is also a function of ASIS. Yet ASIS is the only ISA agency with access to class authorisations for activities undertaken in support of the ADF. **We recommend that all ISA agencies be able to obtain an authorisation to produce intelligence on one or more members of a class of Australian persons when providing assistance to the ADF in support of military operations. The same oversight arrangements recommended above in relation to class authorisations for Australian persons involved with proscribed terrorist organisations should apply under this regime.**

Ministerial Authorisation for Direct Effects

6.37 A further important issue in relation to Australian persons arises when intelligence is being produced which could have an effect on an Australian. At present, the ISA does not contain a single regime that governs the process that should apply in such circumstances. The situation is clear in regard to ASIS. It is required to seek an MA for activities under its section 6(1)(e) function that are likely to have a direct effect on an Australian.[41] But there is no corresponding provision relating to ASD or AGO.

6.38 **We recommend that the ISA include a requirement for all ISA agencies to obtain an MA for activities that are likely to have a direct effect on an Australian.** In circumstances where an ISA agency is undertaking such activities in support of the ADF, we consider it would be appropriate for this to be achieved through a class MA, as previously recommended (paragraph 6.36).

Intrusiveness of Activities as a Defining Principle

6.39 We also considered whether intrusiveness of the activity, as opposed to the nationality of the person, should be the defining principle for whether an MA is needed. Using intrusiveness as a defining principle could basically limit MAs to activities overseas that would require a warrant if conducted in Australia. This would mean most of ASIS's current activities to produce intelligence against an Australian would not need an authorisation at the Ministerial level. We are of the view that this approach would diminish the rights of Australian persons in an unacceptable way.

40 For ASD, see ISA s 7(d) and for AGO, see ISA s 6B(g).

41 ISA, s 8(1)(a)(ii). Section 8(1)(a)(ii) provides that the responsible Minister for ASIS must issue a written direction to the Agency Head requiring the agency to obtain an MA to undertake under section 6(1)(e) an activity or series of activities that will, or will likely have, a direct effect on an Australian person. Section 6(1)(e) provides that it is a function of ASIS to undertake such other activities as the responsible Minister directs relating to the capabilities, intentions or activities of people or organisations outside Australia.

6.40 We understand it was the original intention of the ISA to restrict the requirement for Ministerial authorisation to the use of covert intelligence collection capabilities against an Australian person overseas, particularly where that use would require a warrant if conducted in Australia. However, in its current implementation MAs are being sought in broader circumstances than originally envisaged. This inhibits preliminary activities not involving the use of covert intelligence collection capabilities and prevents some apparently benign activities without an MA already being in place.

6.41 In addition, the definition of 'intelligence information' in the ISA has also contributed to disproportionate administrative workloads being required for such benign activities as passing media articles about Australians to partner agencies overseas.

6.42 **We recommend restricting the requirement for Ministerial authorisation to the use of covert intelligence collection capabilities by including an appropriate definition of what is meant by 'producing intelligence' and we also recommend amending the definition of 'intelligence information' under the ISA.**

6.43 We strongly agree that ISA agencies should require Ministerial authorisation for activities against an Australian person that would require a warrant if conducted in Australia. **We also recommend that, for ASIS, an MA should be required when it is proposing to task an agent or its network of agents to produce intelligence on an Australian or class of Australians.** The same requirement would apply when ASIS is requesting an international partner to do likewise. We consider that requiring ASIS to obtain appropriate authorisation before using its network of agents to produce intelligence on an Australian person is an important safeguard.

6.44 For all ISA agencies, activities not involving the use of covert intelligence collection capabilities – such as analysis of existing holdings of information – should be able to be undertaken without the need for Ministerial authorisation. Activities involving the further use of such capabilities would require an MA.

Situations of Inferred Consent

6.45 Another problematic area of the ISA is the application of the MA regime in relation to operations designed to help ensure the safety of individual Australians. These are operations where it is in the interests of the Australian person that the capabilities of the ISA agencies be used to produce intelligence about their activities or whereabouts. The clearest

example is where an Australian is kidnapped or taken hostage, and could also include situations where an Australian person is in arbitrary detention overseas. At present ASIS and ASD are required to seek an MA before undertaking any activity to produce intelligence which may, for example, help identify where that person may be, who may have kidnapped them and what intermediaries may be involved. In these types of circumstances, time can be of the essence and the MA process, including the emergency authorisation provisions, can be an unnecessary delay.

6.46 We consider this situation should be addressed explicitly by amending the ISA. We are of the view that the ISA agency should not have to seek an MA in any circumstances where the agency decision maker (who we consider should be the relevant Agency Head or their delegate) has made a judgment that it is reasonable to believe the Australian person would have consented to the production of intelligence in relation to them if they had been in a position to do so. **We recommend that the MA process not be required in circumstances where it is reasonable to believe that the Australian person in question would consent to the ISA agency producing intelligence on that person.**

6.47 Consistent with this view, we do not consider it is appropriate or necessary for the relevant ISA agency to seek a retrospective MA. **We recommend the appropriate subsequent process should be for the relevant ISA agency to advise both its Minister and the IGIS of the action it has taken as soon as possible and, at the latest, within 48 hours of doing so. In situations involving a threat to security, the Minister responsible for ASIO should also be advised.**

6.48 Relevant records should be available to the IGIS for inspection and review, and the IGIS may provide advice to the Agency Head and the responsible Minister on the legality and propriety of activities undertaken.

- If the relevant Minister disagrees with the judgment the agency has made on consent, then all relevant action should cease and the agency should consider seeking an MA in accordance with the existing provisions of the ISA.
- If the responsible Minister agrees with the judgment the agency has made on consent, the agency will be able to continue producing intelligence on the Australian person for six months. Subsequent renewals would be required every six months. At all times, the agency should notify the responsible Minister of any changes in circumstances pertinent to the agency's original decision.

- If the circumstances change and satisfy a criterion for issuing an MA, then such an authorisation should be sought. At each renewal point the agency should notify both the responsible Minister and the IGIS (and the Attorney-General in situations involving a threat to security) of its decision.

Ministerial Consultation

6.49 We consider there is potential to further streamline the procedure for seeking authorisations for Australians who are considered a threat to security. Section 9(1A)(b) of the ISA requires the Minister issuing such an authorisation to obtain the agreement of the Minister responsible for ASIO.[42] At present, the first step is for ASIO to prepare a case to the Attorney-General that the Australian person is a threat to security.

6.50 The definition of security in the ASIO Act (noted in Box 6.1) has been significantly expanded since it was introduced in 1979 and it is increasingly necessary for ISA agencies to seek the Attorney-General's agreement through ASIO for a broad range of activities.

Box 6.1: The Changing Definition of 'Security' Under the ASIO Act

Section 4 of the ASIO Act currently defines security as:

"(a) The protection of, and of the people of, the Commonwealth and the several States and Territories from:

(i) espionage;

(ii) sabotage;

(iii) politically motivated violence;

(iv) promotion of communal violence;

(v) attacks on Australia's defence system; or

(vi) acts of foreign interference;

whether directed from, or committed within, Australia or not; and

Continued over →

42 ISA, s 9(1A)(b) and s 9(1AA), (1AB) and (1AC).

(aa) the protection of Australia's territorial integrity and border integrity from serious threats; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa)."

An earlier version of this definition of security was included in the original ASIO Act in 1979. This definition was substantially amended by the *Australian Security Intelligence Organization Amendment Act 1986,* consistent with the recommendations of Mr Justice Hope in his second Royal Commission. Mr Justice Hope recommended the following changes, which were adopted by Government, the effect of which was "to allow ASIO's functions and activities to be more carefully defined."[43]

- to replace the reference to "active measures of foreign interference", which emphasised activities designed to advance the interests of a foreign country, with "acts of foreign interference", which emphasises acts detrimental to Australia;[44]
- to replace the reference to "subversion", which Mr Justice Hope found "had produced much adverse reaction and may also, by its vague overtones of anti-government activity, tend to mislead people as to the nature of the activity which ASIO is intended to investigate"[45], with references to "politically motivated violence" and "promotion of communal violence", which are narrower than subversion and more accurately reflect ASIO's remit,[46] and
- to include a separate provision dealing with activities that are, or are likely to, obstruct, hinder or interfere with the performance by the Defence Force of its activities, recognising that such activities "are a proper subject for investigation by a security organisation."[47]

Subsection (aa) was introduced under the *Anti-People Smuggling and Other Measures Act 2010* and was intended to enable ASIO "to play a greater role in support of whole of government efforts to address serious threats to Australia's territorial and border integrity, such as people smuggling."[48] This has allowed ASIO to communicate intelligence relating to serious threats to Australia's territorial and border integrity to the relevant authorities.

43 *Royal Commission on Australia's Security and Intelligence Agencies. Report and Ministerial Statement (22 May 1985)* House of Representatives Official Hansard No.142, Thirty Fourth Parliament First Session – First Period, p.2889.
44 RCIS, *Report on the Australian Security Intelligence Organization,* December 1984, pp. 42–43.
45 ibid., p.70.
46 ibid., Chapter 4.
47 ibid., pp. 63 and 71.
48 Explanatory Memorandum to the Anti-People Smuggling and Other Measures Bill 2010, pp. 2–3.

6.51 For reasons noted at paragraph 6.28 above, we consider that it remains appropriate for the Attorney-General, in both capacities as the First Law Officer of the Commonwealth and the Minister responsible for ASIO, to be involved in the MA process. It is important that the Attorney-General and ASIO maintain a complete understanding of the security environment and relevant security-related operations. We also recognise that the processes currently followed can lead to some delays and difficulties. We consider that reversing the order of the current process for authorisation would address this issue and may also reduce the time required to process authorisations. Under this procedure, ASIO would not be required to prepare a separate case to the Attorney-General; rather we expect it would comment on the case presented by the ISA agency. **We recommend that the Ministers responsible for the ISA agencies first consider a case prepared by their own agency in consultation with ASIO. If the Minister agrees with the arguments presented by the ISA agency, the Minister should then consult with and obtain the agreement of the Attorney-General before issuing the authorisation**.

6.52 We also considered whether the Minister for Foreign Affairs should be advised, or his or her agreement sought, when an agency is conducting activities overseas which could impact on Australia's foreign relations. We recognise that Australia's intelligence agencies are all highly professional and have effectively managed high risk activities on a regular basis, both onshore and offshore.

6.53 Nevertheless, we also consider it important for the Minister for Foreign Affairs to have visibility of sensitive activities undertaken overseas. While we note current arrangements for such advice and we do not consider that the agreement of the Minister for Foreign Affairs needs to be required under legislation, **we recommend that there be regular briefings involving ISA Ministers and their Agency Heads, and the Attorney-General and Director-General of Security, on intelligence collection activities overseas which, if compromised, could damage Australia's foreign policy or international relations.** Provision for such briefings could be made in the Guidelines issued by the Attorney-General for ASIO under section 8A of the ASIO Act, and in Ministerial Directions issued by the responsible ISA Ministers for ASIS, AGO and ASD under section 8 of the ISA.

CO-OPERATION PROVISIONS UNDER THE ISA

6.54 Co-operation among intelligence agencies is essential to maximise the likelihood of success in thwarting attacks and defeating other threats to Australia's national security. Divisions 2 and 3 of Part 2 of the ISA

are intended to enable co-operation among ISA agencies, ASIO and non-government organisations, in Australia and overseas in the proper performance of their functions. However, as with the MA arrangements, the co-operation provisions under the ISA have developed in an ad hoc fashion and can in some instances actively hamper co-operation. In our view, these provisions should be updated to address difficulties in their practical application.

6.55 Section 13 of the ISA permits co-operation between an ISA agency and Commonwealth authorities, State authorities and authorities of other countries approved by the Minister as being capable of assisting the ISA agency to perform its functions. This section is "intended to be mutually beneficial for the performance of the functions of the specified authorities and agencies."[49]

6.56 Section 13A provides that an ISA agency may co-operate with and assist another agency, ASIO or any other body prescribed by the Minister in regulations under the section in the performance of the other agency's functions. This section aims to enable ASIO and ISA agencies to provide greater support and assistance to each other in circumstances outside section 13, for example by providing "agency staff and resources to multi-agency teams and taskforces."[50]

6.57 Sections 13B to 13G of the ISA allow ASIS to undertake less intrusive activities (namely, those acts for which ASIO would not require a warrant in Australia) when acting in co-operation with ASIO to support performance by ASIO of its functions. There is currently no need for ASIS to seek an MA in these circumstances.[51] ASIS can only undertake such activities outside Australia on the basis of notification in writing from ASIO that it requires the production of intelligence on the Australian person or class of an Australian person,[52] except in relation to certain prescribed activities when it is not practicable for ASIO to notify ASIS.[53]

6.58 Difficulties have arisen in implementing these provisions and hamper effective co-operation between intelligence agencies. Under sections 13 and 13A, each ISA agency must obtain an MA in order to co-operate, including in situations where two ISA agencies are working closely

49 Explanatory Memorandum to the Intelligence Services Bill 2001, p.7.
50 Explanatory Memorandum to the Telecommunications Intercept and Intelligence Services Legislation Amendment Bill 2011, p.33.
51 ISA, s 13D. This regime was introduced in 2014 to implement a PJCIS recommendation, drawing on an IGIS submission to an inquiry into proposed national security law reforms in 2012, that "where ASIO and an IS Act agency, such as ASIS, is engaged in a co-operative intelligence operation, consistent protections for Australian persons should apply for the authorisation of ASIO and the IS Act agencies' activities": *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* May 2013, pp.135–136.
52 ibid., s 13B(1).
53 ibid., s 13B(3).

together in relation to the same person of interest and/or where the agency co-operates only briefly to provide specialist skills for a particular matter or operation. Even for ASD–AGO co-operation, each agency must obtain an MA even though both of those MAs will be issued by the Minister for Defence. Section 13 is also silent on the issue of co-operation with non-state actors. For agencies, the requirement to obtain an MA under section 13A means this provision is of little practical value in furthering co-operation.

6.59 While the provisions in sections 13B–13G have enhanced co-operation to some degree, significant limitations remain. The exclusion of ASD and AGO from these provisions is an impediment to co-operation and often prevents these agencies undertaking preparatory acts on behalf of ASIO without an MA. Moreover, the geographic limitation in section 13B restricts co-operation.

6.60 In our view amendments to the co-operation provisions are needed to ensure they work effectively and function as intended. **We recommend clarifying that when two ISA agencies are co-operating with each other under sections 13 and 13A, those agencies can jointly seek a single MA from the relevant Ministers.** A joint MA would maintain direct Ministerial oversight across different portfolios while reducing the overall number of MAs required to be issued. Consistent with the current MA framework, a joint MA would not permit agencies to undertake activities in Australia for which ASIO would require a warrant to perform.

6.61 **We also recommend that sections 13B–13G be amended to include all ISA agencies.** This would ensure all ISA agencies can co-operate effectively with ASIO on less intrusive activities. **We further recommend that the geographical limitation in section 13B(1)(b) be removed to enable all ISA agencies to operate in Australia under a section 13B authority.** The list of persons on whom agencies are seeking to produce intelligence under section 13B should be available for inspection and review by the IGIS.

6.62 Our recommendations concerning the MA regime in the preceding section will also alleviate some of the problems encountered in the practical application of sections 13, 13A and 13B–13G. In particular, introducing a limited class authorisation system in relation to Australian persons connected to proscribed terrorist groups and requiring authorisations for covert intelligence activities only will make it easier for ISA agencies to co-operate with each other and with ASIO. When combined with recommendations in this section, this suite of measures

will facilitate deeper and more sustained co-operation under the ISA, consistent with the spirit and intent of these provisions.

PROHIBITION ON PARAMILITARY ACTIVITIES AND THE USE OF WEAPONS

6.63 Currently, under section 6(4) of the ISA, ASIS staff members and agents, in performing ASIS functions, must not plan for or undertake paramilitary activities, violence against the person or the use of weapons. Paramilitary activities are defined as "activities involving the use of an armed unit (or other armed group) that is not part of a country's official defence or law enforcement forces."[54] These prohibitions were recommendations of the 1984 Hope Royal Commission which concluded that ASIS be prohibited from undertaking "covert action in the form of either special operations or special political action, and from undertaking training for such action" and "that the use by ASIS of weapons be terminated."[55]

6.64 The prohibition on the use of weapons in section 6(4) does not prevent the provision of weapons, or training in the use of weapons or in self-defence techniques, or the use of weapons or self-defence techniques in strictly limited circumstances under Schedule 2 of the ISA.[56] Amendments in 2014 extended these provisions to apply to persons co-operating with ASIS. These exceptions recognise that, since the ISA was introduced in 2001, there have been fundamental changes in ASIS's operating environment as a result of increasing terrorist activities and the threat of weapons proliferation, and agents should be able to protect themselves in these circumstances.[57]

6.65 We consider that restrictions on ASIS developing a paramilitary capability remain appropriate. They align with ASIS's core function of collecting human intelligence about the capabilities, intentions or activities of persons or organisations overseas. It also remains appropriate that ASIS staff members and persons co-operating with ASIS are able to defend themselves and participate in training on the use of weapons and self-defence.

6.66 We also consider, however, there should be changes made to the authorisation process under Schedule 2. Currently, the responsible Minister must approve in writing the provision of a weapon or training in

54 ISA, s 3.
55 *Royal Commission on Australia's Security and Intelligence Agencies. Report and Ministerial Statement (22 May 1985)* House of Representatives Official Hansard No.142, Thirty Fourth Parliament First Session – First Period, p.2886–2887.
56 ISA, sch 2.
57 Explanatory Memorandum to Intelligence Services Amendment Bill 2003 [2004], pp.2–3.

the use of a weapon or in self-defence techniques.[58] Ministerial approval must specify the purpose for which the weapon or training is provided, any conditions to be complied with, and the kind or class of weapon involved.[59] A copy of the Ministerial approval must be given to the Director-General of ASIS and to the IGIS as soon as practicable.[60] ASIS is also required to provide a written report to the IGIS on the circumstances surrounding use or discharge of a weapon by an ASIS staff member or agent.[61]

6.67 Rather than seeking Ministerial authorisation, **we recommend that authorisation be required at the Director-General level under Schedule 2, with the Director-General notifying the Minister on a monthly basis of any new authorisations or changes to existing authorisations. The IGIS's oversight and reporting role under Schedule 2 should be maintained.**

ENHANCED CO-ORDINATION IN POLICY DEVELOPMENT AND LEGISLATIVE REFORM

6.68 AGD develops most reforms to national security legislation in consultation with intelligence agencies and relevant departments. The effective development of legislative reforms requires an in-depth understanding of the relevant field of intelligence activity, to properly identify the issues to be addressed, determine whether a legislative solution is required, and design changed arrangements that are fit for purpose and balances operational need and rule of law considerations.

6.69 While AGD is the Commonwealth Department with primary responsibility for progressing amendments to national security laws, a number of Commonwealth departments administer components of the legislative framework governing the intelligence community. They include:

- The Department of the Prime Minister and Cabinet for the IGIS and ONA Acts, and for ISA provisions relating to the Prime Minister's powers or functions;
- AGD for the ASIO and TIA Acts, and for ISA provisions relating to ASIO;
- the Department of Defence for ISA provisions relating to ASD, AGO and DIO; and

58 ISA sch 2, cl 1, ss 3 and 3A.
59 ibid., cl 1, s 4.
60 ibid., cl 1, s 5.
61 ibid., cl 1, s 5 and cl 3.

- the Department of Foreign Affairs and Trade for the remainder of ISA provisions, including those relating to ASIS.

These divisions of responsibility are consistent with Ministerial responsibility, oversight and accountability requirements and promote compliance with the law by intelligence agencies.

6.70 While AGD maintains strong, collaborative working relationships with all the AIC agencies and the Office of the IGIS, the division of responsibility presents problems for development of timely and comprehensive legislative reform proposals that are fit for purpose and, to the extent possible, anticipate future developments. In our view, this situation together with the quickening pace of technological advancements and operational secrecy requirements mean that legal problems may not come to light until after they have been encountered in practice. The existing division of responsibility also increases the risk that departments and agencies will adopt different interpretations of key provisions, particularly in relation to provisions in the ISA that apply to agencies in both the Defence and Foreign Affairs portfolios.

6.71 Furthermore, AGD may not always have access to legal advice provided on parts of the ISA administered by other departments. While paragraph 10 of the *Legal Services Directions 2017,* which set out a range of obligations in relation to the provision and receipt of legal advice by the Commonwealth, requires agencies to consult in relation to legal advice on the interpretation of legislation, there are exceptions for national security matters.

6.72 **We recommend the existing consultation arrangements between AGD and the intelligence community be strengthened through a memorandum of understanding or other form of written agreement between AGD, the departments which administer intelligence legislation and the intelligence agencies themselves.** Such an agreement should require AGD to convene a meeting involving all relevant departments, agencies and the Office of the IGIS, at least three times a year to align with the Parliamentary sitting periods, to discuss key legislative impediments for agencies in the performance of their functions, legal advices received in the preceding six months and forecasted legislative activity.

6.73 Regular meetings would not preclude emergency action to address measures in the intervening period but would provide key actors with greater visibility of legal advices relating to the intelligence community and a deeper understanding of the challenges arising from

implementation of intelligence legislation. They would also facilitate more considered policy analysis and development of legislation within AGD that addresses issues holistically, rather than targeting specific legal barriers. In particular, AGD would be equipped with the expertise and knowledge to support the comprehensive review of the legislative framework under which our intelligence agencies operate that we recommend in this Chapter.

6.74 Consistent with the *Legal Services Directions 2017,* AGD should also be provided with a summary of all requests for legal advice on provisions of intelligence-related legislation to guard against provision of conflicting advice on the same or similar sections. It is important that AGD also maintain a central repository of all relevant legal advices once finalised, subject to operational secrecy requirements.

CHAPTER 7: OVERSIGHT OF AUSTRALIA'S INTELLIGENCE AGENCIES

7.1 This Chapter addresses the Review's Term of Reference in relation to *the effectiveness of current oversight arrangements.*

7.2 It is critical in a democracy that intelligence agencies are subject to strong oversight and accountability mechanisms. Indeed, oversight of intelligence services is a central tenet of the 'state of trust'[62] between intelligence services and the community of which they are part. A critical element of this 'state of trust' is the understanding that agencies provide intelligence which contributes to safeguarding national interests and the lives of citizens and that, in doing so, those agencies act with propriety, legality and proportionality, are responsive to Ministerial direction and control, and are accountable for their activities.

7.3 Since much of the work of intelligence agencies is necessarily secret, many of the traditional means by which the broader community can determine that government agencies are operating in an appropriate manner are not fully applicable to the intelligence community. Intelligence agencies need purpose-designed, strong institutional safeguards and arrangements.

7.4 The Hope Royal Commissions addressed this issue and the government of the day subsequently established a combination of government, parliamentary and independent oversight of intelligence agencies, complemented by increased Ministerial oversight and accountability to Parliament. This combination remains in place today. In our view, it strikes an appropriate balance between the need for intelligence agencies to function with confidentiality, to be operationally effective (subject to checks and balances applied by legislation and responsible Ministers) and the requirement for robust accountability in a democratic society.

7.5 Accordingly, we consider the broad architecture of Australia's oversight arrangements remains appropriate and does not require fundamental change. Rather, our recommendations in this Chapter focus on the components of the architecture. We consider changes are needed to some of these components to ensure they are able to cope with the increasing complexity and size of Australia's modern national intelligence enterprise.

62 See David Omand, *Securing the State,* London, Hurst Publishers, 2010.

EXISTING OVERSIGHT ARRANGEMENTS

7.6 Existing oversight arrangements represent a carefully constructed architecture. They reflect appropriate divisions of responsibility while also incorporating important checks and balances. Ministers have direct responsibility for the actions of Australian Intelligence Community (AIC) agencies and for laws that fall within their portfolios which define the functions, responsibilities and powers of those agencies. Accountable to the Parliament, responsible Ministers – including the Prime Minister in respect of the Office of National Assessments (ONA), the Attorney-General for the Australian Security Intelligence Organisation (ASIO), the Minister for Foreign Affairs for the Australian Secret Intelligence Service (ASIS), and the Minister for Defence for the Australian Signals Directorate (ASD), the Australian Geospatial-Intelligence Organisation (AGO) and the Defence Intelligence Organisation (DIO) – have a legal duty as well as a compelling incentive to ensure agencies operate effectively and efficiently, and act with propriety and in accordance with the law. Ensuring elected representatives are directly responsible for our intelligence agencies enhances democratic accountability.

7.7 The Parliamentary Joint Committee on Intelligence and Security (PJCIS) currently reviews the administration and expenditure of AIC agencies (including their annual financial statements),[63] addresses matters referred to it by the responsible Minister or by a resolution of Parliament,[64] and reports its recommendations to Parliament and the responsible Minister.[65]

7.8 The PJCIS also has a role in reviewing counter-terrorism and national security legislation and a limited role in operational oversight of ASIO and the Australian Federal Police (AFP) with respect to retained metadata.[66] Except in these limited circumstances, the PJCIS is restricted from undertaking assessments of operations conducted by AIC agencies and does not have the power to review operational material or reporting.[67]

7.9 The PJCIS and its predecessors have played a critical role in overseeing Australia's intelligence agencies for around 30 years. A Parliamentary Committee to oversee ASIO was established under the *Australian Security Intelligence Organization Amendment Act 1986* to improve oversight of the intelligence community by "directly involving the Parliament – on

63 *Intelligence Services Act 2001* (ISA), section 29(1)(a).
64 ibid., s 29(1)(b).
65 ibid., s 29(1)(c).
66 Under section 29(1)(baa)–(ca) of the ISA, the Committee is required to monitor and review the operation, effectiveness and implications of the questioning and detention powers in the ASIO Act and the Crimes Act, the control order and preventative detention order provisions in the Criminal Code, the data retention provisions in the TIA Act, and the citizenship loss provisions in the *Australian Citizenship Act 2007*.
67 ISA, s 29(3).

both sides and in both houses – in imposing the discipline of an external scrutiny of the intelligence and security agencies quite independent of the Executive."[68]

7.10 In 2001 the Committee's remit was expanded to cover ASIS and the then Defence Signals Directorate (DSD, now ASD). The Intelligence Services Bill 2001 implemented recommendations of the 1995 Commission of Inquiry into ASIS which found that the control and accountability as well as internal organisation and management of ASIS could be improved by parliamentary oversight.[69] In considering the Bill, the Joint Select Committee on Intelligence and Security recommended that DSD also be subject to oversight by the new Committee as "the most significant Defence collection agency."[70]

7.11 In 2004, the Flood Inquiry recommended that the then Defence Imagery and Geospatial Organisation (now AGO), DIO and ONA also be subject to oversight by the Committee to "enhance confidence in the parliament and the public that the full range of intelligence agencies is accountable to a senior group of parliamentarians" and to "contribute to a better understanding of the agencies in the parliamentary and the broader community."[71] The PJCIS came into existence following passage of the Intelligence Services Amendment Bill 2005.

7.12 The PJCIS comprises 11 members – six members of the House of Representatives and five Senators – a majority of whom must be Government members.[72] Members from the House of Representatives are appointed by resolution of the House on nomination by the Prime Minister in consultation with the Leader of the Opposition,[73] and Senators are appointed by resolution of the Senate on nomination by the Leader of the Government in the Senate in consultation with the Leader of

68 *Royal Commission on Australia's Security and Intelligence Agencies. Report and Ministerial Statement (22 May 1985)* House of Representatives Official Hansard No.142, Thirty Fourth Parliament First Session – First Period, p.2888. In his 1984 Report, Mr Justice Hope noted that his "preferred approach" to Parliamentary oversight was "to suggest ways in which the capacity of Ministers to account to Parliament for the activities of intelligence agencies could be strengthened – for example, by means of the role of the proposed Inspector-General – rather than to propose separate new lines of accountability." However, Mr Justice Hope noted that, ultimately, the decision to establish a Parliamentary committee to oversee the intelligence agencies was a matter for Parliament. Mr Justice Hope endorsed a number of guidelines for how such a committee should operate in the event that Parliament chose to establish such a committee: Royal Commission on Australia's Security Intelligence Agencies, *General Report,* December 1984, 3.27–3.28, p.25; and *Report on the Australian Security Intelligence Organization,* December 1984, 17.30–17.35, pp.344–346

69 Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service,* March 1995, p.xxx–xxxi.

70 Joint Select Committee on the Intelligence Services, *An Advisory Report on the Intelligence Services Bill 2001, the Intelligence Services (Consequential Provisions) Bill 2001 and certain parts of the Cybercrime Bill 2001,* August 2001, p.64.

71 Flood, op.cit., pp. 57–58.

72 ISA, s 28 (2) and (3).

73 ibid., Schedule 1 Part 3 s 14(1) and (2).

each recognised political party that is represented in the Senate and does not form part of the Government.[74] Members of the PJCIS cannot include a Minister, President of the Senate or Speaker of the House of Representatives.[75]

7.13 The Inspector-General of Intelligence and Security (IGIS) is an independent executive oversight body established following a recommendation of the second Hope Royal Commission in 1984. The IGIS reviews the legality and propriety of AIC agencies' activities, ensures that those activities are consistent with human rights, and investigates complaints about alleged misconduct.[76] Established under the *Inspector-General of Intelligence and Security Act 1986,* the IGIS has significant powers, akin to those of a Royal Commission, which include obtaining information and requiring persons to answer questions and produce documents. It can also undertake regular inspections of agency files and documentation to identify issues with governance and control frameworks within agencies.[77]

7.14 The IGIS can make submissions containing suggestions to improve the governance and legal frameworks under which AIC agencies operate to Parliamentary inquiries and independent reviews. Through its functions of inquiry and reporting, the Office of the IGIS is designed to provide assurance to Parliament and the public that AIC operations are subject to thorough and independent oversight, while maintaining the operational requirement for secrecy.

7.15 The Independent National Security Legislation Monitor (the Monitor), an independent executive oversight body established under the *Independent National Security Legislation Monitor Act 2010* (INSLM Act), is responsible for reviewing the operation, effectiveness and implications of counter-terrorism and national security legislation.[78] This includes considering whether laws contain appropriate safeguards for protecting the rights of individuals, remain proportionate to any threat of terrorism or threat to national security, and remain necessary. The Monitor can also provide expert, independent legal advice and analysis to Parliament and Parliamentary committees on counter-terrorism and national security legislation.

7.16 In our view, the role of the Monitor provides a value-adding, independent perspective on the balance between necessary counter-terrorism and

74 ISA, Schedule 1 Part 3 s 14(3) and (4).
75 ibid., s 14(6).
76 *Inspector-General of Intelligence and Security Act 1986* (IGIS Act), ss 8 and 9.
77 ibid., s 18.
78 *Independent National Security Legislation Monitor Act 2010* (INSLM Act), s 6.

national security legislation and the protection of civil liberties. Since 2011, the Monitor has conducted inquiries on legislative issues, including a recently completed review on questioning and detention powers under the ASIO Act and Crimes Act,[79] and an additional three inquiries on matters referred to it by the Prime Minister under section 7 of the INSLM Act.[80] The Monitor has also issued six annual reports assessing counter-terrorism and national security legislation and making recommendations for reform.

7.17 The Australian National Audit Office (ANAO) includes the AIC agencies within the scope of its audit program. For example, in relation to ASIS, ANAO has visibility and scrutiny of all ASIS financial matters through participation on the ASIS Audit Committee and independent audit of ASIS financial systems and records by senior ANAO officers. By conducting such audits, ANAO plays an important oversight role, providing public assurance that agencies are using public funds appropriately.

7.18 In considering changes to the components of Australia's oversight architecture, we have taken account of the comparable arrangements in Five Eyes partners – the United Kingdom, the United States, Canada and New Zealand. However, we recognise that compared with those arrangements, Australia's oversight framework is unique, with significant powers afforded to the independent statutory office of the IGIS.

OVERSIGHT OF THE NATIONAL INTELLIGENCE COMMUNITY

7.19 As we note in Chapters 3 and 4, the intelligence enterprise that supports Australia's national security is no longer limited to the six AIC agencies. The contemporary threat environment, particularly the rise of terrorism and irregular immigration as major concerns, means that the intelligence capabilities of the AFP, the Department of Immigration and Border Protection (DIBP), the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Criminal Intelligence Commission (ACIC) also make a critically important and increasingly significant contribution to national security. The intelligence capabilities of these agencies allow some activities to be undertaken that can impact significantly on Australian citizens. Furthermore, there is a need for increased collaboration as well as a greater sharing of capabilities and information

79 Section 6(1B) of the INSLM Act requires the Monitor to complete a review of questioning and detention powers under the ASIO Act and Crimes Act by 7 September 2017. A report into these powers – *Certain Questioning and Detention Powers in Relation to Terrorism* – was tabled in Parliament on 8 February 2017.

80 The Monitor has also conducted three inquiries on matters referred by the Prime Minister under section 7: *Certain Matters Regarding the Impact of Amendments to the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (2 May 2016); *Section 35P of the ASIO Act* (2 February 2016); and *Control Order Safeguards* (29 January 2016).

across the ten intelligence agencies of the National Intelligence Community (NIC). We consider, therefore, that there is a compelling case for a consistent oversight regime to apply to all the intelligence capabilities that support national security, across the ten agencies of the NIC.

7.20 **We recommend the oversight role of the PJCIS and the IGIS be expanded to apply to all ten agencies within the NIC, with oversight of the AFP, ACIC and DIBP limited to their intelligence functions, and with current oversight arrangements in relation to ONA applied to the Office of National Intelligence (ONI).** The precise lines of demarcation would need to be agreed between DIBP, AFP, ACIC and the IGIS. Given the breadth of the functions of the AFP, ACIC and DIBP, and the complementary oversight arrangements, it would be neither appropriate nor necessary to expand the role of the PJCIS or the IGIS beyond the exercise of intelligence capabilities that contribute to national security.

7.21 Extending PJCIS and IGIS oversight to all NIC agencies would need to avoid duplicating existing oversight of other functions exercised by these agencies. For example, the AFP is currently subject to oversight by the Commonwealth Ombudsman, who can investigate the actions of AFP members as well as the policies, practices and procedures of the AFP as an agency. The AFP is also oversighted by the Parliamentary Joint Committee on Law Enforcement. The PJCIS's limited oversight of AFP's performance under Part 5.3 of the Criminal Code, noted in Box 7.1, provides a useful example of how oversight of an agency's intelligence capabilities directed towards national security can be separately identified in legislation.

Box 7.1: PJCIS Oversight of the Australian Federal Police's Counter-Terrorism Functions

The PJCIS has limited powers to inquire into AFP's performance with respect of terrorism offences, control orders and preventative detention orders under Part 5.3 of the *Criminal Code Act 1995.*

Section 29(1)(baa) and (bab) of the ISA permit the PJCIS to "monitor and review the performance by the AFP of its functions under Part 5.3 of the *Criminal Code*" and to "report to both Houses of Parliament ... upon any matter appertaining to the AFP or connected with the performance of its functions under Part 5.3 of the *Criminal Code* ...".

Continued over →

The Parliamentary Joint Committee on Law Enforcement (PJCLE) is also empowered to monitor and report to Parliament on the performance by AFP of its functions under the *Parliamentary Joint Committee on Law Enforcement Act 2010*. The PJCLE also has oversight of the ACIC.

However, there is a specific exemption relating to Part 5.3 of the Criminal Code.[81] This implements a recommendation of the PJCIS in its inquiry into the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*. While the PJCIS noted the AFP is already subject to a rigorous internal and external accountability regime, including through the PJCLE, extension of PJCIS oversight powers to the counter-terrorism activities of the AFP could "provide a useful additional oversight function ... particularly in relation to classified material that is not able to be considered by other parliamentary committees."[82]

7.22 In our view, the IGIS is mandated with the necessary independence and has the appropriate powers to perform effective oversight of the NIC agencies. This oversight would help to reinforce the prevailing culture of compliance across agencies exercising similar powers. However, as noted below, greater resourcing for the Office of the IGIS (IGIS Office) would be required for the IGIS to perform this expanded role.

INCREASED RESOURCING FOR THE IGIS

7.23 The IGIS is a critically important component of Australia's oversight arrangements. One of its great strengths is its unfettered access to the records of the intelligence agencies. Staff of the IGIS Office have the highest security clearances and the necessary training to enable them to interrogate systems freely. With the ability to compel witnesses, this represents a powerful combination that underpins the compliance architecture.

7.24 We consider that bodies performing oversight of intelligence functions, particularly the IGIS Office, must be appropriately resourced commensurate with the scale and complexity of the intelligence community and its operations. In our view, resourcing of the IGIS Office has not kept pace with the functions it is tasked to perform, notwithstanding receiving an exemption from the Efficiency Dividend in 2015.

81 *Parliamentary Joint Committee on Law Enforcement Act 2010*, s 7(2).
82 PJCIS, *Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (17 October 2014), recommendation 14, p. 80.

7.25 To address this, we consider the resources available to the IGIS Office should be increased to enable the IGIS to effectively oversee the ten agencies of the NIC and enhance its ability to maintain oversight of the additional powers granted to the AIC agencies in recent years. Increased resourcing would also allow the IGIS Office to expand important outreach activities designed to "raise awareness of the Inspector-General and to enhance public confidence in the extensive and powerful oversight of this office."[83]

7.26 In considering the appropriate quantum of additional resources, we consider that the IGIS Office should expand from 17 to around 50 full-time staff. This number of staff would enable the IGIS to conduct a more regular and comprehensive program of random inspections to increase its assurance that agencies are operating legally and with propriety.

7.27 Accordingly, **we recommend that the Office of the IGIS be allocated additional resources to enable it to sustain a full-time staff of around 50.**

EXPANDED ROLE FOR THE PJCIS

7.28 The reviews undertaken and reports produced by the PJCIS are vitally important accountability mechanisms for the intelligence agencies. Annual reports into the administration and expenditure of AIC agencies, which are tabled in Parliament, inform the Parliament and the wider community about the resources that intelligence agencies are using. These reports also acknowledge that "the transparency and public accountability of the intelligence agencies must be balanced with the need to protect national security."[84]

7.29 In recent years the Committee has also undertaken a range of value-adding reviews of proposed changes to counter-terrorism and national security legislation.[85] Since 2014, Parliament has passed eight pieces of counter-terrorism and national security legislation which have enhanced the powers available to law enforcement, security, intelligence and prosecution agencies. Upon introduction, all Bills have

83 IGIS, *Annual Report 2015-2016,* p.v.
84 PJCIS, *Review of Administration and Expenditure: No. 13 (2013-2014) – Australian Intelligence Agencies,* June 2015, p.2.
85 For the PJCIS reports on the legislation referred to, see *Advisory Report on the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (17 October 2014), and *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (27 February 2015).

been referred to the PJCIS for inquiry and report[86] and the Committee has made a number of recommendations, the majority of which have been accepted by the government of the day, to make contentious legislation more workable. In particular, we note Patrick F. Walsh's Submission to this Review that "the PJCIS has played an effective bipartisan role in providing reasonable amendments to the Foreign Fighters and Data Retention Acts" which assisted their passage through Parliament.[87]

7.30 Submissions to this Review have been received from a number of interested parties proposing that the role of the PJCIS should be enhanced.[88] The Queensland Council for Civil Liberties argued that the Committee was "the main mechanism of democratic accountability" for intelligence agencies and should "take a more front and centre role in ensuring that intelligence agencies are held accountable for their actions."[89] Patrick F. Walsh noted that following the Wikileaks and Snowden unauthorised disclosures and growing interest in the broader community in perceived failures of intelligence, providing public reassurance that "the AIC is operating lawfully, ethically risk manages operational decision-making and is value for money just like any other government entity" is critically important.[90]

7.31 We have also carefully considered the views of former Senator the Hon John Faulkner to enhance the role of the PJCIS[91] and the proposals set out in the Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015 (PJCIS Amendment Bill) introduced by Senator the Hon Penny Wong in the Senate in August 2015.[92] Senator Faulkner argued that, to ensure public trust and confidence in the intelligence community, "strong and rigorous oversight and scrutiny" through the Parliament is necessary.[93] He argued that Parliament is responsible for

86 A function of the PJCIS under section 29(2)(b) of the ISA is to review any matter relating to intelligence agencies referred to the Committee by the responsible Minister or a resolution of either House of Parliament. The Committee has also completed the following reports on legislative changes since 2014: *Inquiry into the National Security Legislation Bill (No 1) 2014* (17 September 2014); *Advisory Report on the Counter-Terrorism Legislation Amendment Bill (No 1) 2014* (20 November 2014); *Advisory Report on the Australian Citizenship Amendment (Allegiance to Australia) Bill 2015* (4 September 2015); *Advisory Report on the Counter-Terrorism Legislation Amendment Bill (No 1) 2015* (15 February 2016); *Advisory Report on the Criminal Code Amendment (High Risk Terrorist Offenders) Bill 2016* (4 November 2016); and *Advisory Report on the Criminal Code Amendment (War Crimes) Bill 2016* (18 November 2016).

87 Patrick F. Walsh Submission, p.15.

88 The Queensland Council for Civil Liberties Submission; Patrick F. Walsh Submission; Anthony Bergin and Kate Grayson Submission.

89 The Queensland Council for Civil Liberties Submission, p.6.

90 Patrick F. Walsh Submission, p.16.

91 Senator the Hon John Faulkner, *Surveillance, Intelligence and Accountability: an Australian Story*, 21 October 2014. Available at https://www.senatorjohnfaulkner.com.au/wp-content/uploads/2016/03/JF-INTEL.pdf.

92 The PJCIS Amendment Bill was introduced on 10 August 2015 but lapsed when Parliament was dissolved in advance of the 2016 federal election in May 2016. The Bill was reinstated to the Senate Bills List on 31 August 2016.

93 Faulkner, op.cit., p.1.

striking a "balance between our security imperatives and our liberties and freedoms" and is best placed to assure the public that "agencies are serving the purpose for which they were created and that they are doing so in a cost effective way."[94]

7.32 In the Second Reading speech accompanying debate on the Bill, Senator Wong noted that Parliamentarians cannot "outsource [their] duty to ensure the security of our nation and the people who entrust us with the responsibility of governing."[95] A summary of the provisions in the Bill are in Box 7.2.

Box 7.2: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015

The PJCIS Amendment Bill proposes amendments to the sections of the ISA governing the membership, powers and functions of the PJCIS. The Bill contains provisions that seek to:

- require the IGIS to provide the PJCIS with copies of any report given to the responsible Minister or Prime Minister within three months;[96]
- permit the Independent National Security Legislation Monitor to provide a report to the Committee on matters referred to it by the Committee or any inquiries conducted into legislation which is due to expire;[97]
- enable the PJCIS, by resolution, to conduct inquiries into any matter in relation to the six AIC agencies;[98]
- enable the PJCIS to review the operation, effectiveness and continuing need for counter-terrorism and national security legislation that contains a sunset provision, no later than six months before the sunset date;[99]

Continued over →

94 Faulkner, op.cit., pp.1 and 50.
95 Second Reading Speech accompanying PJCIS Amendment Bill, p.1720.
96 PJCIS Amendment Bill, schedule 1 section 3.
97 ibid., sch 1 s 1.
98 ibid., sch 1 s 6.
99 ibid., sch 1 s 7.

- permit the PJCIS, by resolution, to review AIC agency activities following consultation with the responsible Minister;[100] and
- change the requirements for Committee membership, by mandating that the Committee must include one Government member from both House of Representatives and the Senate, and one Opposition member from both the House of Representatives and the Senate. The remainder of the Committee members can be drawn from either the Senate or House of Representatives. As is currently the case, the Committee will consist of 11 members in total.[101] In nominating members, the Prime Minister and Leader of the Opposition must be satisfied that the nominees are "the most appropriate members available to serve on the Committee" and "have regard to the desirability of ensuring that the composition of the Committee reflects the representation of recognised political parties in Parliament."[102]

7.33 We agree that the oversight role of the PJCIS should be enhanced. In framing our recommendations on this issue, we have been particularly conscious of the need to reinforce and build on the valuable role the Committee has played, and to ensure that changes to its role should strengthen the overall compliance architecture and certainly not weaken it by introducing disproportionate compliance burdens or undesirable duplication. We have also considered the remits of Parliamentary Committees in the Five Eyes partners that have oversight of the activities of intelligence agencies, including their operations.

7.34 **We recommend that interactions between the PJCIS and the Independent National Security Legislation Monitor be enhanced by including the Monitor as a person who may be requested to brief the Committee. We also recommend the Committee be able to ask the Monitor to report on matters referred by the Committee, and to provide the Committee with the outcome of the Monitor's inquiries into existing legislation at the same time as the Monitor provides such reports to the responsible Minister.**

7.35 The PJCIS has developed significant expertise in reviewing proposed legislation. This constitutes an important accountability mechanism which, as Patrick F. Walsh argued in his Submission to this Review, "helps build trust between the Australian public and the government that the AIC is accountable in its operations."[103] We consider this value-adding

100 PJCIS Amendment Bill, sch 1 s 8.
101 ibid., sch 1 s 5.
102 ibid., sch 1 s 11.
103 Patrick F. Walsh Submission, p.15.

role should be explicitly recognised as one of the Committee's functions in the *Intelligence Services Act 2001* (ISA), and note that this recognition would be consistent with the role of current and prospective Parliamentary Committees in the Five Eyes community. Proposals in the PJCIS Amendment Bill to enhance interactions between the Monitor and the PJCIS – which we support – would significantly assist the PJCIS in this role. Accordingly, **we recommend that the Committee's role in reviewing proposed reforms to counter-terrorism and national security legislation should be specifically recognised in the ISA as one of its functions. We also recommend that:**

a) **the Committee have a role in reviewing legislation which is about to expire – either by conducting the review itself or referring the matter to the Monitor for inquiry and report; and**

b) **the role of the Committee be expanded to enable it to conduct own-motion inquiries consistent with this expanded remit to cover the administration and expenditure of the ten intelligence agencies of the NIC as well as proposed or existing provisions in counter-terrorism and national security law.**

7.36 It is important that the PJCIS and Director-General of ONI (DG ONI) closely interact, particularly as ONI would subsume ONA's current strategic foreign intelligence assessment role and would have a significant co-ordination and evaluation role in relation to NIC agencies. We consider DG ONI should brief the Committee at least twice a year, including as part of the PJCIS's annual review of administration and expenditure but also in relation to the role of DG ONI in enhancing co-ordination across the NIC. Accordingly, **we recommend that the PJCIS receive regular briefings from DG ONI**.

The PJCIS and Oversight of Operations

7.37 We have given much thought to arguments in support of PJCIS oversight of intelligence operations. This is an important feature of the PJCIS Amendment Bill and we received views both strongly in support and firmly opposed. The Queensland Council for Civil Liberties argued that empowering the Committee to review operational activities would be consistent with oversight arrangements in a number of comparable overseas jurisdictions. It argued that claims to secrecy, while "a legitimate area of concern" for intelligence agencies, are often overstated and less justifiable as agencies now have "distinct powers to affect the rights of Australians."[104]

104 The Queensland Council for Civil Liberties Submission, p.8.

7.38 Conversely, it was clear to us from the views expressed in a number of meetings that there are concerns that PJCIS oversight of operational matters, in particular that it would duplicate existing oversight provided by the responsible Minister, by IGIS and by the Monitor. In our view, these concerns have substance and validity, and they need to be taken into account in any proposed changes to oversight arrangements.

7.39 While a democracy does require effective Parliamentary oversight of intelligence agencies, we consider expanding the role of the PJCIS to include own-motion inquiry into the operational activities of intelligence agencies is not required to ensure agencies are operating effectively, legally and with propriety. In reaching this conclusion, we have looked at the operation of Australia's existing oversight system as a whole rather than its individual component parts in isolation. Further informing our view has been an examination of the legislation governing Parliamentary committees in comparable Five Eyes jurisdictions, in particular the United Kingdom and Canada. Such legislation limits, to varying degrees, Parliamentary oversight of operations.

7.40 In the United Kingdom, the Intelligence and Security Committee of Parliament oversees the operations of intelligence agencies and can request agencies disclose information to the Committee.[105] The Committee must make an annual report and may make any other report on its functions to the United Kingdom Parliament, but only after sending the report to the Prime Minister.[106] The Committee excludes anything from a report if the Prime Minister considers the matter would be prejudicial to the continued discharge of the functions of the United Kingdom's intelligence agencies or any person carrying out activities in relation to intelligence and security matters.[107]

7.41 In Canada, the proposed National Security and Intelligence Committee of Parliamentarians (NSIC) will be able to review "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."[108] The enabling Bill specifically provides that, while NSIC members must be Members of Parliament, the NSIC is not a committee of either House of Parliament or of both Houses.[109] The NSIC will report to the Prime Minister. If the Prime Minister believes there is information in a report disclosure

105 *Justice and Security Act 2013* (United Kingdom), s 1.
106 ibid., s 3(1), (2) and (3).
107 ibid., s 3(4).
108 National Security and Intelligence Committee of Parliamentarians Bill 2016, clause 8.
109 ibid., cl 4(3).

of which would be injurious to national security, national defence or international relations, the Prime Minister may direct the NSIC to submit a revised report that does not contain such information.[110]

7.42 In the Australian context, we consider the responsible Ministers are best placed to judge the effectiveness of the operations of the agencies and to be accountable for them to the Parliament and the broader Australian community. Ministers have the information, insights and powers necessary to perform this role and they have the ability to engage with the PJCIS by referring matters to it.

7.43 In our view, it is appropriate and effective for the primary oversight of the legality and propriety of operations conducted by intelligence agencies to be carried out by the IGIS Office. With the exception of New Zealand, none of the Five Eyes partners has an oversight body directly comparable to the IGIS. Our recommendations concerning the IGIS (paragraphs 7.23 to 7.27) are designed to ensure that the IGIS Office can exercise comprehensive and rigorous oversight of intelligence community operations. We assess there is significant practical benefit in having the required expertise located in a single body, backed by appropriate powers and independence. Giving the PJCIS a role to conduct its own inquiries into the operations of the intelligence agencies would duplicate the reporting requirements already in place for AIC agencies in respect of the IGIS. It would also duplicate resourcing needs of the IGIS and PJCIS and it could result in simultaneous inquiries by both the PJCIS and the IGIS on the same issue.

7.44 Rather than giving the PJCIS the power to conduct its own inquiries into agency operations, we favour strengthening the connection between the PJCIS and the IGIS. This would increase the Parliament's visibility of the issues raised by the activities of the intelligence agencies without introducing duplication.

7.45 **We recommend that the ISA be amended to enable the PJCIS to request the IGIS conduct an inquiry into the legality and propriety of particular operational activities of the NIC agencies, consistent with the IGIS's remit, and to provide a report to the Committee, the Prime Minister and the responsible Minister.** This provision, including the reporting arrangements, would operate in accordance with the relevant sections in the IGIS

110 National Security and Intelligence Committee of Parliamentarians Bill 2016, cl 21(1) and (5).

Act relating to the conduct of inquiries and reports of inquiries.[111] Furthermore, we consider it would be appropriate for the IGIS to consult with the relevant agency Heads and responsible Ministers before providing a report to the PJCIS, even when the report is not critical of a Commonwealth agency.

7.46 A similar power is included in the New Zealand *Intelligence and Security Act 2017*, which provides that New Zealand's Intelligence and Security Committee of Parliament may "request the Inspector-General to conduct an inquiry into any matter relating to an intelligence and security agency's compliance with New Zealand law" or "the propriety of particular activities of an intelligence and security agency."[112] The New Zealand Committee's request may relate to operationally sensitive matters. The New Zealand Inspector-General must provide a report on that inquiry to the Committee, complementing the requirement that the Inspector-General provide reports on completed inquiries conducted on own motion, or at the request of the responsible Minister or Prime Minister.[113]

7.47 **We also recommend the IGIS be required to brief the Committee at regular intervals on investigations into the NIC agencies.** While the Committee may request a briefing from the IGIS under section 30 of the ISA, we understand such briefings only occur in the context of Committee inquiries into the administration and expenditure of agencies or proposed legislative reform.[114] In our view, the ISA should be amended to require the IGIS to provide briefings at least four times a year to the Committee on the IGIS Office's investigations into the legality and propriety of activities conducted by NIC agencies and any complaints against NIC agencies. Regular briefings would also be consistent with the IGIS's public outreach function. Furthermore, it would provide Committee members with a broader view on the role of the IGIS, the IGIS's interactions with and investigations into intelligence agencies, and findings on compliance standards across the intelligence community.

111 In particular, section 17 of the IGIS Act contains provisions relating to the conduct of inquiries and provides that the IGIS shall not make a report in relation to an inquiry which sets out opinions that are critical of a Commonwealth agency, unless the IGIS has, before completing the inquiry, given the Agency Head a reasonable opportunity to appear before the IGIS and make submissions in relation to the inquiry. Section 17 also provides that the IGIS shall not make a report setting out opinions that are critical of a Commonwealth agency, unless the IGIS has given the responsible Minister an opportunity to discuss the proposed report with the IGIS. In addition, section 21 of the IGIS Act notes that the IGIS must provide a copy of a draft report into a completed inquiry to an Agency Head and the Agency Head is able to comment on the draft report within a reasonable time after being given the draft agency copy.

112 New Zealand *Intelligence and Security Act 2017,* s 193(1)(e).

113 ibid., s 185(3) and (4).

114 See, for example, *Submission to the Parliamentary Joint Committee on Intelligence and Security–Inquiry into the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015* (10 December 2015) and *Submission to the Parliamentary Joint Committee on Intelligence and Security–Review of Administration and Expenditure No. 13 (2013-2014)* (3 December 2014).

[This page intentionally left blank]

APPENDICES

APPENDIX 1: PRIME MINISTER'S MEDIA RELEASE

PRIME MINISTER
THE HON. MALCOLM TURNBULL MP

MEDIA RELEASE

7 November 2016

Independent Intelligence Review

The Government has commissioned an independent review into Australia's intelligence agencies.

This is an opportunity to assess whether our current intelligence arrangements, structures and mechanisms are best placed to meet the security challenges we are likely to face in the years ahead.

Consistent with previous reviews conducted in 2004 and 2011, this process will examine how our intelligence community serves Australia's national interest. The review will consider the ongoing suitability of legislative and oversight provisions.

I have asked Professor Michael L'Estrange AO and Mr Stephen Merchant PSM to conduct the review and report to the Government in the first half of 2017. The Reviewers will also provide a public version of their report.

Professor L'Estrange and Mr Merchant are eminently qualified to undertake this review. Professor L'Estrange has held several senior public service appointments, including Secretary of the Department of Foreign Affairs and Trade and Australia's High Commissioner to the United Kingdom. He was the inaugural Head of the National Security College at the Australian National University and the inaugural Executive Director of the Menzies Research Centre in Canberra. He also served on the staff of Mr Justice Hope's second Royal Commission into Australia's security and intelligence agencies.

Mr Merchant has held senior positions in Defence and Australia's intelligence community, including Director of the Defence Signals Directorate and the Deputy Secretary responsible for the three Defence intelligence agencies. In addition, Mr Merchant has extensive experience in defence strategy, international policy, defence capability development and working with the intelligence communities of our major allies.

I have also asked Sir Iain Lobban KCMG CB to assist the reviewers. Sir Iain will bring valuable overseas intelligence experience and insights to review deliberations, having been the Director of the United Kingdom's Government Communications Headquarters, which is the UK counterpart of our Australian Signals Directorate. He was also a member of the expert panel for Australia's 2016 Cyber Security Strategy, which was released in April this year.

Public submissions can be made to the review at intelligencereview@pmc.gov.au or by post to '2017 Independent Intelligence Review' c/o Department of the Prime Minister and Cabinet, PO Box 6500 Canberra, ACT 2600. The closing date for public submissions is 4 January 2017.

Further information on the review, including the Terms of Reference, is available online.

APPENDIX 2: LIST OF INTERVIEWS AND SUBMISSIONS

Interviews

Government Ministers

The Hon Malcolm Turnbull MP, Prime Minister

The Hon Barnaby Joyce MP, Deputy Prime Minister

The Hon Julie Bishop MP, Minister for Foreign Affairs

Senator the Hon George Brandis QC, Attorney-General

Senator the Hon Mathias Cormann, Minister for Finance

The Hon Scott Morrison MP, Treasurer

Senator the Hon Marise Payne, Minister for Defence

The Hon Michael Keenan MP, Minister for Justice and Minister Assisting the Prime Minister on Counter-Terrorism

The Hon Peter Dutton MP, Minister for Immigration and Border Protection

The Hon Dan Tehan MP, Minister Assisting the Prime Minister on Cyber Security

Senator the Hon Arthur Sinodinos AO, then Cabinet Secretary

Parliament and Former Members

The Hon Michael Sukkar MP, then Chair Parliamentary Joint Committee on Intelligence and Security

Mr Andrew Hastie MP, Chair Parliamentary Joint Committee on Intelligence and Security

The Hon Anthony Byrne MP, Deputy Chair Parliamentary Joint Committee on Intelligence and Security

Mr Julian Leeser MP

The Hon Mark Dreyfus MP QC, Shadow Attorney-General and Shadow Minister for National Security

The Hon Tony Abbott MP

The Hon Richard Marles MP, Shadow Defence Minister

The Parliamentary Joint Committee on Intelligence and Security

The Hon Philip Ruddock (Former MP and Member of PJCIS)

Australian Public Service and Australian Defence Force (Principals Only)

Mr Neil Orme PSM, Director Australian Geospatial-Intelligence Organisation

Mr Bruce Miller, A/g Director-General Office of National Assessments

Mr Richard Maude, then Director-General Office of National Assessments and later Head of the Foreign Policy White Paper Taskforce

Mr Nick Warner AO PSM, Director-General Australian Secret Intelligence Service

Mr Duncan Lewis AO DSC CSC, Director-General Australian Security Intelligence Organisation

Dr Paul Taloni PSM, Director Australian Signals Directorate

Air Vice-Marshal John McGarry AM CSC, then Director Defence Intelligence Organisation

Major General Matthew Hall AM CSC, Director Defence Intelligence Organisation

Mr Andrew Colvin OAM APM, Commissioner Australian Federal Police

Mr Chris Dawson APM, CEO Australian Criminal Intelligence Commission

Mr Chris Moraitis PSM, Secretary Attorney-General's Department

Mr Mike Pezzullo, Secretary Department of Immigration and Border Protection

Mr Roman Quaedvlieg APM, Commissioner Australian Border Force

Mr Paul Jevtovic APM, then CEO Australian Transaction Reports and Analysis Centre

Mr Peter Clarke, A/g CEO Australian Transaction Reports and Analysis Centre

The Hon Margaret Stone, Inspector-General of Intelligence and Security

Dr Heather Smith PSM, Secretary Department of Communications and the Arts

Ms Rosemary Huxtable PSM, Secretary Department of Finance

Ms Frances Adamson, Secretary Department of Foreign Affairs and Trade

Mr Dennis Richardson AO, then Secretary Department of Defence

Air Chief Marshal Mark Binskin AC, Chief of the Defence Force

Vice Admiral Ray Griggs AO CSC, Vice Chief of the Defence Force

Vice Admiral David Johnston AM, Chief of Joint Operations

Mr John Fraser, Secretary to the Treasury

Mr Brendan Sargeant, then Associate Secretary Department of Defence and later A/g Secretary of Defence

Dr Martin Parkinson AC PSM, Secretary Department of the Prime Minister and Cabinet

Mr Allan McKinnon, Deputy Secretary Department of the Prime Minister and Cabinet

Ms Celia Perkins, First Assistant Secretary Security and Vetting Service

Ms Rebecca Skinner, Deputy Secretary Department of Defence

Dr Alex Zelinsky AO, Chief Defence Scientist

Ms Lynwen Connick, then First Assistant Secretary Department of the Prime Minister and Cabinet

Mr Tony Sheehan, Commonwealth Counter-Terrorism Co-ordinator

Ms Dara Williams, Open Source Centre Office of National Assessments

Mr Alastair MacGibbon, Special Adviser to the Prime Minister on Cyber Security

Mr Clive Lines, Co-ordinator Australian Cyber Security Centre

Other interlocutors

Dr James Renwick SC, A/g Independent National Security Legislation Monitor

Mr Robert Cornall AO

Dr Doug Kean PSM

Mr Allan Behm

Mr Kim Jones AM

Mr Martin Brady AO

Professor Hugh White AO

Professor Rory Medcalf

Mr David Irvine AO

Mr Peter Jennings PSM

Mr Ric Smith AO PSM

Sir Angus Houston AK AFC

Dr Margot McCarthy

Emeritus Professor Paul Dibb AM

Mr Frank Lewincamp PSM

Dr Michael Fullilove

Mr Peter Varghese AO

Dr Vivienne Thom AM

Mr Ian McKenzie PSM

Mr Ashton Robinson

Lieutenant Colonel Nick Rose

The Reviewers also held discussions with key interlocutors from the United States, United Kingdom, Canada and New Zealand.

Submissions Received

The Review received Submissions from the following government departments and agencies:

- Attorney-General's Department
- Australian Criminal Intelligence Commission
- Australian Federal Police
- Australian Geospatial-Intelligence Organisation
- Australian Secret Intelligence Service
- Australian Security Intelligence Organisation
- Australian Signals Directorate
- Australian Transaction Reports and Analysis Centre
- Defence Intelligence Organisation
- Department of Defence
- Department of Foreign Affairs and Trade
- Department of Finance
- Department of Immigration and Border Protection
- Department of the Prime Minister and Cabinet
- Office of National Assessments

The Review also received public Submissions from:

- Queensland Council for Civil Liberties
- Dynamic Alternatives
- Data to Decisions Co-operative Research Centre
- Law Council of Australia
- Veriluma Software
- Australian Institute of Professional Intelligence Officers
- John M. Schmidt
- Dr Anthony Bergin and Ms Kate Grayson
- Associate Professor Patrick F. Walsh
- Mr Paul Wayper
- Mr Ashton Robinson
- Ms Corinne Caqueux
- Mr Peter Grullemans
- Mr Steven Weathers
- Mr Peter Jennings PSM
- Mr Kevin Monks
- Mr John Wilson
- Mr Cameron Skirving
- Mr Ian Dudgeon

APPENDIX 3: KEY ACRONYMS

ACIC	Australian Criminal Intelligence Commission
ADF	Australian Defence Force
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGO	Australian Geospatial-Intelligence Organisation
AGSVA	Australian Government Security Vetting Agency
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
DFAT	Department of Foreign Affairs and Trade
DIBP	Department of Immigration and Border Protection
DIO	Defence Intelligence Organisation
GEOINT	Geospatial Intelligence
HUMINT	Human Intelligence
ICT	Information and Communication Technology
IGIS	Inspector-General of Intelligence and Security
NIC	National Intelligence Community
NICC	National Intelligence Co-ordination Committee
NICMC	National Intelligence Collection Management Committee
NIPs	National Intelligence Priorities
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PM&C	Department of the Prime Minister and Cabinet
ONA	Office of National Assessments
SIGINT	Signals Intelligence