Independent Intelligence Review

2024

2024 Independent Intelligence Review

2024 Independent Intelligence Review

ISBN [978-1-925365-71-9] (PDF)

Copyright Notice

Third party copyright

Attribution

This publication should be attributed as follows:

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the following website: https://pmc.gov.au/cca

Other uses

Enquiries regarding this document are welcome at:

Department of the Prime Minister and Cabinet
PO Box 6500
CANBERRA ACT 2600

Contents

Chapter 1. Executive summary **6**
A Review in three parts 7
Chapter 2. Table of recommendations 10
Chapter 3. Terms of Reference and consultation 19
Consultation 20
Part I: Foundations **22**
Chapter 4. The global context 23
Contest and fragmentation 23
Technology 25
Climate change 26
Other transnational issues 26
Implications for the NIC 27
Chapter 5. Intelligence principles and foundations 32
What is intelligence? 32
Intelligence as a tool of statecraft 32
Roles and responsibilities 33
Accountability, trust and the role of oversight 37
Part II: Reflections on past reform **38**
Chapter 6. The National Intelligence Community since 2017 39
The 2017 Independent Intelligence Review – managing the NIC as an enterprise 39
Chapter 7. The National Intelligence Community's evolving architecture 49
From six to ten – strength in numbers 49
The Office of National Intelligence 50
The Australian Signals Directorate 50
Establishment of the Defence Intelligence Group 50
Australian Geospatial-Intelligence Organisation 51
Establishment of Home Affairs and changes to portfolio structures 51
Part III: Positioning for the future **52**
Chapter 8. Building on intelligence community strengths 53
Chapter 9. Intelligence and Australian statecraft 55
Intelligence support for ministers 56

Intelligence and policy 58
Economic security 60
Value of contestability 62
Effects and intelligence diplomacy 64
Chapter 10. Preparedness 65
Collective and coordinated efforts 65
Chapter 11. National Intelligence Community investment 70
Major NIC programs 70
Coordinating and prioritising NIC investment 72
Joint Capability Fund 73
Chapter 12. Collective capabilities and shared services 74
Chapter 13. Technology 76
Current approaches 76
The TOP SECRET Cloud 77
Data 77
Artificial intelligence 78
Innovation 80
Technology strategy 82
Regulatory considerations 82
Chapter 14. Insight and advantage through open source 86
The OSINT landscape 86
Implications for the NIC 86
Delivering capability 87
Partnerships 90
Open source and covert collection 90
Chapter 15. Collective action on people and skills 92
Attraction and retention 92
Clearances 96
Organisational suitability assessments 97
Talent management, leadership and culture 97
Training 98
A Chief People Officer 98
Chapter 16. Partnerships 100
Domestic partners 100
International partners 102

Chapter 17. Legislation 103
Electronic surveillance reform 103
Other legislative changes 105
Chapter 18. Oversight 110
The jurisdiction of the IGIS and PJCIS – Intelligence Services Legislation Amendment Bill 2023 110
Proposed changes to oversight powers, information sharing and resourcing 113
Oversight resourcing 115
Appendix A: Media release 118
Appendix B: Terms of Reference 119
Appendix C: List of interviews and submissions 120
Interviews 121
Submissions 124
Appendix D: Glossary 126

Chapter 1. Executive summary

Note: While information within this report was accurate at the time the Review was finalised, some additional amendments have been made throughout the declassification process to ensure the currency of information.

1.01 Since 2004, periodic independent reviews of Australia's intelligence community have been conducted to give Australian governments and the Australian people assurance that the nation has a well-governed, effective intelligence service.

1.02 The current review, announced by Prime Minister the Hon Anthony Albanese MP in September 2023, was timely.

1.03 The pace and scale of change since the last independent review in 2017 are remarkable. The world in which Australia seeks security and prosperity is significantly more contested, fragmented and volatile. Major-power conflict is no longer unimaginable. New security threats are prominent, many amplified by technological change. The fragility of borders, a feature of our security landscape for some time, is more evident than ever. Australia faces both a more dangerous international environment and a growing need to defend itself against threats to its democracy, social cohesion and essential infrastructure.

1.04 The recent past has also been a period of significant change for the National Intelligence Community (NIC). The 2017 Independent Intelligence Review (2017 Review) was perhaps the most consequential since the Hope royal commissions, making important changes to the structure and operation of the intelligence community, including establishing the Office of National Intelligence (ONI).

1.05 A comprehensive review of Australia's intelligence laws was conducted in 2019 and was followed by significant legislative reform. And additional funding is helping intelligence agencies to modernise and meet new and complex missions.

1.06 This is the context in which the 2024 Independent Intelligence Review (the Review) conducted its work. The Review's Terms of Reference were broad, but our most important tasks were twofold: first, to gauge the effectiveness with which the NIC serves the national interest and meets the needs of government; and, second, to examine how well positioned the community is for the future.

1.07 In a challenging security environment, Australia's intelligence agencies work hard and with considerable success to protect the nation and support government priorities. Like all major reforms, the restructure and expansion of the intelligence community following the 2017 Review was not always smooth or easy. Still, the NIC today is a more capable and integrated intelligence enterprise as a result.

1.08 Australia's international intelligence partnerships, especially but not exclusively within the Five Eyes group, are deep and healthy. Australia gains significantly from these – information, technology and other support that it could not possibly generate alone – but also makes its own valuable and valued contribution. Indeed, Australia and its geography are becoming more important to efforts to improve the collective resilience of the Five Eyes enterprise in the event of a crisis or conflict.

1.09 Overall, we find that the NIC is highly capable and performing well. Even so, in a high-stakes era, we have identified areas in which greater – or different – collective responses are required so that the intelligence community can more effectively serve the national interest and meet the needs of government in the future.

1.10 The recommendations in this Review are informed by the following principal findings:

- First, welcome progress has been made towards the vision of the 2017 Review for a world-class intelligence community in which the strengths of individual agencies are complemented by stronger enterprise-level management. Integration and coordination across Australia's national intelligence enterprise have improved. Even so, there remains at times an imbalance between what ONI is expected to achieve by government and ONI's ability to bring the rest of the intelligence community along with it. Greater integration is possible on some issues. And more can be done to institutionalise a deep and genuine culture of collaboration and the idea of 'community'.
- Second, if stronger enterprise management of the NIC was the major theme of the 2017 Review, a complementary focus of this Review is the need for deeper integration of intelligence with other arms of government. Closer, more effective working relationships will ensure the intelligence community's output aligns closely with government priorities. It will also ensure intelligence is used systematically as a tool of statecraft to maximise Australia's competitive edge in this challenging era.
- Third, intelligence agencies must innovate in order to keep pace with a shifting landscape of national security threats. Four interlinked challenges are especially consequential. Intelligence agencies must be well prepared for a future crisis or conflict. They must successfully deploy new technologies, such as artificial intelligence (AI). They must continue to invest in international partnerships and develop stronger ones outside government. And they must be able to recruit, retain and train a highly skilled and committed workforce.

A Review in three parts

1.11 Part I of this Review describes the major trends influencing Australia's national security and explains what they mean for intelligence agencies. We also discuss some of the most important principles that underpin the design and operation of the intelligence community. We hope these chapters will help members of the public who may read this Review to better understand how Australia's intelligence community works and the important role it plays in protecting Australia and Australians.

1.12 As required by our Terms of Reference, Part II of the Review reflects on lessons learned from the 2017 Review and the 2019 Comprehensive Review of intelligence legislation (2019 Comprehensive Review). We also map changes to the structure and functions of agencies.

1.13 The 2017 and 2019 reviews reformed the operation and oversight of the intelligence community. Some ambitions have not, however, been fully realised. Continuing to build collective capabilities and ensuring effective coordination of Australia's intelligence community must remain a priority. In particular, we make recommendations to reinforce

ONI's leadership of the community and its enterprise management role. In this we build on the foundations laid down by the 2017 Review.

1.14 A central recommendation from the 2019 Comprehensive Review not yet implemented is a new single Act governing the use of electronic surveillance powers. The need for this reform is becoming more urgent.

1.15 Part III of the Review looks forward. We emphasise the decision making advantages that come with effective use of intelligence. Optimising the integration of intelligence and policy for an age of heightened risk and challenge requires change in both intelligence and policy agencies, including new investment in 'enablers' like clearances and secure information and communications technology systems.

1.16 The business model for meeting the intelligence needs of executive government is no longer keeping up with demand and needs re-imagining so that a broader range of ministers can be supported more regularly, including in capitals other than Canberra.

1.17 The Review examined the structures that support economic security decision making, an emerging area of policy in which national security risks are becoming more challenging to manage and where gaps in processes to support government are the greatest. We recommend a holistic approach, proposing both an uplift in intelligence support and a matching review by the Treasury of the architecture for economic security policy making. In our judgement, a system re-design is needed.

1.18 We also propose stronger central coordination of national security policy matters, such as resourcing, intelligence requirements and legislation, by the Department of the Prime Minister and Cabinet.

1.19 Contestability – subjecting analytical judgements to rigorous challenge – is essential to robust intelligence assessment. It is more important than ever in a complex, fast-changing world. We build on existing contestability processes to help ensure a diverse range of expertise is brought to bear by ONI on analytical challenges.

1.20 Open source intelligence (OSINT) is an increasingly powerful source of intelligence insight and decision-making advantage. While we recommend retaining the current 'federated' model for the production of OSINT in the intelligence community, with a leadership role for ONI, all NIC agencies need to invest in OSINT tradecraft and technology and in partnerships with the private sector.

1.21 In Part III we also make proposals to strengthen the capabilities, resilience, skills and capacity for innovation that are essential for the intelligence community to meet the demands of the current era. We pay particular attention to workforce, technology and preparedness, but also make recommendations to improve government consideration of major NIC capability investments. We range widely in these sections, but among our conclusions are: the need to bolster the NIC's strategic warning capability; the desirability of a national security-focused investment fund to bring new technologies into the intelligence community; and additional measures to support governance of AI technology in intelligence agencies.

1.22 We emphasise the vital importance of strong partnerships to the NIC's ability to meet current challenges and prepare for future ones. Australia's international intelligence

relationships are in good shape but there is scope to give more substance to the NIC's partnerships with the private sector and research institutions.

1.23 We recommend a small number of legislative changes to help agencies keep pace with technological or other changes.

1.24 Australia's multilayered system of oversight is working effectively, supporting compliance with the law and protecting the rights of Australians.

1.25 Nonetheless, a larger intelligence community, the high tempo of intelligence effort and the complex implications of technological change all put pressure on Australia's oversight mechanisms. So too has the weight of new or amended legislation in recent years. In our judgement, some modest additional support is necessary.

1.26 We are conscious the global trends identified in this report will keep driving consequential change. Much of this will challenge Australia's security and prosperity. Continuing the tempo of independent intelligence reviews every five to seven years would be appropriate. One conclusion of this Review is that maximising the value of reform in the intelligence community sometimes requires matching change in the policy community. There may also therefore be a need for government to look more regularly at the intersections between intelligence and government policy making architecture.

1.27 The recommendations in this Review are based on a nine-month survey of the Australian intelligence enterprise. The insights we gained from discussions with ministers were important in framing our recommendations. We are also grateful for the extensive support we received from intelligence community leaders and their agencies, and for their patience in answering our many questions. As previous reviews have done, we worked closely with policy agencies to understand both how they use intelligence now and how they envisaged their future intelligence requirements.

1.28 Finally, we wish to record our admiration and gratitude for the members of the Review Secretariat, without whom this report would not have been possible.

1.29 More than ever, a world-class intelligence enterprise is a national asset – an element of national power and an arm of statecraft essential to the successful prosecution of Australia's national interests. We hope the proposals in this Review build on the strengths of the NIC and by so doing enhance and protect Australia's security, prosperity and values.

Dr Heather Smith PSM
Reviewer

Mr Richard Maude
Reviewer

Chapter 2. Table of recommendations

Role of the Office of National Intelligence

Recommendation 1 **p.41**

That the Prime Minister writes to the intelligence community with a statement of expectations at the beginning of each term of government.

Recommendation 2 **p.41**

That the Director-General of National Intelligence be made a member of relevant sub-committees of the Secretaries Board.

Enterprise management

Recommendation 3 **p.41**

That the Office of National Intelligence receive an uplift in resourcing to support additional leadership and enterprise management responsibilities.

Recommendation 4 **p.42**

That, informed by a survey, the Department of the Prime Minister and Cabinet conduct an annual evaluation of intelligence support for policy and decision making.

Recommendation 5 **p.42**

That the NIC more clearly articulate the allocation and reprioritisation of resources against the intelligence missions.

Recommendation 6 **p.46**

That capability reviews be considered following the appointment of a NIC agency head. For those agencies under the *Public Service Act 1999*, this review should be performed by the Australian Public Service Commission. Otherwise, these reviews should be self-initiated.

Intelligence support for ministers

Recommendation 7 **p.57**

That the Directors-General of National Intelligence and Security develop an ‘Introduction to Intelligence’ briefing for ministers and appropriately cleared ministerial staff. This briefing should be offered after a change of government or following a ministerial reshuffle, and could also be made available on request at other times.

Recommendation 8 **p.57**

That, building on briefings already provided to the National Security Committee of Cabinet on the foreign and domestic security environment, the Directors-General of National Intelligence and Security provide dedicated annual or six-monthly oral briefings to the full Cabinet on shifts in Australia's security environment with particular implications for the operation of government, such as espionage and foreign interference.

Recommendation 9 **p.57**

That the Office of National Intelligence provide more regular customer support to a broader range of ministers and strengthen its ability to deliver timely intelligence advice, including outside Canberra.

Policy and intelligence

Recommendation 10 **p.58**

That the Department of the Prime Minister and Cabinet be resourced to provide stronger central coordination of national security policy matters.

Recommendation 11 **p.59**

That policy agencies invest in adequate classified infrastructure and other enablers to allow the most effective use of intelligence to inform policy making.

Recommendation 12 **p.60**

That the NIC develop a coordinated intelligence outreach and education initiative to the policy community that recognises the distinct roles of agencies while leveraging the National Intelligence Academy where appropriate.

Economic security

Recommendation 13 **p.61**

That the Treasury lead a broad review of the structure and effectiveness of economic security functions across government.

Recommendation 14 **p.62**

That a distinct economic security function be established in the Treasury, including secondees from relevant NIC agencies.

Recommendation 15 **p.62**

That the capacity of the Office of National Intelligence to support economic security decision making be strengthened.

Value of contestability

Recommendation 16 **p.63**

That the Office of National Intelligence bolster its contestability processes for analytical products by: convening intelligence and policy agency roundtable discussions on selected intelligence assessments on major global challenges; making more use of structured analytical techniques; and acknowledging differences of analytical perspectives, where they might exist.

Recommendation 17 **p.64**

That the Office of National Intelligence produce at least two National Assessments each calendar year.

Public release of intelligence

Recommendation 18 **p.64**

That the Office of National Intelligence and relevant policy agencies develop a policy for the declassification and public release of intelligence.

Preparedness

Recommendation 19 **p.65**

That the Office of National Intelligence appoint a senior officer to coordinate NIC preparedness for regional crises or conflicts and track progress against activity.

Recommendation 20 **p.66**

That the Prime Minister issues a directive under the *Office of National Intelligence Act 2018* to set out expectations for NIC preparedness for regional crises or conflicts.

Recommendation 21 **p.66**

That regular exercises be undertaken within the NIC and with policy agencies to test and improve preparedness for regional crises or conflicts.

Recommendation 22 **p.67**

That the Department of Finance and the NIC lead scoping of options to build NIC resilience and engagement outside Canberra.

Recommendation 23 **p.68**

That a cell be established in the Office of National Intelligence to develop warning tradecraft, bolster its warning functions and strengthen the NIC-wide warning network.

Recommendation 24 **p.68**

That the Office of National Intelligence produce a National Assessment each year to chart emerging trends likely to threaten Australia's security and prosperity.

Recommendation 25 **p.68**

That the Director-General of National Intelligence continues to provide an annual high-level overview of emerging trends and issues that present risks to Australia to the National Security Committee of Cabinet.

NIC investment

Recommendation 26 **p.72**

That a holistic overview of the status and risks of major NIC programs be presented annually to the National Security Committee of Cabinet.

Recommendation 27 **p.72**

That NIC advice to government detail current and future capability gaps and major investment requirements for each NIC agency.

Recommendation 28 **p.73**

That the scope of the Joint Capability Fund be narrowed to focus on delivering key enterprise level capability for the NIC.

Collective capabilities and shared services

Recommendation 29 **p.75**

That the NIC adopt a more systematic approach to the identification, evaluation and pursuit of collective capabilities and shared services.

Technology

Recommendation 30 **p.77**

That all relevant NIC agencies develop TOP SECRET Cloud transition strategies.

Recommendation 31 **p.78**

That NIC agencies prioritise support to data cataloguing efforts to maximise opportunities for data interoperability.

Recommendation 32 **p.80**

That the NIC develop intelligence community-wide artificial intelligence governance principles and artificial intelligence public messaging principles.

Recommendation 33 **p.80**

That NIC agencies consider appointing a Senior Executive Service officer to support the development and deployment of Artificial Intelligence.

Recommendation 34 **p.80**

That all Senior Executive Service officers in the NIC undertake training to better understand the applications, risks and governance requirements of artificial intelligence in the intelligence context.

Recommendation 35 **p.80**

That NIC agencies develop artificial intelligence governance frameworks to support the internal development and deployment of artificial intelligence.

Recommendation 36 **p.82**

That government scope the establishment of a national security focused technology investment fund.

Recommendation 37 **p.82**

That the NIC develop a technology strategy to articulate the enterprise-level vision, requirements, priorities, and risks regarding the current and future technological environment.

Recommendation 38 **p.83**

That the Independent National Security Legislation Monitor undertake a review of the legislative context around the NIC's current use of artificial intelligence to inform legislative and policy changes.

Recommendation 39 **p.84**

That the *Intelligence Services Act 2001* be updated to expand the application of agency privacy rules to include reference information.

Recommendation 40 **p.85**

That the Attorney-General's Department consider what, if any, regulation would be required to enable NIC agencies to combine and interrogate multiple datasets (including reference information) for the purposes of proactively identifying criminal and national security concerns.

Insight and advantage through open source

Recommendation 41 **p.88**

That the NIC's federated approach to open source intelligence under the functional leadership of the Office of National Intelligence continue. The Office of National Intelligence's leadership role should be strengthened by additional investment in the skills and capabilities needed to build an integrated community of practice.

Recommendation 42 **p.89**

That the next independent intelligence review consider how open source intelligence functions are best organised across the intelligence community to ensure optimal intelligence outcomes for government.

Collective action on people and skills

Recommendation 43 **p.94**

That a NIC-wide employee value proposition be developed to inform branding and recruitment campaigns.

Recommendation 44 **p.95**

That the Office of National Intelligence publish aggregated NIC diversity statistics and gender pay gap data annually.

Recommendation 45 **p.95**

That the Office of National Intelligence work with NIC agencies to develop a more consistent approach to data collection on NIC workforce trends.

Recommendation 46 **p.96**

That the Office of National Intelligence lead the development of a program to support intra-community mobility.

Recommendation 47 **p.96**

That adequate investment and resources be provided for the TOP SECRET-Privileged Access Vetting Authority to achieve a single high-assurance vetting standard, enable staff mobility in the NIC and harden the community against compromise.

Recommendation 48 **p.97**

That security clearance processes at different levels be optimised via a phased approach, leveraging efficiencies from the TOP SECRET-Privileged Access Capability.

Recommendation 49 **p.97**

That NIC agencies utilising organisational suitability assessments continue to identify opportunities to harmonise processes to facilitate intra-community mobility, including leveraging TOP SECRET-Privileged Access clearances.

Recommendation 50 **p.98**

That current leaders and staff with potential to become future leaders in the NIC be identified, independently assessed and nurtured via Australian Public Service Commission talent programs.

Recommendation 51 **p.98**

That, in consultation with secretaries and agency heads, a regular succession scan for NIC agency leadership be commenced, as part of the Australian Public Service–wide enterprise succession scans led by the Secretaries Talent Council.

Recommendation 52 **p.98**

That the National Intelligence Academy continue in existence and be funded accordingly.

Recommendation 53 **p.99**

That a NIC Chief People Officer be established in the Office of National Intelligence.

Partnerships

Recommendation 54 **p.102**

That the NIC establish a public–private talent exchange to deepen partnerships with private industry through knowledge and capability sharing.

Legislation

Recommendation 55 **p.104**

That the 2019 Comprehensive Review of intelligence legislation's recommendation for holistic electronic surveillance reform be implemented as a matter of priority.

Recommendation 56 **p.104**

That as part of the electronic surveillance reform project, government revise the range of communications providers subject to electronic surveillance obligations in order to provide clarity and better reflect the entities involved in the modern telecommunications system.

Recommendation 57 p.105

That the *Telecommunications (Interception and Access) Act 1979* and *Australian Security Intelligence Organisation Act 1979* be amended urgently, and in advance of holistic electronic surveillance reform if necessary, to enable the Australian Security Intelligence Organisation to obtain interception and computer access warrants against particular groups. If progressed ahead of holistic reform, it would be appropriate that these amendments implement relevant safeguards recommended by the 2019 Comprehensive Review of intelligence legislation.

Recommendation 58 p.106

That the *Intelligence Services Act 2001* be amended to enable NIC agencies to obtain ministerial authorisations in relation to Australians working for a broader range of companies that are acting on behalf of a foreign government, but that are not subject to actual control or direction. This could be done by adopting the definition of 'foreign public enterprise' in the *Criminal Code Act 1995*.

Recommendation 59 p.107

That government review the appropriate legislative settings for foreign intelligence requirements onshore, having regard to the principles underlying the foundational distinction between onshore and offshore collection of foreign intelligence.

Recommendation 60 p.108

That the *Telecommunications (Interception and Access) Act 1979* and the *Australian Security Intelligence Organisation Act 1979* be amended to more effectively enable the Australian Security Intelligence Organisation to share raw foreign intelligence information with the Office of National Intelligence.

Recommendation 61 p.109

That relevant policy agencies, in consultation with NIC agencies, lead a body of work to identify whether there are legislative barriers that may prevent the intelligence community from effectively responding to a conflict and consideration be given to what legislative reform may be required in advance of, and in the event of, conflict.

Oversight

Recommendation 62 p.112

That, subject to Parliament's consideration of relevant legislation, the next independent intelligence review consider the effectiveness of expanding the oversight jurisdiction of the Inspector-General of Intelligence and Security and the Parliamentary Joint Committee on Intelligence and Security to include the Australian Criminal Intelligence Commission and the intelligence functions of the Australian Federal Police, Department of Home Affairs and Australian Transaction Reports and Analysis Centre.

Recommendation 63 **p.112**

That the Commonwealth Ombudsman be empowered to oversee the propriety and proportionality of the use of covert, intrusive and coercive powers by the Australian Federal Police, Department of Home Affairs and Australian Transaction Reports and Analysis Centre.

Recommendation 64 **p.114**

That the Independent *National Security Legislation Monitor Act 2010* should be amended to ensure the Independent National Security Legislation Monitor is able to conduct own-motion inquiries into any Commonwealth legislation relating to counter-terrorism or national security. At a minimum, this should include the IS Act, the entirety of the ASIO Act, the ONI Act and provisions relating to intelligence agency powers in the TIA Act, Telecommunications Act and SD Act.

Recommendation 65 **p.115**

That in the context of broader reform to the Auditor-General Act 1997, the Australian Government consider amending the Act to enable confidential information relating to an agency overseen by the Parliamentary Joint Committee on Intelligence and Security to be disclosed to the committee.

Recommendation 66 **p.116**

That the chair and the deputy chair of the Parliamentary Joint Committee on Intelligence and Security be allocated an additional staff member each to assist in the performance of their functions. These roles should be filled by positively vetted secondees from either the policy or intelligence community.

Recommendation 67 **p.117**

That the Australian Government establish a panel of technological advisers to provide advice to intelligence oversight bodies on an as-needed basis.

Chapter 3. Terms of Reference and consultation

3.01 On 22 September 2023, the Prime Minister, the Hon Anthony Albanese MP, announced the 2024 Independent Intelligence Review (the Review). The Prime Minister's full press release is at Appendix A. The timing of this Review aligns with the regular cadence of intelligence reviews that are conducted every five to seven years in accordance with the outcomes of the Inquiry into Australian Intelligence Agencies (Flood Inquiry) in 2004.

3.02 While the Australian intelligence community operates under strong and multiple layers of oversight – by independent authorities, executive government and the Australian Parliament – the Flood Inquiry saw value in periodic external reviews to ensure Australia continues to build a world-class intelligence service.

3.03 Continuing as the Flood Inquiry began, the Review provides an external, independent assessment of the National Intelligence Community (NIC) and its effectiveness, considers the NIC as an enterprise rather than a collection of individual parts, and makes recommendations to help position Australian intelligence agencies for the future. While not all of our report can be declassified – portions of our original report to government (including some recommendations) have been redacted or amended to remove sensitive material, enable narrative coherence and clarity, and ensure currency of information – we have sought to include as many of our conclusions as possible in a public report. This is in keeping with previous reviews. We believe such transparency helps build trust and confidence in Australia's intelligence community and provides important context for the powers it exercises.

3.04 The following Terms of Reference were issued for the Review:

The 2024 independent review of Australia's National Intelligence Community (NIC) will prepare findings and recommendations on the NIC 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 2024 and will focus on the ten agencies of the NIC (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 Home Affairs and the Office of National Intelligence).

The work of the NIC underpins Australia's national security objectives, including safeguarding Australia's sovereignty in an increasingly uncertain security environment. The NIC is required to respond, in complex and changing circumstances, to protect Australia's security, prosperity and values.

The NIC has undergone significant structural changes since the last Independent Intelligence Review in 2017. Further transformative changes to the NIC are also mid-implementation following the 2019 Comprehensive Review of the Legal Framework of the National Intelligence Community (2019 Comprehensive Review).

The 2024 Independent Intelligence Review will consider:

- *The impact of the implementation of the recommendations of the 2017 Independent Intelligence Review and the 2019 Comprehensive Review, including the benefits of the establishment of the Office of National Intelligence, the expansion to create the NIC, and the effectiveness and outcomes of the Joint Capability Fund;*

- *How effectively the NIC serves, and is positioned to serve, national interests and the needs of Government, including in response to the recommendations of recent reviews relevant to defence and security, and the evolving security environment;*

- *The status, risks and potential mitigations of major investments in the NIC since 2017;*

- *Topics identified by the 2019 Comprehensive Review for consideration by future reviews, and whether further legislative changes are needed;*

- *Whether workforce decisions by the NIC at both the agency and community level reflect a sufficiently strategic response to current and future workforce challenges, anticipate future capabilities of other states so we are best positioned to counter threats, are in line with Australian Public Service commitments to diversity and inclusion and offer options if recruitment targets cannot be met;*

- *NIC preparedness in the event of regional crisis or conflict;*

- *Whether the use of the classification system by the NIC achieves the right balance between protecting sensitive information and providing decision making advantages to policy makers and operators; and*

- *Whether current oversight and evaluation mechanisms are effective and consistent across the NIC.*

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 cooperate fully with the review and provide assistance as requested. Ministers will also be asked to meet and assist the review team. The review team is to consult widely, including seeking submissions publicly.

Consultation

3.05 The Review met the Prime Minister, relevant ministers, the Leader of the Opposition, the Parliamentary Joint Committee on Intelligence and Security, intelligence agencies,

government departments, oversight bodies, industry representatives, academics, think tanks, and other individuals and entities that interact with or consider the intelligence community. The Review also met intelligence agencies and other relevant stakeholders from Australia's Five Eyes partners and Japan. Submissions were sought and received from government and the public.

3.06 Lists of those consulted and submissions received are at Appendix C.

Part I: Foundations

Chapter 4. The global context

4.01 The global context in which Australia seeks prosperity and security directly shapes the roles and functions of the National Intelligence Community (NIC). The world – as it is now and as it is forecast to be – presents a kaleidoscope of threats and opportunities for intelligence agencies, shaping priorities, driving the allocation of resources, and informing investment in skills and technical capabilities.

4.02 Today, Australia's intelligence community confronts more threats, more complexity and more demand from governments than at any time in recent decades. Of the major trends shaping global affairs, we single out three as most consequential for the intelligence community:

- There have been shifts in relative global power balances, accompanied by a sharp contest between nation-states for power and influence. This contest is at once diplomatic, military, economic and technological, and is pursued within Australia's borders as much as beyond them, including through cyber attacks and foreign interference.
- New technologies are being used to amplify some old threats while creating entirely new ones.
- There are a range of transnational challenges, including climate change, pandemics, irregular migration, terrorism, and polarisation and fraying social cohesion in many democracies. In a globalised world, the ripples from even geographically distant conflicts inevitably reach Australia, with significant, often grave, consequences.

Contest and fragmentation

4.03 The post-Cold War order has collapsed. It is not yet clear what will take its place, but for the foreseeable future Australia faces a world shaped by competition between nation-states and global geopolitical and economic fragmentation.

4.04 This fundamental transformation of Australia's external environment, including China's emergence as a more powerful, assertive and authoritarian actor, is extensively analysed and recorded elsewhere, including in Australian government statements such as the *2024 National Defence Strategy*.

4.05 Here we touch on seven factors we regard as having particular implications for the intelligence community.

4.06 First, competition between nation-states, especially between China and the United States, is deeply rooted and structural in nature. It is a feature of the era, not a passing moment.

4.07 Second, this contest is marked by a clash of interests and values that has proved impossible to reconcile and hard even to manage peacefully. Competition is global, extending to the developing world, but is sharpest in the Indo-Pacific. As the *2024 National Defence Strategy* observes, this tense dynamic is amplified by China's military modernisation – the largest and most ambitious of any country since World War II.

4.08 While still not likely, a major regional conflict is no longer unthinkable. And, short of conflict, coercion, disinformation and propaganda are now used routinely in the Indo-Pacific to support geopolitical objectives.

4.09 Third, the contest with China, and now Russia, is not confined to hard power – it extends to the norms and rules that regulate the behaviour of nation-states.

4.10 China and Russia are working to weaken the global influence of the United States and the West more broadly, including by promoting concepts that legitimise authoritarian regimes, support non-interference in internal affairs, and privilege state-centric approaches to human rights. Understanding the ideational elements of competition is therefore essential to any broader analysis of geopolitics.

4.11 Fourth, systemic competition is creating new alignments. Closer cooperation between China and Russia in the wake of Russia's invasion of Ukraine is a notable shift. Russia, Iran and North Korea are deepening ties. A loose bloc of autocracies is now forcibly pursuing their national interests in ways that undercut global security and stability.

4.12 Fifth, competition between nation-states extends to trade, finance and technology. Countries are vying to secure advantage in the technologies that are essential to modern warfare and that will power economic growth and the transition to a clean-energy future. The United States and the European Union want to 'de-risk' economic dependencies on China. Nor does China, in turn, want to be dependent on the West for critical technologies and resources. Intervention in markets to build nation-state competitiveness and resilience is now the norm. For Australia, an open, globalised economy with a small industrial base, economic nationalism and the rapid rise of 'economic security' as an essential component of national security creates complex policy choices.

4.13 Sixth, the global contest for power and influence does not respect national borders. For Australia, the domestic flow-on effects are large and consequential. These include high levels of cyber intrusions, espionage, foreign interference and threats to diaspora communities. According to the Australian Security Intelligence Organisation's *2024 Annual Threat Assessment*, more Australians are being targeted for espionage and foreign interference than ever before.

4.14 Australian data, technology and scientific research are regular targets for espionage. Foreign investment, especially in critical infrastructure, requires careful scrutiny. Protecting military and critical technology and intellectual property is an essential national security priority. This will be especially important as Australia embarks on its nuclear-powered submarine program.

4.15 Finally, the mix of national-level policy responses to systemic global competition – alignment, multi-alignment, accommodation and balancing – is an important variable in itself, one that intelligence agencies must track and understand. This is true even of the West. The election of more nationalist or populist governments in Europe and the United States, for example, could introduce considerable uncertainty in global affairs and alter some of Australia's current foreign and economic policy planning assumptions.

Technology

4.16 Technological advances are amplifying some old national security threats and creating entirely new ones. The net effect for intelligence agencies is a dramatic shift in the complexity, scale and tempo of some security challenges.

4.17 Australia's *2024 National Defence Strategy* recognises that technology has already overturned one of Australia's longstanding advantages – geography. Distance cannot protect Australia from long-range missiles, space and cyber attacks, disinformation and supply chain disruptions.

4.18 Current technologies, like end-to-end encryption, help state actors and criminal groups hide their activities from intelligence and law enforcement agencies.

4.19 The Australian Signals Directorate's *Annual Cyber Threat Report 2022-2023* warns that cyber actors are targeting Australian governments, critical infrastructure, businesses and households. Malicious actors look for weaknesses in Australia's cyber defences and use sophisticated techniques to avoid detection. The motivations for cyber attacks vary and include criminal intent, espionage or even sabotage. Regardless, the potential for harm – particularly involving critical infrastructure – is high.

4.20 Advances in information technology enable propaganda and disinformation. China, for example, spends billions of dollars annually on foreign information manipulation efforts.[1] Russia's use of social media platforms to influence the 2016 and 2020 United States elections and undermine trust in the electoral process is well documented. No democracy is immune to such breaches of sovereignty.

4.21 Ubiquitous technical surveillance and the near impossibility of operating in the modern world without leaving a digital footprint make it more difficult – and more expensive – for intelligence agencies to operate securely and safely.

4.22 Technology challenges the functions of intelligence agencies in other ways. The sheer volume of publicly and commercially available data and information, still expanding at exponential rates, threatens to overwhelm intelligence collectors and assessors.

4.23 Looking ahead, emerging technologies – especially artificial intelligence (AI), quantum computing, sensing and communications technologies, and synthetic biology – have the potential to boost productivity, support economic growth, drive environmental and medical breakthroughs and improve social welfare. But emerging technologies also create security challenges.

4.24 A recent United Kingdom Government assessment of the risks of generative AI to 2025, for example, included: enhanced cybercrime and hacking; risks to political systems and social cohesion, including through manipulation and deception of populations; and growing threats to critical infrastructure.[2]

[1] US Department of State Global Engagement Center, *How the People's Republic of China seeks to reshape the global information environment,* 28 September 2023, p 3.
[2] Department for Science, Innovation & Technology (UK), *Safety and Security Risks of Generative Artificial Intelligence to 2025*, 25 October 2023,

4.25 If successfully realised, advances in quantum computing could enable adversaries to exploit sensitive information not secured by post-quantum encryption. Synthetic biology could be used to develop new weapons of mass destruction.

Climate change

4.26 Government has at its disposal deep scientific expertise on climate change in specialised agencies, research institutions and the private sector. Even so, climate change is a priority for intelligence agencies and is likely to require more collection and assessment focus. One reason is that collaboration on global warming is now tangled in China–United States rivalry. And the technologies central to the clean energy transition – like solar panels, batteries and wind turbines – have become vectors of competition in themselves, as countries worry about security of supply and seek sovereign industrial advantage.

4.27 The potential security challenges of accelerating climate change are also significant. These include poverty, food insecurity, ocean health, water scarcity, disrupted infrastructure and supply chains, and cross-border migration.

Other transnational issues

4.28 In the period ahead, intelligence agencies will confront a complex landscape of other transnational challenges.

4.29 Terrorism remains a persistent threat, despite the rapid rise of systemic state competition, cyber threats, espionage, and foreign interference as Australia's principal security concerns.

4.30 One challenge for the Australian intelligence community is that, in the words of Director-General of Security Mike Burgess, Australia's terrorist threats have reduced in scale while increasing in complexity. Current threats include:

- There is an ongoing risk from Sunni violent extremism. Terrorist groups like ISIL and al-Qa´ida have sought to use conflict in the Middle East to encourage attacks and stoke community tensions.
- The risk of radicalisation of Australian citizens and 'lone actor' attacks remains.
- Racist violence is now a persistent threat.

4.31 Extremism is just one factor fraying social cohesion in many countries around the world, including Australia. The sources of internal fragmentation are varied but often amplify each other. They include the conflicts in Gaza and Lebanon, political polarisation, inequality, declining faith in democracy, large-scale misinformation and disinformation powered by the internet, and deliberate attempts by some countries (notably Russia and China) to stoke internal divides in democracies.

4.32 Promoting social cohesion and keeping communities safe are high priorities for Australian governments. Intelligence agencies support this work to ensure Australia's diversity remains a source of strength.

4.33 Conflict, repression, poverty and the search for opportunity will keep driving irregular migration by land, air and sea. This is a global phenomenon, often facilitated by people-smuggling syndicates. Recent boat arrivals show that irregular migration will continue to test Australia's border settings.

4.34 Governments will also want warning and insight into other transnational challenges. The World Health Organization has warned of the risk of another pandemic in coming years. Global warming and deforestation increase the risk of novel pathogens emerging, with potentially serious consequences for life, economic growth and social stability. Transnational, serious and organised crime has devastating social consequences, including through drug production and importation, modern slavery and industrial-scale scamming operations.

4.35 The state-based pursuit of weapons of mass destruction is growing as arms control frameworks come under greater strain and strategic competition intensifies. The *2024 National Defence Strategy* notes that Russia, China and North Korea are building more diverse and sophisticated nuclear arsenals, while Iran continues to breach its nuclear-related obligations. Russia's invasion of Ukraine raised the possibility of nuclear weapons being used in a conflict for the first time since the close of World War II.

Implications for the NIC

4.36 The 2017 Review accurately forecast that change in the international system and the consequences of technological advances would shape the intelligence community's operational environment. What was not possible to see at the time was the transformative pace and scale of the change that followed.

4.37 The brief survey above is a stark reminder of the sheer number of consequential shifts that have played out in a short few years – China's drive for regional pre-eminence, intense China–United States competition, the rapid rise of economic security as a policy priority, advances in information and other technologies, high levels of cyber attacks and foreign interference, threats to social cohesion, record levels of global warming, and a coronavirus pandemic.

4.38 The implications for Australia's intelligence agencies are broad and significant.

4.39 First, there will be no respite from current levels of high demand. There is a greater risk of strategic surprise. The expanding agenda of complex issues on which governments want insight, including economic resilience, technological change and global health security, requires new expertise and ways of working. Intelligence will be an essential input to policies that bolster Australia's influence, manage deterrence and build national resilience.

4.40 High demand is stretching resources, capabilities and people, the result of a more or less continuously high tempo of operations since the 11 September 2001 terrorist attacks. The threat environment makes priority setting more important but more difficult. Resource trade offs can increase risk.

4.41 Second, government increasingly will use intelligence agencies not just for information and insight, but to achieve outcomes. Offensive cyber operations, and other activities designed

to disrupt or influence events that would otherwise pose a threat to Australia and its people, are examples of tools now available to governments to support global interests.

4.42 Third, perhaps more than any other part of government, the way Australian intelligence agencies work is being shaped by the data and technology revolution. New technologies create multiple challenges for intelligence agencies, from information overload, to disinformation, to ubiquitous technical surveillance. Open source information and analysis, produced more quickly and in ways that can be read on mobile devices, will present a growing challenge to traditional models of intelligence production and distribution.

4.43 But new technologies, especially AI, are also increasingly used by intelligence agencies to solve some of the problems of the new era. Sustaining a competitive edge in collection, operations and analysis will therefore require well-targeted investment in expertise and technical capacity.

4.44 Fourth, in the current era, preparedness for crisis or conflict assumes even greater importance. This applies at the enterprise level but equally to the resilience of the intelligence community's people, who face daily a raw and confronting set of security challenges.

4.45 Fifth, more than ever, strong intelligence community collaboration will be essential to maximising the value of intelligence as a tool of statecraft. This means intelligence agencies working together so that the sum is greater than the parts. Policy departments and executive government will also need to set clear priorities and requirements and be better able to use highly classified intelligence to inform decision making.

4.46 Sixth, as is already the case, the global context in which Australia's intelligence agencies are operating puts a premium on partnerships and burden sharing. The alliance with the United States and the Five Eyes partnership are national assets for Australia, providing access to information, expertise and technology that would not otherwise be obtainable. The AUKUS partnership is also shaping the way in which Australia works with the United States and United Kingdom intelligence communities. Regional intelligence relations will continue to grow in importance, including directly with Pacific and Asian countries. These partnerships cannot be one-way – expectations on Australian intelligence agencies to do their share will be high.

4.47 The operating environment for intelligence agencies also requires strong partnerships with Australian businesses and the research sector, to help the private sector build its own resilience to cyber and espionage threats, and to ensure the intelligence community has access to the expertise and technologies it needs.

4.48 Finally, what intelligence agencies do, and what they know, is necessarily more public today than it often has been in the past. Intelligence is more likely to be found in the news than in the past. United States and United Kingdom government actions prior to Russia's 2022 invasion of Ukraine demonstrate how the public release of intelligence can provide warning, counter false narratives and shape allied support for collective responses. This is a tool Australia may reach for in the future.

4.49 In an era dominated by national security challenges, the prominence of Australia's intelligence community in supporting government policy is understandable but has not been

without controversy. Building public understanding of, and support for, a strong Australian intelligence enterprise is essential.

Box 1. The National Intelligence Community

Office of National Intelligence

ONI has a range of functions, including providing intelligence support to senior government decision makers, producing open source intelligence and leading the NIC. In performing the latter function, ONI is responsible for leading the 10 agencies of the intelligence community to ensure their respective capabilities and expertise are fully harnessed to meet the needs of government. This is referred to throughout the Review as 'enterprise management' and is discussed in more detail in *Chapter 6*. ONI also provides intelligence assessments to the Prime Minister and other ministers on matters of strategic significance to Australia. ONI is part of the Prime Minister's portfolio and is a statutory agency.

Australian Criminal Intelligence Commission

The ACIC is Australia's national criminal intelligence agency with a focus on the transnational serious and organised crime threat environment and its impact on Australia. The ACIC's purpose is to protect Australia from serious criminal threats by collecting, assessing and disseminating intelligence and policing information. Through its advice the agency supports whole of government decision-making and posture across operational practice, policy, regulatory and legislative environments. The ACIC is part of the Attorney-General's portfolio and is a statutory agency.

Australian Federal Police

While the AFP is primarily a federal law enforcement agency, it also performs an intelligence function to support its policing mandate. The AFP's intelligence efforts support the prevention, disruption and detection of criminal activity relating to a range of Commonwealth crimes. It was formed in 1979 under the *Australian Federal Police Act 1979*. The AFP is part of the Attorney-General's portfolio and is a statutory agency.

Australian Geospatial-Intelligence Organisation

The Defence Imagery and Geospatial Organisation was formed in 2000. It was renamed the Australian Geospatial-Intelligence Organisation (AGO) on 3 May 2013. AGO produces geospatial and imagery intelligence (GEOINT) in support of defence and other national intelligence priorities. It also plays a leadership role across the broader Australian geospatial community. The *Intelligence Services Act 2001* (IS Act) defines AGO's functions and limits. AGO is part of the Defence Intelligence Group within the Department of Defence.

Australian Secret Intelligence Service

ASIS produces intelligence about overseas actors to support national intelligence priorities. ASIS was formed in 1954, but its existence was not publicly acknowledged until 1977. The IS Act provides ASIS with a legislative footing and defines its functions and limits. ASIS is part of the Foreign Affairs portfolio and is a statutory agency.

Australian Security Intelligence Organisation

ASIO collects, assesses and investigates intelligence on security threats targeting Australian interests. Originally established in 1949 by a directive from Prime Minister Ben Chifley, ASIO became a statutory authority in 1956. The scope of what is meant by threats to 'security' is defined in the *Australian Security Intelligence Organisation Act 1979*. This Act also articulates the limits of ASIO's lawful powers. ASIO is part of the Attorney-General's portfolio and is a statutory agency.

Australian Signals Directorate

ASD is responsible for foreign signals intelligence and cyber security. Australia's first signals intelligence organisation – the Defence Signals Bureau – was formed in 1947. The IS Act provides ASD with a legislative footing and defines the organisation's functions and limits, which have evolved over the years. ASD is part of the Defence portfolio and is a statutory agency.

Australian Transaction Reports and Analysis Centre

AUSTRAC is an anti-money laundering and counterterrorism financing regulator and a financial intelligence unit. Its financial intelligence function produces insights that inform law enforcement and national security investigations. AUSTRAC's predecessor – the Cash Transaction Reports Agency – was established in 1988. The functions of AUSTRAC are outlined in the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. AUSTRAC is a statutory agency and is part of the Attorney-General's portfolio.

Defence Intelligence Organisation

DIO was established in 1990 and produces intelligence assessments to support the Minister for Defence, the Department of Defence and other government agencies. DIO is part of the Defence Intelligence Group within the Department of Defence.

Department of Home Affairs

Home Affairs coordinates, and provides strategy and policy leadership on, issues including cyber and critical infrastructure, immigration, border security, counterterrorism, protection of sovereignty, citizenship and social cohesion. Home Affairs also has an intelligence function that supports the department's operational and policy work and informs efforts of other intelligence agencies.

Chapter 5. Intelligence principles and foundations

5.01 Intelligence cannot answer every question or solve every problem. Nor does intelligence predict the future. Forecasting the future with accuracy is extremely difficult. Strategic surprise is an ever-present risk.

5.02 Like any tool of statecraft with which governments seek to influence outcomes and shape the world around them, intelligence is therefore imperfect. But a strong intelligence enterprise can and often does provide decisive advantage.

5.03 The business of intelligence has some enduring qualities, including what constitutes useful or 'good' intelligence for governments. But, like any other part of government, intelligence agencies also evolve and adapt, take on new functions, and are shaped by forces of change, as we discussed in *Chapter 4*.

What is intelligence?

5.04 One way to define intelligence is that it is the output of a process whereby information is collected and transformed – including through the use of all-source collection and analysis – to support, inform, and otherwise provide advantage to decision makers. In line with Justice Hope and others, this definition highlights that intelligence is both a process and a product, while emphasising that its primary purpose is to provide advantage to a customer.[3]

5.05 Secrecy remains an important, but not defining, feature of intelligence. Information does not have to be secret to be valuable. In many cases, intelligence advantage arises from the synthesis of information across a range of sources – covert and overt – and the overlay of subject-matter expertise and analysis.

5.06 The Hope royal commissions established 'quality, timeliness and relevance' as key principles of 'good intelligence'. Justice Hope said intelligence needed to be robust and accurate, linked to a need, and provided in adequate time to support the decision maker. Other sources on the practice of intelligence add qualities such as purposeful, actionable, value-adding and unbiased.[4]

5.07 Intelligence is most often thought of as valuable information. But Australia's intelligence agencies also support government objectives in more direct ways, including through operational activity and intelligence diplomacy, as we discuss below.

Intelligence as a tool of statecraft

5.08 Intelligence agencies serve government and the nation in diverse ways.

---

[3] See Justice Robert Hope, *Royal Commission on Intelligence and Security*, 1976; Justice Robert Hope, *Royal Commission on Australia's Security and Intelligence Agencies*, 1984; Philip Flood AO, *Report of the Inquiry into Australian Intelligence Agencies*, 2004; Robert Cornall AO and Rufus Black, *Independent Review of the Intelligence Community report*, 2011; Michael L'Estrange AO and Stephen Merchant PSM, *2017 Independent Intelligence Review* (2017 Review); Alfred Rolington (ed.), *Strategic intelligence for the 21st century: the mosaic method,* 2013, pp 17–19; David Ormand, 'Reflections on intelligence analysts and policy makers', *International Journal of Intelligence and Counter Intelligence,* 2020, pp 1–12.

[4] Miah Hammond-Errey, 'Big data, emerging technologies and the characteristics of "good intelligence"', *Intelligence and National Security*, 2003, p 1–20.

5.09 Australia's intelligence community provides warnings of threats that are both imminent and on the horizon. Intelligence illuminates geopolitical shifts and other global trends, providing insight and informing policy development. Intelligence helps guard Australia's sovereignty and democracy. It protects citizens against terrorism and extremism. Intelligence supports law enforcement, including against transnational, serious and organised crime.

5.10 Intelligence is essential for effective military operations. And it gives governments tools with which to effect outcomes and even strike back at adversaries, like malicious cyber actors. Intelligence leaders can 'convey messages that advance wider Australian government international and diplomatic priorities',[5] complementing other forms of diplomacy. Intelligence operations can also be used to disrupt or shape events in ways that support Australia's national interest.

5.11 The National Intelligence Community (NIC) is therefore an essential component of Australian national power (see *Box 1*). Given the pace and scale of major global change in recent years, much of which challenges Australia's security and prosperity, a world-class intelligence enterprise is more important than ever.

Roles and responsibilities

5.12 The operation and governance of the intelligence community remain strongly influenced by principles set out by Justice Hope's two major royal commissions on intelligence and security in the 1970s and 1980s.

5.13 Time and change have qualified some of the Hope principles, but their essential relevance was endorsed by the 2019 Comprehensive Review into intelligence legislation (2019 Comprehensive Review) and the 2017 Independent Intelligence Review.

5.14 The NIC cannot be understood without reference to these foundational principles. For this reason, and because they remain important to the fabric of Australian government and democracy, and to public trust, our report restates them.

5.15 Hope's core principles include:

- the roles, responsibilities, and limits of each agency are defined in legislation
- each agency's mission is aligned with the national interest, with vital checks and balances to protect the rights of the individual
- the activities of agencies are coordinated to maximise impact and ensure alignment with defined intelligence priorities
- while each agency reports to their respective minister, some intelligence functions must be independent
- bespoke oversight architecture ensures agencies meet high standards for probity and accountability.

[5] The National Intelligence Community, *Intelligence*. Available at https://www.intelligence.gov.au/intelligence.how-we-protect-australia.

5.16 Justice Hope also saw a need to distinguish between intelligence functions. Hope's principal distinctions were between:

- foreign and security intelligence
- intelligence collection and assessment
- intelligence assessments and policy determination
- security intelligence and law enforcement.

5.17 In Australia, these distinctions have led to the separation of some intelligence functions in a way that is not always done in other nations.

5.18 In the United States, for example, the Central Intelligence Agency is both a collector and an assessor of foreign intelligence. In New Zealand, foreign intelligence and security intelligence are undertaken by a single agency rather than separated, as is the case in Australia.

Foreign and security intelligence

5.19 The distinction between foreign and security intelligence primarily applies to the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD) and the Australian Geospatial-Intelligence Organisation. It is a principle that protects the civil liberties and privacy of Australians. It also helps define the roles of agencies, their unique value-add and the necessary accountability arrangements.

5.20 Security intelligence protects Australia from a range of threats. These include but are not limited to foreign interference, espionage, politically motivated violence and sabotage.

5.21 While foreign intelligence similarly seeks to protect Australia from threats, it also supports Australia's foreign policy objectives and broader national interest. Specifically, foreign intelligence provides insight on the capabilities, intentions or activities of entities or individuals outside of Australia.

5.22 This distinction is not always clear-cut. Geography is not a distinguishing feature and its relevance is further undercut by technology. Nor is it neatly separated by the specific functions of agencies. Some intelligence activities can be considered both security and foreign intelligence.

5.23 As previous reviews have observed, we do not think this overlap is necessarily problematic. On balance, the distinction between security and foreign intelligence continues to serve a key role in protecting the civil liberties and privacy of Australians by ensuring agencies are being held to account by the right legal and oversight mechanisms. This foundational principle should therefore remain intact. However, given the overlap between foreign and security intelligence, there is a need for flexibility in how this principle is reflected in practice.

5.24 Two associated distinctions underpin the community's legislative framework, and were considered by the 2019 Comprehensive Review.

5.25 The first is the distinction between onshore and offshore activities. This primarily arises for foreign intelligence agencies, which have broad powers and immunities to operate offshore, but far more limited ability to use what would normally be unlawful means to gather intelligence in Australia. This distinction is a reflection of the scope of Australia's sovereignty and of the rule of law, and ensures intelligence agencies operating in Australia are bound by, and operating within, Australian laws.

5.26 The second is the distinction between Australians and non-Australians. This distinction arises in several ways, also mainly in relation to foreign intelligence. For example, foreign intelligence warrants must not be sought to collect information on an Australian (unless that Australian is acting on behalf of a foreign power) and foreign intelligence agencies must obtain a ministerial authorisation to collect intelligence on Australians. This distinction provides Australians with greater safeguards and administrative protections, reflecting the increased risk associated with a government collecting intelligence on its own citizens.

Intelligence collection, assessment and policy

Intelligence collection and assessment

5.27 Intelligence assessments are formed through analysis of all sources of collected intelligence (including security and foreign). Objectivity is an essential characteristic of an intelligence assessment – both in terms of its substance and how it is perceived by those who consume it. To ensure objectivity, Justice Hope held that the processes of intelligence collection and assessment needed to be distinct and independent. This buffer would eliminate external biases that may unconsciously occur in agencies focused on specialised collection work.

Intelligence assessment and policy development

5.28 A strong feature of Australia's intelligence system is the separation between intelligence assessors and intelligence consumers. Intelligence assessment is separated from policy development to ensure that neither policy nor political preferences cloud the accuracy and impartiality of judgements. The creation of the Office of National Intelligence's (ONI's) predecessor, the Office of National Assessments, was driven by this principle.

5.29 Successive reviews of the intelligence community have underlined the enduring importance of separating intelligence assessment from policy making, as do we. The integrity and value of intelligence assessments rests fundamentally on their independence. The risk of poor decisions becomes higher if governments receive intelligence assessments that always validate their preferred course of action.

5.30 There is an equal set of obligations on intelligence assessors not to slip themselves into policy advocacy. There is an important role for intelligence assessment in helping governments understand the implications of particular policy choices, and where there is opportunity for Australia to influence outcomes. As the 2017 Review observed, intelligence products and processes cannot operate in 'splendid isolation' from policy priorities. This can make the line between assessment and policy a fine one at times, but it nonetheless exists and must be observed. Governments will discount the advice of intelligence agencies if they come to believe assessments seek overtly to determine rather than inform policy making.

Security intelligence and law enforcement

5.31 The line delineating security intelligence from law enforcement activities has remained steadfast since ASIO commenced operations in 1949. Successive reviews have reaffirmed this distinction. We also judge this separation should continue.

5.32 Justice Hope's observations in this regard remain astute. He acknowledged that while some nations have police forces that perform a function similar to security intelligence, it was important in the Australian context that these functions were separated so that they could be overseen by the necessary mechanisms.

5.33 The Australian Federal Police (AFP) and other state and territory police forces have criminal intelligence functions. AFP's intelligence activities support its law enforcement and policing functions. These are overseen by the courts, the Commonwealth Ombudsman,[6] the Inspector-General of Intelligence and Security and the Parliamentary Joint Committee on Intelligence and Security.

Statutory independence

5.34 The integrity and effectiveness of the intelligence community rests on its ability to exercise independence in the advice it gives and a large measure of independence in the operations it conducts.

5.35 Independence ensures the considerable powers of intelligence agencies cannot be influenced by political considerations, or even misused by governments. It allows the intelligence community to give governments the advice they need, even if this is not always advice governments welcome.

5.36 Public trust is similarly reliant on this independence: any perception that intelligence agencies are politically influenced is highly corrosive to liberal democratic norms.

5.37 Most agencies in the intelligence community are established as statutory agencies. The establishing legislation provides each agency with varying degrees of independence. This independence is assured in a variety of ways:

- each agency head has control of the administration and management of the agency
- there are limitations on termination of agency heads
- there are requirements for agency heads to keep agencies free from improper influence.

5.38 Each agency is required to comply with directions and, in some cases, guidelines from the responsible minister.[7] Though the ministers' powers to direct agencies are broad, there are limitations. For example, the legislation prevents ministers from directing ASIO and ONI in relation to the content of their advice.[8] There are also limits on relevant ministers' ability to direct ASIO, the Australian Criminal Intelligence Commission, the AFP and Australian

[6] If parliament passes the Intelligence Services Legislation Amendment Bill 2023, the IGIS will have an expanded oversight role in relation to the AFP, meaning the Commonwealth Ombudsman will not oversee the AFP's intelligence functions.
[7] See *Office of National Intelligence Act 2018* (ONI Act), s 12(1); *Australian Security Intelligence Organisation Act 1979* (ASIO Act), ss 8(2), 8A; *Australian Federal Police Act 1979*, s 37(2); *Anti-Money Laundering and Counter Terrorism Financing Act 2006*, s 228(7); *Intelligence Services Act 2001* (IS Act), s 8; *Australian Crime Commission Act 2016*, s 18(1).
[8] ASIO Act, s 8(4); ONI Act, s 12(2).

Transaction Reports and Analysis Centre on certain operational matters. There are no legislative limitations on the ministerial directions powers relating to ASIS and ASD.

5.39 It is essential that governments protect and respect agency independence. Nonetheless, we note the independence of the intelligence community is not, and in a democracy should not be, absolute.

5.40 The extent of independence enshrined in legislation is carefully framed and intentionally confined. Intelligence agencies, whether statutory authorities or not, are part of executive government. The requirement, though not unfettered, to comply with ministerial directions ensures that those agencies are accountable for their performance to ministers and ultimately to the parliament. This check on agency independence is a reflection of the typical operation of responsible government. Nor are the usual conventions around consultation and coordination with government inconsistent with independence.

5.41 It is important that the principle of independence does not lead to a sense of psychological or physical separation from executive government. The leadership of NIC agency heads will always be important in this regard. The nature of independence as set out in legislation and the conventions of responsible government should also be part of foundational training for NIC officers. We note in this regard that the 2019 Comprehensive Review recommended that intelligence agencies' training should address the principles underpinning their legal frameworks.

Accountability, trust and the role of oversight

5.42 Intelligence agencies will only be effective in protecting national security if the public has confidence that they are held accountable for their respect for legal and ethical behaviour.

5.43 Many of the typical measures to ensure accountability of government bodies are less effective in relation to the intelligence community. There are limits on parliamentary, judicial and media scrutiny of agencies as a result of the secrecy of many of their activities. As such, Australia has developed bespoke oversight architecture to hold agencies to account.

5.44 Australia's oversight architecture is comprised of specialised, independent bodies that collectively oversee the full remit of agency activities. These bodies are outlined in further detail in *Chapter 18*. Fundamentally, these bodies are designed to ensure agencies and their officers act lawfully and appropriately, and that the legal framework within which they operate is itself appropriate.

5.45 Effective oversight is crucial to public trust in the intelligence community. The activities of intelligence agencies are, necessarily, largely opaque to the public. The broad remit of the various oversight bodies, their strong compulsory powers and their independence from government provide public assurance that agencies will be held accountable for their actions. In this way, Australia's strong oversight system is an essential mechanism to build public trust and enhance agencies' legitimacy.

Part II: Reflections on past reform

Chapter 6. The National Intelligence Community since 2017

6.01 This chapter considers the implementation of the 2017 Independent Intelligence Review (2017 Review) and the 2019 Comprehensive Review of intelligence legislation (2019 Comprehensive Review), as required by our Terms of Reference.

6.02 An evaluation of every element of these major reviews would amount to a long report in itself. This chapter therefore considers the implementation of the most consequential recommendations. We propose new approaches where the intent of a recommendation might not have been met.

The 2017 Independent Intelligence Review – managing the NIC as an enterprise

6.03 The principal theme of the 2017 Review was the need for strong, enterprise-level management of the National Intelligence Community (NIC) to complement the strengths of individual agencies.

6.04 The 2017 Review argued that a stronger central coordinating function was needed to lead the development and implementation of national intelligence priorities, undertake systematic and rigorous evaluation of the performance of the agencies, implement strategic workforce planning and facilitate joint capability planning. The Review's most consequential recommendation was the establishment of the Office of National Intelligence (ONI). We therefore devote much of this chapter, and some of our later recommendations, to ONI's role in the NIC and the path to more effective enterprise management.

6.05 To support ONI's coordination role, the 2017 Review recommended a Joint Capability Fund (JCF) to drive technological innovation and shared capabilities. A new, forward-looking Intelligence Capability Investment Plan (ICIP) was proposed to inform government decision making on future capability requirements and give agencies greater certainty about their budget outlooks.

6.06 The establishment of ONI was an important and successful reform. ONI has a clearer and stronger leadership and convening role in the intelligence community. Integration, coordination and governance across the NIC have improved since 2017, allowing for greater visibility of shared challenges and enabling collective action to address these. ONI is a more capable principal intelligence adviser to the Prime Minister and government. And its expanded role bolsters its standing with counterpart agencies in the Five Eyes intelligence community.

6.07 Nonetheless, like any major reform, the establishment of ONI has not been without its challenges. Some of the ambitions of the 2017 Review for the effective integration and coordination of the NIC have not been fully realised.

Role of the Office of National Intelligence

6.08 ONI was created through legislation that gives the Office and its Director-General a clearer leadership role in the NIC and more responsibility for enterprise management. The *Office of National Intelligence Act 2018* (the ONI Act) does not, however, give the Director-General additional legislative powers, including over budgets. Overall, the intent of the ONI Act is that the Director-General 'guide the direction' of the NIC.

6.09 ONI's ability to lead the community and drive integration remains dependent on its powers of persuasion and ability to add value to the task of enterprise management. This works best when relationships across the NIC, especially between agency heads, are close and collegiate. But the NIC is now large enough, and the roles of agencies discrete enough, that individual agency interests can trump efforts to drive coordination and integration across the community even with good relations at the leadership level.

6.10 In summary, there remains at times an imbalance between what ONI is expected to do by government on enterprise management and its ability to bring the broader intelligence community along with it. Progress has been made but is not institutionalised. Cooperation across the NIC is too often relationship-dependent.

6.11 The Review considered alternatives to the current model but does not recommend further empowerment of ONI through legislative change, for example by giving ONI more control over budgetary planning (as the Director of National Intelligence in the United States has) or the ability to direct cooperation in particular circumstances.

6.12 We have not found any support for legislative changes to the management of the NIC during our consultations. Australia's system of portfolio government, with agencies accountable to their respective ministers and governed by separate legislation, is strong by practice and convention. The ONI Act was drafted in this context, making clear that in exercising its leadership role, ONI cannot encroach on the functions, roles or responsibilities of other agencies.

6.13 We also agree with the conclusion of the 2019 Comprehensive Review that 'effective coordination is not something that can be achieved simply by legislative fiat'.

6.14 Nonetheless, we recommend government should consider practical, non-legislative ways of bolstering ONI's role and authority in the NIC.

6.15 Government should continue to ensure National Security Committee of Cabinet decisions are appropriately informed by intelligence assessments, including those delivered orally at committee meetings by the Director-General of National Intelligence (DGNI). The 2017 Review recommended the head of ONI conduct regular direct briefings of the prime minister of the day. This is hard to achieve consistently given the demands on prime ministerial time, but is encouraged by the Review.

6.16 We recommend the prime minister of the day clearly set out their expectations of ONI and NIC agency heads at the beginning of each term of government. This could occur, for example, through a letter from the prime minister to agency heads that sets out expectations in relation to support for ONI's enterprise management role and leadership-driven collaboration across the community.

Recommendation 1: That the Prime Minister writes to the intelligence community with a statement of expectations at the beginning of each term of government.

6.17 We also recommend that the DGNI be appointed to relevant subcommittees of the Secretaries Board, noting the seniority of the Director-General position and ONI's leadership and coordination functions (which give it a role in the intelligence community not dissimilar to that of central agencies). This will give the NIC more connections to, and the ability to draw from, best practice in Australian Public Service (APS) administration.

Recommendation 2: That the Director-General of National Intelligence be made a member of relevant sub-committees of the Secretaries Board.

6.18 We encourage more use of the 'directions' power embedded in the ONI Act. This allows the Prime Minister to issue 'directions' to the DGNI on the exercise of ONI's powers (except in relation to the substance of assessments). In turn, DGNI may issue directions or 'guidelines' to specific agencies or the community where the Director-General considers this necessary. In both cases, directions and guidelines are not legislative instruments. There are issues identified in this Review that lend themselves to reasonable use of the directions power, including in relation to preparedness for a crisis.

Enterprise management

6.19 Enterprise management requires commitment and resources from all intelligence community members. At times, it also asks them to surrender a degree of autonomy. A challenge for ONI has been to ensure sufficient benefit from enterprise management to justify the impost on other agencies. In response, ONI has streamlined some enterprise management functions and sought to address issues on which its leadership role can add most value.

6.20 The need for effective enterprise management of the intelligence community remains high. Our strategic circumstances are deteriorating. Security challenges are multiplying. The expectation from government is that Australia's intelligence agencies work as a community, so that the sum is greater than the parts.

6.21 A well-targeted approach to enterprise management should include stronger integration and collaboration on issues that are fundamental to the NIC's ability to respond to current challenges. In our view, this is necessary in relation to:

- current challenges such as workforce, technology and capability investment
- emerging issues, notably preparedness and intelligence diplomacy and effects.

6.22 We take up these issues in other sections of this Review, and in separate advice to government. We also acknowledge that the additional leadership and enterprise management responsibilities we propose would require a commensurate increase in staff for ONI. This will require new funding.

Recommendation 3: That the Office of National Intelligence receive an uplift in resourcing to support additional leadership and enterprise management responsibilities.

Coordination of capability investment

6.23 Not all elements of the 2017 Review have been implemented as the reviewers originally intended. The proposed ICIP proved not possible to deliver within Australia's portfolio system of government. The JCF has a mixed record of performance. And ministers still have limited opportunities to consider intelligence community investment requirements on a collective basis and to make choices about priorities. Large capability investments in the NIC since 2017 have been driven by individual agencies through portfolio ministers.

6.24 We make recommendations later in this Review to address shortfalls in the way in which the NIC forecasts and coordinates capability investment requirements (see *Chapter 11*).

Evaluation

6.25 The 2017 Review recommended ONI conduct rigorous evaluations of the performance of each NIC agency. Over time, ONI shifted from agency evaluation to evaluation of intelligence missions (that is, performance against particular intelligence targets). ONI uses mission evaluation to deliver insights on NIC performance, including in relation to intelligence and capability gaps.

6.26 We accept it is difficult for ONI to conduct truly rigorous agency-level evaluations while also retaining the confidence of the intelligence community. While therefore supporting ONI's shift to mission evaluation, we note it is not always easy for ministers to draw out high-level observations about the performance of the intelligence community as an enterprise. One way to fill this gap would be for the Department of the Prime Minister and Cabinet (PM&C) to lead an annual evaluation process narrowly focussed on the NIC's support for policy making.

Recommendation 4: That, informed by a survey, the Department of the Prime Minister and Cabinet conduct an annual evaluation of intelligence support for policy and decision making.

Resource allocation and prioritisation

6.27 Like other parts of government, intelligence agencies make choices about the allocation of resources. This is more difficult in a high-demand, high-threat era. Some decisions require careful consideration of the possible risks of shifting resources from one target to another.

6.28 Appropriately, the NIC consults government on major resource allocation decisions. Even so, it is not necessarily easy for government to see the net effect of resource allocation decisions across the intelligence community. Existing mechanisms for providing advice to government could be used to provide a clearer, holistic picture of prioritisation and resource-trade off decisions that are being made across the NIC.

Recommendation 5: That the NIC more clearly articulate the allocation and reprioritisation of resources against the intelligence missions.

ONI intelligence assessments

6.29 The 2017 Review encouraged the then Office of National Assessments (ONA) to gear its reporting and assessments more directly to the needs and requirements of policy making. In line with recommendations from the Review, ONI's cadre of analysts has grown. ONI reports more on economic and technological issues. A morning 'Daily Brief' on intelligence issues of significance was launched. And ONI expanded its outreach to experts outside government.

6.30 ONI has worked hard to meet the intent of the 2017 Review. Its reporting is well geared to Australia's major international interests and to the global trends shaping the nation's external environment. In the main, ONI reporting is sought out and well regarded by its policy customers and Australia's Five Eyes partners. ONI's daily intelligence brief was widely praised as a 'must read'.

6.31 There is room to build on these successes. The global economy remains highly connected and interdependent. But fragmentation is occurring, driven by security, economic and political factors. The number of complex and consequential economic security policy decisions facing Australia is growing. This era will require ONI to continue to invest in economic expertise, to provide strong analytical support for government, and to effectively coordinative intelligence inputs to decision making. We recommend in *Chapter 9* changes to bolster ONI's support for policy makers on economic security.

6.32 High-quality analysis on geopolitical trends in the Indo-Pacific is, more than ever before, an essential asset for governments grappling with difficult policy decisions. In our consultations, policy makers emphasised the importance of such assessments reflecting government priorities and being timely, accurate and complete.

6.33 To support high-quality assessments, we encourage ONI to:

- Explore alternate futures or differing assessments. Such an approach was encouraged by the 2017 Review, which recommended that ONA should 'more often outline alternative points of view on contentious assessment issues'. ONI should also ensure its external outreach encompasses a diversity of expertise on regional affairs. In *Chapter 9* we outline proposals that will support contestability and bring analysts and policy makers together to share perspectives on major geopolitical developments.
- Ensure appropriate coverage of the global, regional and domestic – including economic and social – factors that will shape the actions of major regional powers.
- Support government to manage often competing national interests, such as protecting Australia's trading relationships while mitigating national security risks.

6.34 ONI employs 'policy opportunity' tradecraft in preparing assessments on geopolitical challenges – that is, it explores the implications and possible consequences of Australia's various policy options. This form of assessment has long been part of the armoury of intelligence assessment agencies. It was endorsed by Justice Hope, who argued that analysts 'cannot avoid, and should not seek to hide, the policy implications in what they report'.[9] The 2017 Review similarly argued that 'independent intelligence assessments

[9] Justice Robert Hope, *Royal Commission on Intelligence and Security*, Volume 3, [172].

need to draw out from their analysis the implications for Australian policy interests' and that 'this connection between high-quality assessments and policy needs to be further accentuated'.[10]

6.35 Understanding the implications of policy choices is more necessary than ever in light of the complexity and risks of the current era. Still, as we discuss in *Chapter 9*, policy opportunity analysis needs to be done with care so it does not become policy prescriptive, a dividing line that must be observed vigilantly.

6.36 There were concerns expressed at the time of ONI's creation, and in some submissions to this Review, that enterprise management would distract from ONI's essential analytical role. Building a stronger enterprise management function inevitably had to be a strong focus for ONI's first leaders. Still, we see no compelling evidence that this has affected the quality of ONI's assessment output. A bigger challenge for ONI is that it does not often operate with deep analytical benches, despite an increase in assessment staff following the 2017 Review.

Cyber security coordination

6.37 The 2017 Review made extensive recommendations in relation to cyber security. These included a new legislative mandate for the Australian Signals Directorate (ASD) to reflect 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'. Cyber security resources and capability were consolidated in 2018 in ASD's Australian Cyber Security Centre (ACSC).

6.38 In 2023, a National Cyber Security Coordinator position was established in the Department of Home Affairs (Home Affairs) to coordinate consequence management of major cyber incidents, amongst other roles. Our consultations, including with major Australian companies, indicate there is still some confusion about how the system works. This extends to the respective roles of the ASD's ACSC and the National Cyber Security Coordinator. In our discussion on NIC preparedness (see *Chapter 10*), we also consider the demands ASD would face, including meeting the needs of the Australian Defence Force (ADF) in the event of a major crisis or conflict, while also supporting government and the private sector on cyber security.

Security clearances

6.39 Clearance timeframes and assurance challenges were identified in the 2017 Review as a critical challenge for the NIC. Since then, clearance processes have been subject to significant levels of scrutiny and innovation through: an independent review in 2019; Australian National Audit Office audits; and the 2020 Future Positive Vetting Capability Taskforce. In December 2021, the TOP SECRET-Privileged Access (TS-PA) Vetting Authority was established within the Australian Security Intelligence Organisation (ASIO), marking the commencement of a new, centralised approach for granting, denying, revoking and maintaining TS-PA security clearances.

[10] 2017 Review, [2.32].

6.40 This is an important milestone in reform of the NIC's security clearance capability. Nonetheless, long clearance processes can still complicate agency recruitment. In part this reflects the imperative of sustaining high assurance standards in a more contested world, along with rising demand for the highest-level security clearances.

6.41 It is too early to assess the performance of the TS-PA Vetting Authority. This should be a matter for the next independent review. With appropriate resourcing, the TS-PA Vetting Authority will be well placed to deliver a high-quality TS-PA security clearance. Still, the demand for the highest-level security clearances is likely to remain very high. Realistic expectations are required about the speed with which clearances can be done while ensuring high standards.

6.42 Multi-classification workplaces are among a suite of innovations adopted by NIC agencies to manage long clearance processes without losing new employees along the way.

6.43 We look at these approaches and make recommendations in our section on clearances in *Chapter 15*.

Technology and data

6.44 The 2017 Review encouraged more innovation in, and greater integration of, NIC approaches to technology, including on data and information and communications technology (ICT) management.

6.45 The NIC has made headway on a number of fronts, including ICT modernisation, greater inter-agency collaboration and capability sharing. The NIC has improved its approach to technology uplift, establishing governance bodies, principles and processes to enhance sharing across the community, reduce capability duplication and strengthen connectivity. Strong, discrete bodies of work are underway that will collectively uplift enterprise-level capability.

6.46 However, practical and cultural barriers continue to impede true interoperability. The NIC could do more to recognise and manage the interdependencies between its various lines of effort on technology and data. Addressing these challenges is particularly necessary to ensure the community can effectively integrate artificial intelligence (AI) and other emerging technologies.

6.47 In our view, the NIC could also do more to support a sovereign technology industry in Australia and deepen its non-government partnerships.

6.48 We look at these issues in greater depth and make recommendations in *Chapter 13*.

Health of the NIC enterprise

6.49 A final reflection, looking back at the journey of the intelligence community since the 2017 Review, is that most NIC agencies do not have access to the increasingly sophisticated tools being used across the APS to build high-performance organisations.

6.50 We see particular value in NIC agencies being able to access the Australian Public Service Commission's capability review methodology (see *Box 2*). This would allow NIC agency heads to holistically consider organisational capability, including in relation to leadership, culture, workforce and enabling functions. This kind of deep internal consideration of

agency capabilities would complement rather than duplicate high-level independent intelligence reviews, which consider the entire NIC and focus in the main on enterprise level issues.

6.51 Where it might not otherwise be mandated by government in the future, we would see value in capability reviews being self-initiated by agencies every five years or so. Incoming agency heads, for example, might see capability reviews as a helpful guide to their organisational leadership.

Recommendation 6: That capability reviews be considered following the appointment of a NIC agency head. For those agencies under the *Public Service Act 1999*, this review should be performed by the Australian Public Service Commission. Otherwise, these reviews should be self-initiated.

Box 2. What is a capability review?

Capability reviews are independent and forward-looking. They assess an agency's ability to meet future objectives and challenges. They facilitate discussions around an organisation's desired future state, highlight organisational capability gaps, and identify opportunities to address them. Reviews are conducted in partnership with agencies.

The analysis covers five domains: leadership and culture; collaboration; delivery; workforce; and enabling functions. These are areas of organisational capability that reflect established models in other jurisdictions and contemporary research.

Implementation of the Comprehensive Review of intelligence legislation

6.52 A comprehensive review of the legal framework governing the NIC was commissioned by government, as recommended by the 2017 Review. The 2019 Comprehensive Review, as it became known, was largely supportive of the design and operation of the NIC's legislative framework, finding it to be 'carefully considered, balancing competing interests', especially those of individual liberties and collective security.

6.53 The 2019 Comprehensive Review's recommendations were based on detailed, thoughtful consideration of the concepts and ideas on which Australia's intelligence laws rest, especially where these preserve the values and ideas that underpin the NIC and democratic governance. We touch on some of these foundational principles in *Chapter 5*, and are in strong agreement with the 2019 Comprehensive Review's approach.

6.54 By its own admission, the 2019 Comprehensive Review is a long report, the unclassified version of which spans 1300 pages over four volumes. While supporting much at the core of the legislative framework for the intelligence community, the 2019 Comprehensive Review made 203 recommendations for reform, of which 190 were unclassified. Some of the most important recommendations were intended to simplify and modernise complex laws that were at times 'unclear and confusing' to NIC agencies.[11]

6.55 Given the scope of the 2019 Comprehensive Review and the deep research that underpinned it, we confine ourselves in this report to four observations.

6.56 First, progress has been made – at the time of writing, 54 recommendations had been implemented or were being considered by parliament. Another 57 have required no further action.

6.57 Second, the 2019 Comprehensive Review's most consequential recommendation – for a new single Act governing the use of electronic surveillance powers – has not been implemented. We recognise the scale and complexity of this reform. Nonetheless, our consultations demonstrated that the need for a new Act is pressing.

6.58 Third, notwithstanding the recency of the 2019 Comprehensive Review, there are areas where technological change and a shifting threat landscape mean some current laws are no longer fit for purpose. We recommend in *Chapter 17* several legislative changes to address these challenges. In one instance, we recommend a change that is sufficiently urgent that it should precede any new Act on electronic surveillance powers if necessary.

6.59 Fourth, the 2019 Comprehensive Review deferred consideration of several issues to future independent intelligence reviews. We therefore take up the following matters in other sections of this report:

- the roles of ONI, the Defence Intelligence Organisation and Home Affairs in collecting open source information, to ensure the boundary between open source and covert collection is not being crossed

[11] Dennis Richardson AC, *Comprehensive Review of the legal framework of the National Intelligence Community* (2019 Comprehensive Review), December 2019, [3.8].

- whether the Australian Geospatial-Intelligence Organisation should be made a statutory authority
- processes for managing potential foreign relations risks posed by the use of intelligence effects
- whether statutory controls on the collection, retention or use of reference data are required
- the use of AI for intelligence purposes.

Chapter 7. The National Intelligence Community's evolving architecture

7.01 The structure of the National Intelligence Community (NIC) has changed considerably in recent years (see *Box 3*). More agencies are at the NIC table, bringing with them important capabilities but also the need for different approaches to integration, governance and oversight. New statutory authorities have been created. Some agencies have taken on additional roles and responsibilities.

7.02 The intelligence community will continue to evolve in response to strategic circumstances, government requirements and reviews such as this one. This is healthy and necessary. At the same time, large structural changes consume a great deal of time and effort. A degree of reform fatigue was evident during our consultations.

Box 3. The journey since the 2017 Intelligence Review

- The community expands from six to ten agencies.
- The Office of National Intelligence is created with additional resources to support management of the intelligence community as an enterprise.
- The Australian Signals Directorate (ASD) becomes a statutory agency. Cyber security resources are consolidated in 2018 in ASD's Australian Cyber Security Centre.
- The Department of Home Affairs and the Defence Intelligence Group are created.
- A 'polycrisis' world emerges.
- Intelligence diplomacy and other activities are used by agencies as tools to achieve outcomes for government.
- Workforce pressures increase due to a tight national labour market.
- New funding supports agency modernisation.
- Intelligence support for the *2024 National Defence Strategy* requires new defence intelligence capabilities.

From six to ten – strength in numbers

7.03 The 2017 Review expanded the former 'Australian Intelligence Community' of six 'core' agencies to a 'National Intelligence Community' of 10 agencies.

7.04 The creation of the NIC reflected the environment at the time, especially the prominence of terrorism and other threats, such as the rise of powerful organised crime groups, many with international links. What constituted intelligence needed to be reimagined and new capabilities brought into the community.

7.05 The expanded intelligence community therefore incorporated the criminal intelligence expertise of the Australian Criminal Intelligence Commission (ACIC), the law enforcement intelligence functions of the Australian Federal Police (AFP), the financial intelligence expertise of Australian Transaction Reports and Analysis Centre (AUSTRAC) and the intelligence functions of the Department of Home Affairs (Home Affairs).

7.06 Differences in agency roles, responsibilities and cultures inevitably mean some agencies work more closely together than others, and this is especially so with the 'original' six agencies of the Australian Intelligence Community.

7.07 The full potential of the expanded community will only be realised through strong collective leadership by heads of agencies. Building a sense of community that transcends individual agency identity is essential. So too is understanding and respecting what the newer NIC members can bring to the table – this will ensure the most effective use of the combined expertise and assets of all 10 NIC members.

The Office of National Intelligence

7.08 As we discussed in the previous chapter, the 2017 Review's most consequential recommendation was to create the Office of National Intelligence, replacing the former Office of National Assessments, to lead enhanced enterprise management of the intelligence community.

The Australian Signals Directorate

7.09 Following recommendations made in the 2017 Review, on 1 July 2018 the Australian Signals Directorate (ASD) became a statutory agency within the Defence portfolio reporting directly to the Minister for Defence.

7.10 Also on 1 July 2018, cyber security-related functions from the Digital Transformation Authority, Attorney-General's Department and Department of the Prime Minister and Cabinet were incorporated into ASD. These elements were integrated into ASD's existing Australian Cyber Security Centre (ACSC).

7.11 ASD's establishment as a statutory agency was underpinned by legislative reform that included expanded functions related to ASD's national responsibilities for cyber security, including the provision of advice to the private sector.

7.12 ASD's prominent position as a statutory agency in the NIC reflects its important national responsibilities, ones that now go well beyond support for the Australian Defence Force (ADF). This successful transition supports the intent of the 2017 Review. Operating as a statutory agency has also allowed ASD more flexibility in its approach to recruiting and remunerating staff, an important consideration given its need for highly skilled employees.

7.13 Following a recommendation from the 2017 Review, a military officer was appointed as the principal deputy in ASD. This was to ensure ASD remained attuned to ADF requirements, even as it took on additional responsibilities. The practice of a principal military deputy was discontinued after a period.

Establishment of the Defence Intelligence Group

7.14 In line with the recommendations of an independent internal review into the Defence Intelligence Enterprise, the Defence Intelligence Group (DIG) was established in 2020 to enhance intelligence support to the war-fighter. The group includes the Australian Geospatial-Intelligence Organisation (AGO) and Defence Intelligence Organisation (DIO). The Chief of Defence Intelligence leads the DIG and is Director DIO.

Australian Geospatial-Intelligence Organisation

7.15 The 2019 Comprehensive Review of intelligence legislation (2019 Comprehensive Review) considered the question of whether or not AGO should be made a statutory authority. The Review concluded that this should occur if Australia acquired its own GEOINT satellite capability.

7.16 This threshold has not yet been met. In these circumstances, we agree with the 2019 Comprehensive Review that there is no compelling argument for AGO to follow in the footsteps of ASD. We are conscious also of the high administrative overheads that come with statutory independence, especially for small agencies. The matter should be reconsidered if and when circumstances change.

Establishment of Home Affairs and changes to portfolio structures

7.17 The Home Affairs portfolio was established in December 2017. The Australian Security Intelligence Organisation (ASIO), AFP, ACIC and AUSTRAC were transferred from the Attorney-General's portfolio to the new portfolio.

7.18 In July 2022, the Albanese Government returned the AFP, ACIC and AUSTRAC to the Attorney-General's portfolio. ASIO was subsequently also returned to the Attorney-General’s portfolio.

7.19 We did not identify during our Review, including in the Hope royal commissions, any principles based barrier to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) being administered by a minister other than the Attorney-General. Nonetheless, regardless of its place in Australia’s system of portfolio government, in our view it will always be essential for the Attorney-General to retain the function of authorising sensitive activities under the ASIO Act, the *Telecommunications (Interception and Access) Act 1979* and those activities provided for under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, including issuing ASIO warrants and authorising special intelligence operations. These responsibilities properly sit with the Attorney-General as the first law officer.

Part III: Positioning for the future

Chapter 8. Building on intelligence community strengths

8.01 Part I of this Review looked at global change and its implications for Australia's intelligence agencies. We concluded that there would be no respite from current levels of high demand on the National Intelligence Community (NIC) and the drain on resources, capabilities and people this entails. We emphasised the way in which intelligence is being reshaped by the technology and data revolution. We highlighted the risk of strategic surprise and the need for the intelligence community to be prepared for major crises. And we recognised the power of strong partnerships in this complex and demanding environment.

8.02 Part III of this Review is informed by these conclusions. We look ahead, and consider how well placed the intelligence community is to meet a future that, at least in part, is already evident. In our view:

- Stronger and deeper integration between the NIC and its policy counterparts is urgent and essential. These efforts should be guided by one unifying objective – to maximise the effective use of intelligence as an arm of Australian statecraft in a more contested and competitive era, informed by policy priorities.
- Intelligence agencies must work closely together and in innovative ways to meet the future needs of government. This is especially so when it comes to technology, workforce, preparedness and partnerships, including with domestic stakeholders.
- Legislative change is needed to enable the NIC to better combat threats emerging from a fast-changing geopolitical and technological landscape. In some instances, the need for reform is urgent.

8.03 In setting out a forward-looking agenda, we look to complement work already underway in intelligence agencies, and to do so in ways that bolster cross-community collaboration and integration. This approach reflects the importance of managing the intelligence community as an enterprise, as recommended by the 2017 Review.

8.04 Our recommendations also build on the clearly evident strengths of the NIC. While we identify some challenges across this Review, Australia's intelligence community is performing well and generally effectively meeting the needs of government. The NIC brings world-class capabilities to bear on Australia's security challenges and is staffed by highly skilled and committed individuals.

8.05 The NIC has proved its ability to adapt and innovate in a challenging environment. For example, the community has boosted collection and assessment on strategic and economic developments in the Indo-Pacific. This intelligence provides insight for government and is an essential input to policy making on Australia's highest foreign policy priorities and in support of the *2024 National Defence Strategy*. Stronger international intelligence partnerships, especially with the Five Eyes, ensure government benefits from the combined strengths and expertise of the nation's closest partners.

8.06 The NIC is introducing new technologies, including AI, to make sense of large volumes of information, inform analysis and operations, and provide additional decision making advantage to government.

8.07 Agencies have responded to a sharp rise in espionage and foreign interference, devoting additional resources and attention to these challenges. This has included outreach to Australian companies and universities to help them understand and respond to a new threat environment. And the NIC is now integral to government efforts to ensure the integrity of Australian elections.

8.08 The NIC continues to identify, disrupt and help harden Australia against terrorist threats. The community remains vigilant against a possible resurgence of terrorism, including from conflict in the Middle East.

8.09 The inclusion of the AFP, Australian Criminal Intelligence Commission (ACIC) and Australian Transaction Reports and Analysis Centre (AUSTRAC) in the NIC increases the community's understanding of, and ability to respond to, security challenges. For instance, the ACIC's unique coercive powers provide valuable intelligence on transnational crime. And the Australian Federal Police has worked with ACIC, Australian Signals Directorate (ASD) and AUSTRAC to combat ransomware threats and to respond to major private sector cyber data breaches.

8.10 The intelligence community also continues to effectively support the Australian Defence Force (ADF). Those agencies with a specific defence focus – Defence Intelligence Organisation (DIO), Australian Geospatial-Intelligence Organisation (AGO) and ASD – demonstrate clear ongoing value through their military and strategic insights. Their work remains critical to Defence decision making, strategic planning and defence operations. The broader community's work also often intersects with and supports defence operations.

Chapter 9. Intelligence and Australian statecraft

9.01 Australia's intelligence and policy communities generally work together closely and collaboratively. And, collectively, Australia's intelligence agencies work hard to support executive government.

9.02 Nonetheless, a principal finding of this Review is the need to optimise the integration of intelligence and policy for an age of heightened risk and challenge. This will require change in policy agencies as much as it imposes new demands on the intelligence community.

9.03 Intelligence is only one of several primary inputs for policy making – it does not and should not drive policy by itself. Still, it is undeniable that intelligence is more prominent in some areas of policy making today than it has been in past decades. This experience is not unique to Australia – it is a reflection of the times.

9.04 The importance of maximising the value of intelligence to Australian statecraft was therefore a strong theme running through submissions to the Review and in our consultations. There was agreement from both intelligence leaders and policy makers that Australia's deteriorating national security circumstances demanded change. But perspectives on 'good' intelligence–policy integration varied, as did views on whether incremental or deeper structural reform is needed.

9.05 Points commonly made to us by policy makers included the importance of the intelligence community working to objectives and priorities set by government, the desirability of strong central coordination of intelligence policy by the Department of the Prime Minister and Cabinet (PM&C), and the need for additional intelligence support for ministers and agencies newly drawn into national security decision-making.

9.06 Intelligence agencies want stronger intelligence literacy in the policy world – an understanding of how they work and the ways in which they support government – and the best possible use of intelligence in informing policy and responding to threats to national security.

9.07 In our view, strong intelligence–policy integration is needed to:

- ensure the intelligence community is aligned with policy priorities and working closely and in a coordinated way with executive government
- animate the processes of contestability that help develop robust intelligence insight for government
- ensure intelligence is well used in warning, planning and policy development, and that intelligence tools are deployed where appropriate to respond to threats and influence outcomes
- maximise the return on the cost of running a world-class intelligence enterprise.

9.08 It is generally accepted among Five Eyes partners that it is intelligence agencies that bear most responsibility to grab the attention of busy policy makers – to build understanding of how intelligence can help decision making and to ensure governments have the intelligence support they need, when they need it, and where they need it.

9.09 This is also the case for Australia. Still, in the current era such obligations cannot be one sided. We identify an equal set of responsibilities for the policy community, including clarity on intelligence priorities and requirements and being able to operate securely in a world in which Australia's secrets are more vulnerable than ever to espionage.

9.10 The intelligence–policy integration challenge is evident not just in 'traditional' security challenges but in the rapidly growing domain of economic security, where risks to prosperity, security and sovereignty are increasingly complex to manage and pose difficult choices and trade-offs for Australia.

9.11 Support from the intelligence community for economic security decision making is improving. In some instances, however, government has sought faster advice and more options to manage risk.

9.12 Across this Review, we identify reforms that, if undertaken collectively, would significantly bolster intelligence–policy integration. In this chapter, for example, we propose:

- an enhanced model for intelligence support for ministers
- stronger central coordination of intelligence policy matters
- investment in the 'enablers' both physical – like secure IT systems – and cultural that promote effective use of intelligence by policy agencies
- an uplift in intelligence support on economic security and a matching review of economic security policy-making architecture
- mechanisms to bolster contestability processes for all-source intelligence assessment
- a policy to manage the public release of intelligence where this would support national interests.

Intelligence support for ministers

Understanding the business of intelligence

9.13 Ministers are often sworn into office having had little to no prior engagement with the intelligence community. It will not always be immediately obvious to them how intelligence agencies can help them in their duties. They and their offices may not have had to manage, store and protect classified information before.

9.14 As we understand it, there is no standardised briefing for ministers on intelligence matters – for example, the distinct roles of each agency, the role intelligence plays in national security decision making, classifications and security handlings, and what products are available for ministers to access. Nor is there a similar briefing for ministerial staff.

9.15 In the current era, this is too ad hoc. Intelligence is a vital enabler of national security decision making. It would help ministers when they are sworn in to have a good understanding of what intelligence is and what it does, and also – importantly – what it cannot do.

Recommendation 7: That the Directors-General of National Intelligence and Security develop an 'Introduction to Intelligence' briefing for ministers and appropriately cleared ministerial staff. This briefing should be offered after a change of government or following a ministerial reshuffle, and could also be made available on request at other times.

9.16 Annual or six-monthly briefings to the full Cabinet by the Directors-General of National Intelligence and Security would be a complementary initiative. This would ensure a common information base on shifts in the foreign and domestic security landscape, and provide ministers with the most contemporary perspectives regarding precautions against espionage and foreign interference.

Recommendation 8: That, building on briefings already provided to the National Security Committee of Cabinet on the foreign and domestic security environment, the Directors-General of National Intelligence and Security provide dedicated annual or six-monthly oral briefings to the full Cabinet on shifts in Australia's security environment with particular implications for the operation of government, such as espionage and foreign interference.

Intelligence when it is needed, where it is needed

9.17 Intelligence support for ministers is a particularly important function of the National Intelligence Community (NIC). The nature and frequency of NIC engagement with ministers understandably varies depending on portfolio responsibilities. Still, as we note elsewhere, as Australia grapples with a more complex world, intelligence is informing policy on a broader range of issues, including where globalisation and economic dependencies create national security risk. This means more ministers require intelligence support more often. A more volatile international environment also means ministers need intelligence support out of Canberra more often. This is especially so in a crisis, when speed is of the essence in getting advice to ministers.

9.18 In short, increasingly the intelligence community is required to provide fast, agile, nation-wide intelligence support for executive government, and on a diverse set of issues. In our view, current processes cannot fully meet this objective. All NIC agencies must and should continue to engage ministers directly. Nonetheless, given the importance to government of assessed intelligence, we believe there is a strong case to resource the Office of National Intelligence (ONI) so that it can re-gear its intelligence support business model to the new era. This will require coordination with other agencies to make best use of the NIC network across Australia and new investment in production, dissemination and engagement.

9.19 We also encourage the development of innovative technological solutions to support the delivery of classified material to government more quickly and easily than is possible at the moment.

Recommendation 9: That the Office of National Intelligence provide more regular customer support to a broader range of ministers and strengthen its ability to deliver timely intelligence advice, including outside Canberra.

Intelligence and policy

9.20 While many Australian intelligence agencies are statutory entities, and exercise their powers independently, the intelligence community does not operate in isolation. Intelligence agencies are accountable to ministers and ultimately to the Parliament. There is regular collaboration with policy agencies. And governments make decisions on resourcing, develop laws that govern intelligence activities, consider agency performance, and agree intelligence priorities.

9.21 In Australia, the financing and governance of the intelligence community involves a number of policy agencies, with PM&C having a coordinating role. This mirrors, albeit not in identical ways, arrangements in Australia's closest intelligence partners. In the United Kingdom, for example, the Cabinet Office supports government decision making on the intelligence community. Similar functions are performed by National Security Council staff in the United States.

9.22 In the United States and the United Kingdom, central policy agency engagement with the intelligence community is regular, dynamic and robust, especially when it comes to resource allocation.

9.23 Effective management of intelligence policy provides contestability, helps with performance and supports the alignment of intelligence activities with government priorities. PM&C should be adequately resourced to undertake this role, especially in light of the growth in both the size of the intelligence community and its current importance to policy making.

9.24 More broadly, it was clear from our consultations that agencies in both the intelligence and policy communities see a need for, and would welcome, a strong central coordinating role for PM&C across the entire national security agenda.

9.25 We recommend additional focus by PM&C on intelligence priorities and requirements, resource allocation and funding trade offs. We have recommended elsewhere in this Review a role for PM&C in the evaluation of the intelligence community's support for policy makers (see *Chapter 6)*. There is also an important role for PM&C in working with agencies on issues that have implications well beyond the intelligence community, such as preparedness for crises or conflict, legislative matters and national-level governance of new technologies like artificial intelligence (AI).

9.26 The intent of these recommendations is not to cut across ONI's statutory responsibilities. These must be respected. Rather, the objective is stronger governance of intelligence policy matters.

Recommendation 10:

That the Department of the Prime Minister and Cabinet be resourced to provide stronger central coordination of national security policy matters.

Capabilities of policy departments

9.27 Policy departments recognise that in a more contested era, intelligence provides unique insights and important context for policy agencies preparing advice for government. Senior policy officers are among the NIC's most important customers.

9.28 Still, managing intelligence in policy departments is resource intensive. Curating, distributing and protecting classified information requires considerable investment in "enablers" such as security clearances and secure IT infrastructure. This is taxing even for large policy departments in the national security community, but particularly so for agencies that have had in the past only occasional need to deal with intelligence, but which are now being drawn into complex economic security decision making.

9.29 In our judgement, the need for policy agencies to be able to effectively incorporate intelligence insights, and intelligence effects, into their operations will only grow. Where they might not already be doing so, policy agencies need to audit their ability to work at the highest classification levels and make realistic judgements about future needs. Optimising intelligence-policy integration will be more difficult without adequate ongoing investment in the necessary "enablers". This is an urgent priority.

Recommendation 11: That policy agencies invest in adequate infrastructure and other enablers to allow the most effective use of intelligence to inform policy making.

Is over-classification the problem?

9.30 Most policy agencies want more intelligence at lower classification levels. Options to help policy agencies with limited staff cleared to the highest levels include lower classification 'tear lines' – summaries of intelligence reports that remove the most sensitive information – and more reporting using open source information, including commercially available imagery.

9.31 The NIC could also do more training to guard against the bias in intelligence agencies to operate at the TOP SECRET level. Culture matters to some extent here, but so do practical considerations, including the NIC's predominant use of TOP SECRET systems. At least to some extent, the NIC produces at TOP SECRET level because it can. Most of its customers, however, operate on SECRET-level information and communications technology systems, or below.

9.32 We encourage the NIC to consider, in a more determined way, how it can get lower classification products into the hands of its customers. It is in its own interests to do so.

9.33 Equally, it is important for policy agencies to understand this is in many ways more difficult today than it has been in the past. The most valuable intelligence for policy makers will often be the most highly classified, and this intelligence must be protected vigilantly against espionage and unauthorised access.

9.34 We have provided separate advice to government on additional options for supporting the production of intelligence at lower levels of classification.

Intelligence literacy

9.35 Fostering a culture that encourages policy officials to use intelligence early and comprehensively in developing guidance for government is important. This has not proved easy in the past in some policy agencies, not least because it is often difficult for mid-ranking officers to access intelligence products.

9.36 Higher levels of intelligence literacy – an understanding of the structure and foundational principles of the NIC and how it can support statecraft – is important.

9.37 We see an important role for ONI's National Intelligence Academy in this regard and encourage policy agencies to use the academy's training courses. Recognising the distinct roles and functions of individual agencies, we also recommend stepped-up direct intelligence community education outreach to the policy community.

9.38 Greater mobility between NIC and policy agencies will also foster a sense of shared culture and go some way towards improving interoperability. Where possible, we recommend leadership support the flow of staff across the communities through secondments and exchanges. Such arrangements would benefit both the intelligence and policy communities.

Recommendation 12: That the NIC develop a coordinated intelligence outreach and education initiative to the policy community that recognises the distinct roles of agencies while leveraging the National Intelligence Academy where appropriate.

Matching intelligence outputs to policy priorities

9.39 The value of intelligence as a tool of statecraft will always be strongest where it is closely aligned to priorities and objectives set by governments. This is one of the benchmarks for effective intelligence–policy integration.

9.40 The NIC's mission management processes are designed with this objective in mind. They help align intelligence outputs with policy requirements and manage resource trade offs.

9.41 This is a two-way process. Policy agencies must be – but are not always – clear and specific about their intelligence requirements. The NIC can help by talking regularly to policy agencies about their requirements and by building understanding of where the intelligence community can and can't help. Regular outreach also helps policy agencies navigate the necessary secrecy that cloaks some NIC structures and processes. Some need more support than others. In our view, this is particularly so for policy agencies that have less experience of working with the intelligence community, but are now drawn into economic security decision making. These agencies can find it particularly difficult to navigate and influence unfamiliar mission management processes. While ONI can't deliver the same intensity of mission management for all intelligence priorities, there is scope for it to apply the lessons learned from success across other intelligence missions when it comes to supporting economic security policy making.

Economic security

9.42 Of all the changes since the last review of the intelligence community in 2017, three stand out as the most profound for intelligence and statecraft. One is a much more contested

global order defined by tense competition between nation-states, and especially between the United States and China. A second is technological shifts. The third is a new era of global economic fragmentation, economic nationalism, coercion and protectionism, de-risking, and industrial strategy.

9.43 Australia now balances multiple interdependent economic security[12] policy objectives, including the need to bolster the resilience of supply chains and trade, build capacity to deter or respond to economic coercion, support a clean-energy transition, ensure the effectiveness of sanctions, protect critical infrastructure and technologies, and manage sensitive foreign investment.

9.44 Policy agencies and the intelligence community are responding to this new era. The Australian Security Intelligence Organisation, ONI, and the Defence Intelligence Organisation, for example, have enhanced their assessments and advice on economic security issues. Recently announced reforms take a stronger risk-based approach to foreign investment in sensitive sectors like critical infrastructure and critical minerals.

9.45 Collectively, these are welcome initiatives. Even so, in our judgement Australia's intelligence and policy agencies will have to keep innovating and adapting to match the pace of global change and the complexity of policy choices governments must now make. Many of Australia's closest partners are doing just this.

9.46 While we predominantly confine ourselves to recommendations to drive stronger intelligence support for policy makers, our consultations suggest that more holistic and structural changes across the public service are required. Outside of the Treasury, policy frameworks and principles to aid economic security decision making could be strengthened. It is important to ensure advice to government encompasses all relevant national interests and is not siloed.

9.47 Agencies covering important policy areas like agriculture, infrastructure, telecommunications, climate change, energy, industry, resources and health need to be fully consulted and brought into economic security decision making processes at an early stage.

9.48 Given the Treasury's broad economic perspective and responsibilities, it is best placed to lead development of cross-agency arrangements to balance economic and national security priorities and support government decision making on economic security.

Recommendation 13: That the Treasury lead a broad review of the structure and effectiveness of economic security functions across government.

9.49 We also recommend that a distinct function be created in the Treasury whereby a small number of intelligence officials from relevant NIC agencies are embedded to more closely fuse intelligence and policy efforts on economic security issues. The intent is to provide:

- visibility of strategic trends, shifts and threats with implications for Australia's economic security

[12] Economic security can be defined in various ways. We are concerned in this Review with a broad area of policy making that considers how, in an era of geopolitical rivalry, Australia can best balance the opportunities and risks that arise from economic interdependency.

- analysis of long-term implications of Australia's economic security decisions, including the aggregation of risk
- horizon-scanning to better anticipate and plan for future economic security challenges
- scenario planning and the integration of intelligence and policy expertise into such activities
- inject intelligence insights and analysis into policy frameworks and tactical government decision making such as investment decisions and sanctions activities
- help align intelligence efforts and policy priorities.

Recommendation 14: That a distinct economic security function be established in the Treasury, including secondees from relevant NIC agencies.

9.50 In our view, the intelligence community should invest more in the economic and other expertise needed to support economic security policy making. The demand for such expertise will only grow in the future. Complex economic security issues are multi-dimensional, often encompassing geopolitical, security, technological, economic, financial, legal and corporate structure considerations. NIC agencies can't be expert in all these domains, but they do need to be able to navigate across them. Australian governments also need sovereign intelligence advice when it comes to balancing security and prosperity and managing the associated trade offs.

9.51 We encourage NIC agencies to progressively build and deploy the expertise needed to provide accurate, timely advice for policy makers. In particular, we recommend that ONI's capacity to support economic security decision making be strengthened, including so that it can better lead intelligence integration and coordination on economic security and work more closely with policy agencies outside the traditional national security community.

Recommendation 15: That the capacity of the Office of National Intelligence to support economic security decision making be strengthened.

Value of contestability

9.52 We recommend reinforcing the contestability processes that help ONI, as Australia's peak all-source assessment agency, develop robust analytical judgements and bring intelligence and policy agencies together to consider Australia's most pressing global challenges. This was an objective also encouraged by the 2017 Review. Similarly, the *2004 Report of the Inquiry into Australian Intelligence Agencies* (Flood Inquiry) underlined the value of contestability processes to provide a check against faulty assessment and ensure that the full weight of government and non-government expertise is brought to bear on analytical challenges.

9.53 Our recommendations build on ONI's strong existing contestability mechanisms. There are several ways in which this could be achieved. First, we recommend ONI convene roundtable discussions involving all relevant intelligence and policy agencies to consider selected draft intelligence assessments. While ONI already consults individual agencies in

the drafting process, we believe roundtable discussions on those assessment products that address the highest government priorities would support contestability.

9.54 These collective discussions should occur at an appropriately senior level, with representatives from all agencies empowered to make an active contribution. Final analytical judgements should properly remain ones for ONI alone. But ONI should ensure there are opportunities for differences of view, where they might exist, to be expressed and subsequently explained in the assessment product being considered, as is possible when National Assessments are prepared. Senior policy makers from Australia's close partners told us they found explanation of differences healthy and useful and encouraged this in their respective intelligence communities.

9.55 We also encourage:

- more use of structured analytical techniques (SATs) on big picture issues, with broad participation including at senior levels from intelligence and policy agencies
- distributing SAT summaries with the list of participating agencies to senior customers to make the consultation more visible
- acknowledging differences of analytical perspectives, where they might exist, in a box in reports
- ensuring readers have better visibility of policy and other agency input to scoping processes and identifying where opportunity has been provided to comment.

Recommendation 16: That the Office of National Intelligence bolster its contestability processes for analytical products by: convening intelligence and policy agency roundtable discussions on selected intelligence assessments on major global challenges; making more use of structured analytical techniques; and acknowledging differences of analytical perspectives, where they might exist.

9.56 National Assessments are joint assessment products, representing the views of relevant intelligence and policy agencies. They are major pieces of work prepared by ONI that tackle large trends and issues affecting Australia's security and prosperity.

9.57 National Assessments are a powerful vehicle for discerning emerging trends and signals amidst the noise of daily intelligence flows. They retain value for warning and strategic planning, sometimes simply for reducing to digestible form complex global trends. Done well, they illuminate long-term national interests and where they might be threatened. As a joint assessment product where dissenting views can be expressed, National Assessments also make an important contribution to the contestability of intelligence assessments, as emphasised by the Flood Inquiry.

Recommendation 17: That the Office of National Intelligence produce at least two National Assessments each calendar year.

Effects and intelligence diplomacy

9.58 Some intelligence agencies have a legislative mandate to conduct activities to disrupt or influence activities harmful or contrary to Australian interests.[13] This is one manifestation of a more contested world of rivalry between nation-states. Where such activities are being considered, it is vitally important that they are closely and carefully managed to ensure they are lawful, advance national interests and do not create disproportionate foreign relations risks.

9.59 Australia's intelligence leaders and their agencies also play an important role in the Indo-Pacific and globally in building relationships and conveying messages that advance wider government foreign policy priorities. The value of such "intelligence diplomacy" is maximised when it supports, and is carefully aligned with, traditional Australian diplomacy.

Public release of classified intelligence

9.60 In some circumstances, declassifying and then publicly releasing intelligence can be a powerful tool of statecraft, in peacetime or during a crisis or conflict. The United States and the United Kingdom used intelligence extensively in this way in the run-up to, and following, Russia's invasion of Ukraine. Foreshadowing the invasion did not deter Russia, but it did warn Ukraine and significantly diminish Russia's efforts to justify its actions through disinformation.

9.61 The public release of intelligence should be undertaken judiciously and in support of clear and practically defined policy objectives. It must be done mindful of:

- the risk of compromising sources and intelligence capabilities
- the interests of Australia's intelligence partners
- possible consequences for foreign relations.

9.62 Clear guidelines, thresholds, operating procedures and frameworks are needed and will position the intelligence community to support the release of intelligence when government determines this is appropriate.

Recommendation 18: That the Office of National Intelligence and relevant policy agencies develop a policy for the declassification and public release of intelligence.

[13] The National Intelligence Community, *How we protect Australia.* Available at: https://www.intelligence.gov.au/how-we-protect-Australia.

Chapter 10. Preparedness

10.01 The need to be better prepared for a regional crisis or conflict is now an important focus of national security planning and policy making. The *2024 National Defence Strategy* places preparedness and resilience at the centre of effective deterrence. The Government wants to strengthen the ability of the Australian Defence Force (ADF) to 'endure and recover from disruption'.[14] And in the current era, the intelligence community needs to be prepared for a broader range of crises, such as another major pandemic.

10.02 In crisis and conflict scenarios, government and the ADF's resilience will depend in part on the intelligence community, including for decision making advantage, strategic warning and direct support to military operations. But demands on the intelligence community will go well beyond military operations to encompass national security and economic decision making and support for social cohesion.

10.03 State and territory governments and the private sector will also want warning, advice and support, especially in relation to protecting critical infrastructure. The expectations of Australia's close intelligence partners will be high.

10.04 There is some preparedness work underway in the community. More effort won't be wasted – a well-designed approach will also support the day-to-day operations of the intelligence community, whether or not a crisis occurs in the future.

Collective and coordinated efforts

10.05 There is no straightforward answer to the question of how much to invest in preparedness for events that are inherently uncertain, especially in a period when demands on the intelligence community are high. And, to some extent, the NIC can rely on necessity to drive adaptation and innovation in a crisis.

10.06 Even so, the immense challenges the NIC would face in meeting government needs during a major crisis or conflict demand a focused and committed approach to preparedness.

10.07 Preparedness efforts could be assisted by the appointment of a single senior officer with responsibility for the coordination of preparedness activities and tracking their progress.

> **Recommendation 19:** That the Office of National Intelligence appoint a senior officer to coordinate NIC preparedness for regional crises or conflicts and track progress against activity.

10.08 Our Review makes other recommendations that will directly support NIC preparedness. In particular, in *Chapter 9*, we recommend an uplift in the NIC's ability to meet the intelligence needs of its customers in government and policy agencies. Also in *Chapter 9*, we recommend work begin immediately on a policy and procedural framework for the public release of intelligence. In *Chapter 17*, we recommend policy agencies lead a review to identify whether there are legislative barriers that may prevent the NIC from effectively responding to a conflict.

[14] Australian Government, *National Defence Strategy*, 2024, p 27.

10.09 In addition, we judge the NIC preparedness agenda would benefit from:

- a mandate from government
- regular exercising and scenario planning
- better definition of what the NIC will need to do to meet requirements in a crisis or conflict and what capability gaps can reasonably be remedied given resource constraints
- more secure space outside Canberra
- an enhanced national-level strategic warning capability.

A mandate

10.10 It is sensible for the NIC to consider its preparedness for a regional crisis or conflict given the current global context, reduced warning times and the prominence preparedness now has in defence planning.

10.11 Even so, a clear mandate from government, including to define expectations of the NIC in a crisis, will help with prioritisation and resource allocation. This guidance could be issued by the Prime Minister to the Director-General of National Intelligence (DGNI) through the directions power in the *Office of National Intelligence Act 2018.*

Recommendation 20: That the Prime Minister issue a directive under the *Office of National Intelligence Act 2018* to set out expectations for NIC preparedness for regional crises or conflicts.

10.12 There is appetite within the community for more preparedness scenario planning and for exercising to be done on a regular tempo. This will stress-test current NIC systems, clarify requirements and allow the Office of National Intelligence (ONI) to identify any shortfalls that can be remedied.

10.13 Central coordination of NIC preparedness should be accompanied by close working relations between the intelligence community and policy agencies on national-level preparedness and resilience policy making. This is essential both to inform both the NIC's preparedness agenda and to ensure the needs of the intelligence community are considered in national-level planning.

Recommendation 21: That regular exercises be undertaken within the NIC and with policy agencies to test and improve preparedness for regional crises or conflicts.

Workforce pressures

10.14 The NIC's people will be its primary asset during a major crisis or conflict. Many parts of the community will operate on a 24/7 basis. Sustaining this tempo would not be easy; managing staff welfare will be a priority.

10.15 We explored the feasibility of a workforce surge program as one response to a prolonged major crisis. This could draw on resources elsewhere in government and/or 'reactivate' former NIC employees.

10.16 Ultimately, however, we concluded that neither option would provide more people quickly. This judgement is broadly shared across the community. Experienced staff will be in demand everywhere in government. And even in a conflict, perhaps especially in a conflict, security clearance standards must remain high.

Operating outside Canberra

10.17 The NIC is conscious of the need to be able to work securely in locations outside Canberra. This would be especially important in a major global crisis. An existing network of agency offices in capital cities helps to an extent. Some agencies also have a regional presence. Under ASD's REDSPICE program, more secure space is being built in Melbourne, Perth and Brisbane.

10.18 Additional options for the NIC to work in an integrated fashion in secure locations outside Canberra would nonetheless be helpful.

10.19 Continuing to invest in a larger footprint outside Canberra makes sense for the intelligence community. This would help the NIC work with one or more state and territory governments. It would provide additional options to support the intelligence needs of ministers. And it would provide secure collaboration spaces for the NIC, industry and the research sector. Importantly, in a major crisis it would provide additional redundancy of NIC facilities. While not directly related to preparedness, more secure space could also provide opportunities to recruit people with essential skills who might not want to move to Canberra.

Recommendation 22: That the Department of Finance and the NIC lead scoping of options to build NIC resilience and engagement outside Canberra.

Warning

10.20 Warning government of imminent or emerging national security threats is an essential NIC function. Some NIC agencies have well-established warning functions, but we propose an enhanced, national-level 'strategic warning' capability that can respond to political, economic and strategic matters.

10.21 In the Cold War, strategic warning usually related to conflict. Its purpose was to alert leaders that an attack was imminent (as opposed to already underway). Today, strategic warning encompasses a diverse range of threats and challenges that require some kind of response. Alerting government to a global climate tipping point, future pandemic or a large geopolitical shift is as necessary as warning of imminent conflict.

10.22 The Defence Intelligence Organisation (DIO) has responsibility for strategic warning to inform defence policy, the planning and conduct of operations, and to guide capability development. While not 'strategic warning', we note here for completeness that the Australian Security Intelligence Organisation (ASIO) has a warning function through the National Threat Assessment Centre's advice to government on threats such as terrorism and foreign interference. The Australian Criminal Intelligence Commission (ACIC)

increasingly performs a similar role in relation to transnational, serious and organised crime.

10.23 Warning is implicit or explicit in much of the analysis ONI produces, but in our judgement there is both scope and need, given current strategic circumstances, to bolster ONI's strategic warning role.

10.24 One model proposed to us was the appointment of a National Intelligence Officer for Warning – a senior intelligence official to operate within ONI and across the community as 'chief warner'. We considered this model carefully. While a strong central warning function has some advantages, we ultimately concluded that in a polycrisis era warning was best done across ONI's expert all-source analytical teams.

10.25 We recommend instead that a warning methodology cell be established in ONI. Over time, the goal would be to build a centre of excellence on warning tradecraft. This would support the analytical rigour of warning work across ONI. It could help strengthen the warning network in the NIC that includes DIO, ASIO and ACIC.

10.26 An annual ONI-led National Assessment covering strategic and other trends that might pose significant risk to Australia would also support government horizon scanning. Subject to the views of government, there could be scope for a public version of the assessment, or a speech on it, as is the case for the annual threat assessment coordinated by the Office of the Director of National Intelligence in the United States.

10.27 Strategic warning requires strong engagement with government. Warnings can fail if it is not clear to readers that they have been warned. And even a clear warning is of little use unless action is taken in response to it. How to respond to strategic warning is not often straightforward. Large, complex trends or events are hard for Australia to influence. They may require significant, costly changes in policy or capabilities.

10.28 Continuing a regular, annual strategic overview by DGNI to the National Security Committee of Cabinet would help draw the attention of ministers to emerging trends and issues that present risks for Australia. The enhanced national security coordination role we recommend for the Department of the Prime Minister and Cabinet would also support policy agency consideration of NIC warnings.

Recommendation 23: That a cell be established in the Office of National Intelligence to develop warning tradecraft, bolster warning functions and strengthen the NIC-wide warning network.

Recommendation 24: That the Office of National Intelligence produce a National Assessment each year to chart emerging trends likely to threaten Australia's security and prosperity.

Recommendation 25: That the Director-General of National Intelligence continues to provide an annual high-level overview of emerging trends and issues that present risks to Australia to the National Security Committee of Cabinet.

Support for the ADF

10.29 In a conflict, DIO, ASD and the Australian Geospatial-Intelligence Organisation (AGO) will lead intelligence support for military operations and defence planning. But other NIC agencies, including ASIO, the Australian Secret Intelligence Service and ONI, will work closely on some issues with the ADF.

10.30 Demands on ASD would be particularly high in a major crisis or conflict given its broad responsibilities, which include intelligence collection and liaison, offensive cyber operations and cyber security in support of the ADF and broader government. ASD's cyber security role encompasses government systems, critical infrastructure and support for industry, small and medium businesses and the Australian public.

10.31 It would be prudent for government to consider how ASD's multiple roles could best be balanced during a major crisis or conflict. The highest priorities would appear to be strategic-level cyber operations, support for the ADF and protecting critical infrastructure.

Chapter 11. National Intelligence Community investment

11.01 In this chapter, we examine the implementation of major new funding programs for the intelligence community since 2017. This is required by the Review's terms of reference. We also consider National Intelligence Community (NIC) processes for identifying and prioritising investment in new technologies, skills and business systems.

11.02 The programs we consider are complex and there are many risks to their full implementation. But if successful, they will deliver (and in some cases already are delivering) important benefits that support government priorities. It is notable, though, that these new funding proposals were driven largely through individual portfolios. There is scope to improve the ability of government to consider a holistic picture of current and future NIC capability investment requirements. This will help government to better coordinate and prioritise the funding of capability investments in the NIC.

11.03 The case for effective coordination is strong. Funding for the intelligence community has risen steadily in recent years, to $4.5 billion in 2023. Even so, intelligence agencies confront rapid technological change and ever more diverse and sophisticated threats to their ability to work securely and effectively. In an era of tight national budgets and competing priorities, Australian governments will continue to confront difficult decisions about how much to invest in sustaining the community's competitive edge.

Major NIC programs

Status and governance

11.04 Since 2017, a number of NIC agencies have received new funding to modernise the way they work.

11.05 In our Review, we examined five programs that are significant in terms of spending and ambition (see *Box 4*). Each responds in distinct ways to a deteriorating and complex security environment, technological change and government priorities.

11.06 We reviewed the status, governance and delivery risks of each project. In doing so, we drew on existing reporting and analysis, notably reports to government, including Gateway Reviews (a Department of Finance-led process to help Commonwealth agencies successfully deliver major programs). We also spoke to the relevant agencies, to the Treasury and the Department of Finance, and to ministers.

11.07 From our consultations, we judge that all programs are on track, although we note some are still in their early stages. Implementation risks are identified clearly and are being managed.

11.08 In addition to workforce, common risks across all projects include the ability of agencies to hire or develop the program and financial management expertise needed for large, transformational projects. Although not unique to the NIC, the rapid pace of technological change also poses significant risks – potentially rendering major investments obsolete.

11.09 We found all projects have governance boards with an appropriate mix of expertise, including external participation in some instances. And each program has adopted variations of additional subcommittees and subordinate governance structures to more closely manage implementation and risks.

11.10 Given the scale of these projects, agencies will need to continually monitor and adjust their governance mechanisms and implementation and risk management strategies in line with public sector best practice. Closer engagement and information sharing with the Department of Finance is essential, as is early warning for government when a project might be heading off track.

Box 4. Major NIC programs

REDSPICE

Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers, or REDSPICE, was funded in 2022. It provides ASD with $9.9 billion over ten years to deliver new lines of signals intelligence to inform decision makers along with stronger defensive and offensive cyber capabilities.

ASIS Modernisation

In the 2023-24 Budget, ASIS was provided with $468.8 million over four years to modernise the agency.[15]

ASIO Capability Program

In the 2021-22 Budget, ASIO received $1.25 billion over 10 years to strengthen its ability to protect Australia and Australians from threats to Australia's security.[16]

TOP SECRET Cloud

The TOP SECRET Cloud will be purpose-built for Australia's Defence and National Intelligence Community (NIC) agencies to securely host sensitive information. It will improve the NIC's ability to securely share and analyse classified data at speed and at scale, and will help harness leading technologies including artificial intelligence and machine learning.

TOP SECRET-Privileged Access

The TS-PA Vetting Authority capability is led by ASIO and centralises the approach for granting, denying, revoking and maintaining TS-PA security clearances. It will also deliver high assurance standards.

[15] Budget Paper No. 2, 2023-24, p 118.
[16] ASIO Corporate Plan 2022-26, p 21.

Oversight and reporting

11.11 We consider there is scope for agencies to provide government with greater visibility of the progress of major projects, including how funds are being spent and whether projects are delivering the outcomes that were promised.

11.12 In our view, reporting to government on individual projects is adequate. But the community could better survey the implementation of large NIC investments as a whole. A simple solution would be to use regular reporting mechanisms to present a consolidated overview of the status and risks of such programs to government. The five programs described earlier should be included in a consolidated overview. We do not propose to be prescriptive beyond this, but judge ministers will be most interested in a relatively small number of programs that are designed to deliver significant change.

Recommendation 26: That a holistic overview of the status and risks of major NIC programs be presented annually to the National Security Committee of Cabinet.

Coordinating and prioritising NIC investment

11.13 The need for stronger coordination and prioritisation of capability investment across the intelligence community was a feature of the 2017 Review. The Review recommended an intelligence capability investment plan to identify and prioritise major capability projects that agencies wished to commence over the period of the forward estimates, with an indicative total cost.

11.14 This ambitious recommendation was implemented but ultimately proved unworkable due to Australia's system of portfolio government. An additional complication is that funding for some capabilities for the Australian Signals Directorate, even though it is now a statutory authority, continues to be managed through the Department of Defence *Integrated Investment Program*.

11.15 The question arises, then, whether there are options, short of a fully-developed Department of Defence–style integrated investment program, that would give ministers greater visibility of capability investment plans across the intelligence community. The objective of the 2017 Review was to help ministers make informed decisions on the trade-offs between competing priorities. ONI has sought to fill this gap through alternate reporting mechanisms to government. This is a useful process but in our view would benefit from some adjustment. We assess a more detailed forecast of investment plans is possible and should be mandated by government. This can be done without cutting across portfolio responsibilities and would bring current processes closer to the objective of the 2017 Review. Such a forecast should: be comprehensive; sufficiently forward-looking; include detail on each agency's existing and future major capability gaps, along with the consequences such gaps will have on the community's ability to deliver against intelligence requirements; and include indicative costings.

Recommendation 27: That NIC advice to government detail current and future capability gaps and major investment requirements for each NIC agency.

Joint Capability Fund

11.16 The Joint Capability Fund (JCF) is an initiative from the 2017 Review designed to foster inter-agency collaboration, innovation and collective capability uplift and efficiencies. Funding proposals are managed by ONI on behalf of the intelligence community. Enterprise-level funding proposals are approved by Government. Smaller projects may be approved by the Director-General of National Intelligence.

11.17 The JCF is an innovative mechanism that has few parallels elsewhere in government, providing seed funding for new intelligence community capabilities. We heard differing evaluations of the performance of the Fund in our consultations. Challenges in implementing the fund include identifying sufficient projects with a genuinely whole-of-community benefit and insufficiently rigorous evaluation of projects.

11.18 We agree the performance of the JCF has been mixed. Nonetheless, we recognise work by ONI to improve management of the Fund. In our view, the JCF has been an important and flexible source of seed funding for a number of technological and enterprise-wide projects that will be transformative and that address cross-agency needs.

11.19 It is our view that the JCF should be retained. We believe the more recent projects it has supported demonstrate its potential and ongoing importance. We also note that the JCF is the only funding tool available to ONI to help drive greater NIC integration. It is a lever for ONI in a system in which it has considerable enterprise management responsibilities but very little power other than persuasion.

11.20 Narrowing the scope of the JCF so that its use is confined to large scale, enterprise level projects would ensure it remains focused on areas of most benefit to the whole community.

11.21 The JCF would benefit from more robust evaluation. Stronger data on its contribution to capability uplift and innovation would help justify this unique funding model. In particular, we judge that linking the scope and purpose to clearly articulated outcomes and indicators will assist future evaluations.

11.22 In summary, if used well to support NIC modernisation, we believe the JCF continues to have value as a tool of enterprise management and a driver of innovation and integration.

Recommendation 28: That the scope of the Joint Capability Fund be narrowed to focus on delivering key enterprise level capability for the NIC.

Chapter 12. Collective capabilities and shared services

12.01 Sharing administrative services and building more capability, like information and communications technology (ICT) platforms that more than one intelligence agency can use, have been objectives of the National Intelligence Community (NIC), and, indeed, the Australian Public Service as a whole, for some years and have been encouraged by successive governments.

12.02 The rationale is compelling – collective capabilities and shared services can create efficiencies, make scarce dollars go further and promote collaboration. The reality usually proves more complex, as we discuss below. Some welcome progress has been made and some reasonable limits are evident. Still, in our judgement there is scope for further gains to be made.

12.03 The NIC continues to improve its approach to capability and service collaboration. Strategies and principles have been put in place to underpin the community's efforts to build new capabilities in a coordinated way and to minimise wasteful duplication.

12.04 Well coordinated initiatives include the TOP SECRET-Privileged Access Vetting Authority led by the Australian Security Intelligence Organisation, TOP SECRET Cloud and the National Intelligence Academy led by the Office of National Intelligence (ONI). These examples demonstrate the willingness of agencies to make significant investments for collective benefit.

12.05 The barriers to faster and deeper collaboration were also evident in our consultations:

- Operational requirements take priority for busy agencies - it is easy for shared service and collective capability opportunities to go to the back of the administrative queue.
- The post-2017 intelligence community is more diverse in organisational structure and functions. While there are some broadly common operating requirements across agencies, care is needed with the idea that the NIC can easily or simply share capabilities and services just because it is a 'community'.
- Managers may be reluctant to make up-front investments in shared services when the dividends for doing so are not always immediately evident or easy to realise.

12.06 Despite these challenges, agencies have themselves identified new opportunities that could be seized. For example, the TOP SECRET Cloud could allow the community as a whole, or in part, to introduce a common ICT model and more sharing of data and software tools. Common physical security services for some agencies could enhance security outcomes while also realising cost efficiencies.

12.07 In our judgement, the processes for identifying, evaluating and progressing potential initiatives need to be more effective. ONI, as part of its enterprise management responsibilities, should lead this shift in close partnership with all other NIC agencies. The community needs to better:

- explore and evaluate shared service and collective capability opportunities

- prioritise identified opportunities
- ensure senior leaders drive outcomes
- strengthen accountability for failure to take proposals forward.

Recommendation 29: That the NIC adopt a more systematic approach to the identification, evaluation and pursuit of collective capabilities and shared services.

12.08 As a starting point, we suggest the community prioritise evaluation of the new initiatives identified above and which were raised through consultation.

12.09 As initiatives progress, ONI will have an ongoing leadership role to play. But other agencies should lead initiatives where they have relevant expertise and clear advantages.

Chapter 13. Technology

13.01 Perhaps more than any other single factor, the ability of the intelligence community to harness new and emerging technologies will determine how well it keeps pace with a shifting threat landscape, sustains a competitive edge over adversaries and engages with 'big data'. Not surprisingly, therefore, technology was a prominent theme in submissions to this Review and in our consultations. Intelligence, policy, and public stakeholders emphasised the benefits of embracing technological responses to address challenges associated with tradecraft, partnerships, workforce and analysis.

13.02 Adapting new technologies to the needs of intelligence agencies, especially in highly classified environments, is rarely straightforward. And some technologies can advance so quickly that an investment today could be wasted money tomorrow. Other barriers to the use of new technologies in intelligence agencies include shortages of in-house expertise and funding gaps.

13.03 We approach technology as an ecosystem. Activity at both the agency and enterprise level interacts to collectively support the effective delivery of the government's national security intelligence mission. An approach to technology focused on component parts in isolation will fail. The National Intelligence Community (NIC) must manage the interdependencies of its technology-focused work – particularly classified information and communications technology (ICT), data, Artificial Intelligence (AI), and partnering for innovation. This will ensure a stronger, more agile foundation for future technological and capability uplift.

13.04 We pay particular attention to AI as it represents the technology with the most far-reaching implications for the NIC.[17] While it will reshape the threat environment, AI is creating opportunities to enhance agency operations as well as address long-term workforce pressures.

Current approaches

13.05 The NIC uses technology, including in some cases AI, to collect, protect, sort, analyse, translate and disseminate information. New capabilities are employed to support operational tradecraft and to find efficiencies in administration. Intelligence agencies also invest heavily in understanding the potential for emerging technologies to drive security threats.

13.06 The NIC possesses world-class capability and deep subject-matter expertise. But partnerships are also integral to how agencies approach technology. Collaboration and capability sharing with Five Eyes counterparts is strong and vitally important. As highlighted in *Chapter 16*, agencies partner with research centres and industry. Formal and informal forums across the NIC encourage cross-agency collaboration and capability sharing.

13.07 Individual science and innovation hubs also support partnerships and capability development. The Office of National Intelligence's (ONI's) Cyber and Critical Technology

[17] We use AI as a general term for a collection of technologies that enable computers to act in a way that is similar to, or indistinguishable from, the human intelligence and capability required to solve problems and perform tasks. Our use encompasses a range of AI forms, including machine learning and 'deep learning' models such as generative AI.

Intelligence Centre (CCTIC), established in 2022, for example, aims to provide a unified approach to partnerships and innovation across the community.

13.08 The NIC is currently undertaking a range of technology-related projects. In our view, recognising and managing their interdependencies is essential. It is the ecosystem as a whole that will enable the NIC's future operating environment.

The TOP SECRET Cloud

13.09 In July 2024, the Government announced the development of a sovereign TOP SECRET Cloud (TS Cloud) computing environment for the NIC and Defence.

13.10 If successfully deployed, the TS Cloud will represent the largest single leap forward in ICT for the intelligence community in its history, replacing ageing legacy systems with a platform built with cutting-edge private sector knowledge. Importantly, the TS Cloud will provide the processing power needed to support greater use of AI and machine learning, as well as improve the ability to securely share and analyse our nation's most classified data at speed and scale. It will also deliver greater resilience and enable greater interoperability between Australia and Five Eyes partners, some of which are also operating classified cloud environments.[18]

13.11 The NIC does not have to build the TS Cloud, but it does have to manage a transition to it. Where they might not already be doing so, relevant NIC agencies need to begin planning now for this vital stage of the TS Cloud project.

Recommendation 30: That all relevant NIC agencies develop TOP SECRET Cloud transition strategies.

Data

13.12 Robust data is the foundation for good intelligence. It is also a versatile, strategic asset capable of providing insight into the health and efficacy of Australia's intelligence enterprise.

13.13 The NIC collects, holds, and creates a vast array of qualitative and quantitative data. Much of it is highly sensitive, subject to strict statutory controls and, if compromised, could have far-reaching consequences for Australia's strategic interests and foreign relations. But failure to capitalise on opportunities to improve efficiencies and generate collective insights could simultaneously impede the community's ability to effectively serve government.

13.14 The 2017 Independent Intelligence Review (2017 Review) recognised that an individualistic, agency-specific approach to data needed to change. It recommended ONI coordinate data management and ICT connectivity across the NIC and that the community prioritise a shared data analytics and common computing environment. Since then, the NIC has adopted a more strategic and coordinated approach to data and data governance.

[18] Centre for Strategic and International Studies, *Fireside chat with Andrew Shearer*, 4 December 2023. Available at: csis.org/events/fireside-chat-andrew-shearer.

Efforts are focused on making data more discoverable, accessible and useable across the enterprise.

13.15 This coordination is an important first step towards more effective management and exploitation. It will provide the foundation for stronger, more consistent and auditable approaches to data governance and security.

Recommendation 31: That NIC agencies prioritise support to data cataloguing efforts to maximise opportunities for data interoperability.

Artificial intelligence

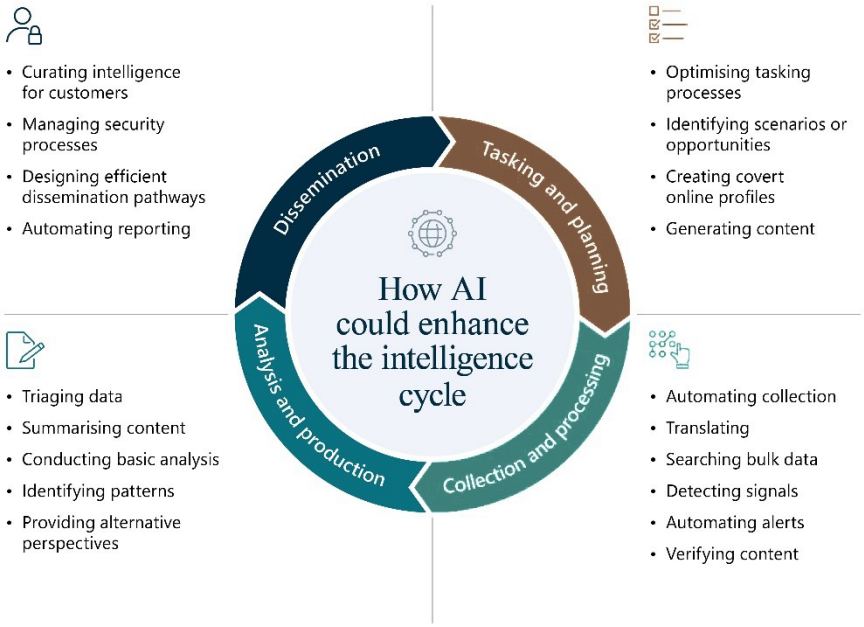
13.16 AI is transforming the domestic and global threat landscape. It is improving the capability and scale of both state and non-state actors. AI technologies are being used to generate realistic deepfake images, videos and sound files in support of politically motivated mis- and disinformation campaigns. AI is also being used to attack other AI models via methods such as data poisoning, model replication or vulnerability exploitation.

13.17 The volume and sophistication of adversary use of AI will only increase as the technology evolves over the next decade. Accelerated cyber attacks, enhanced data harvesting and AI-enabled biotechnology are examples of the future threat landscape. The combination of AI and ubiquitous technical data collection will increase the risk and complexity associated with intelligence collection and operation.

13.18 AI also has the power to transform and improve the intelligence cycle. Discriminative AI, for example, will be able to automate detection and response processes, support resource management and do predictive modelling.[19] Generative AI will be able to create tailored intelligence insights and generate content in support of operations.[20] Increasingly, AI-enabled capabilities will likely be the only effective way to respond to and mitigate the scale and speed of AI-enhanced threats (see *Figure 1*).

[19] Discriminative AI refers to AI models that use conditional logic to categorise existing data.
[20] Generative AI refers to AI models capable of generating new content, including text, images and video.

Figure 1. How AI could enhance the intelligence cycle



Sources:

Centre for strategic and International Studies (2021) *Maintaining the intelligence edge: reimagining and reinventing intelligence through innovation;* ASD (2023) *Ethical artificial intelligence in the Australian Signals Directorate;* GCHQ (n.d.) *Pioneering a new national security: the ethics of artificial intelligence;* GCHQ (2021) *GCHQ to use AI to tackle child sex abuse, disinformation and trafficking,* media release; Patrick; Tucker (2020), Spies like AI: the future of artificial intelligence for the US intelligence community, *Defence One*, 27 January.

13.19 NIC agencies vary in the extent to which they are utilising AI. In the main, AI is being used to augment human capacity for tasks such as translation and the generation of intelligence insights from large or complex data sets.

13.20 A recent Inspector-General of Intelligence and Security (IGIS) inquiry did not identify any legal, propriety or human rights concerns with agencies' current use of AI.[21] Nonetheless, the use of AI tools by companies and governments is already raising significant public concerns in Australia and globally. The public wants assurance that AI will be used ethically and legally. There is apprehension that biases will be introduced into analysis and decision making, depending on the datasets and algorithms used by AI tools. Human involvement in decision making where AI has been involved is essential but may not be sufficient to overcome such biases.

13.21 As intelligence agencies increasingly take up AI of one kind or another, they have a particular obligation to establish rigorous oversight and governance mechanisms, and to ensure staff are appropriately trained.

[21] Inspector-General of Intelligence and Security, *Preliminary inquiry – use of artificial intelligence by Intelligence agencies*, 29 May 2024.

13.22 The intelligence community accepts this obligation. The Australian Signals Directorate (ASD) and the Australian Security Intelligence Organisation (ASIO), for example, have developed and publicly published the principles that underpin the ethical use of AI for intelligence purposes. These include lawful and appropriate use of AI and the primacy of human decision making.

13.23 This is a welcome start. Not all agencies have followed the lead of ASD and ASIO. A common set of ethical AI principles for the whole intelligence community would be an appropriate next step. This should take into account individual agencies' equities, and should be paired with a consistent, community-wide approach to public engagement on the use of AI by intelligence agencies in order to build public confidence. Intelligence agencies will need to do more in the future to show how principles relating to the ethical use of AI are being applied and managed in practice.

Recommendation 32: That the NIC develop intelligence community-wide artificial intelligence governance principles and artificial intelligence public messaging principles.

13.24 To further bolster the governance of AI use in the intelligence community, we make the following recommendations to support agency-level leadership. Our purpose is to encourage NIC leadership to champion stronger uptake of AI along with rigorous governance. We recognise the recommendation on AI training for Senior Executive Service officers is less straightforward to implement in the Department of Home Affairs and the Australian Federal Police. One option would be to apply the recommendation to those areas of each agency that have NIC-related functions.

Recommendation 33: That NIC agencies consider nominating a Senior Executive Service officer to support the development and deployment of artificial intelligence.

Recommendation 34: That all Senior Executive Service officers in the NIC undertake training to better understand the applications, risks and governance requirements of artificial intelligence in the intelligence context.

13.25 Finally, where they have not done so already, intelligence agencies should develop an internal AI governance framework. This would help staff understand their obligations when it comes to AI, reflect relevant policies, legislation and the principles of administrative law, and identify the responsible officer or officers for the use of AI in agencies. AI governance frameworks will need to be living documents.

Recommendation 35: That NIC agencies develop artificial intelligence governance frameworks to support the internal development and deployment of artificial intelligence.

Innovation

13.26 The NIC today has stronger partnerships with the private sector and research institutions than it did at the time of the 2017 Review. The National Security Science Advisory Board, programs operated by Cyber and Critical Technology Intelligence Centre, and innovation hubs in some agencies support this engagement.

13.27 These endeavours help the NIC scan for emerging technologies that could support intelligence functions. They bring intelligence agencies and technology specialists together in ways that are not always possible in public settings.

13.28 Even so, procurement policies, niche technical requirements and classified operating environments can make it harder for agencies to adapt and integrate new technologies. Most leading-edge technologies are developed in other countries – Australia's sovereign technology industry is still developing and engagement is sometimes hampered by secrecy requirements.

13.29 At least some of these barriers could be addressed as part of a broader technology strategy, discussed below. Features of shared ICT, for example, will have implications for how easily newly developed capabilities can be integrated at scale. Similarly, potential subject-matter expertise gaps in the workforce will affect the capacity for in-house innovation and development.

13.30 Nonetheless, we recommend a bolder approach. External partnerships are essential to the community's ability to innovate. Shared capabilities – such as those developed under AUKUS Pillar 2 – represent a cost-effective way to maintain advantage. However, the community needs capacity to develop sovereign capabilities to ensure it can remain resilient and self-reliant in changing strategic circumstances.

13.31 Both the United States and United Kingdom governments have established investment funds to support sovereign technology industries and develop national security capabilities. These funds – In-Q-Tel (IQT) in the United States and the National Security Strategic Investment Fund (NSSIF) in the United Kingdom – operate in somewhat different ways. But both invest in dual-use technologies that may have national security and commercial applications. Areas of NSSIF investment, for example, include digital intelligence, audio and visual processing, biotechnology, space, computing and cyber security.

13.32 There are important differences between the Australian and United States and United Kingdom contexts. Both the United States and United Kingdom funds work with established and diverse private technology industries with deep research and development linkages. These industries have experience collaborating with intelligence agencies and understand their requirements. Australia's sovereign technology industry is smaller in scale and still developing. Dedicated investment could therefore simultaneously support domestic industry growth and national security innovation.

13.33 In our view, if designed well, a national security investment fund could work in Australia and deliver important outcomes, despite the smaller size of Australia's technology sector. This would be particularly so if it focuses on companies developing technology that has both commercial and national security applications. An Australian fund would operate separately to the Joint Capability Fund, which would remain focused on broader capability uplift in specific areas, including those not specific to technology (see *Chapter 11*).

13.34 If agreed, the final design of a national-security-focused investment fund will require broad consultation and consideration. Regardless of structure, like IQT and NSSIF, an Australian fund would deliver a unique commercial and strategic opportunity to invest in critical intelligence capabilities while simultaneously supporting the growth of Australia's technology industry.

Recommendation 36: That government scope the establishment of a national security focused technology investment fund.

Technology strategy

13.35 Intelligence community needs are diverse. Agencies will have, and should be able to pursue, different technology and capability requirements. Even so, in our view the NIC needs a stronger enterprise approach to technology, one that recognises and exploits the interdependencies of the technology ecosystem.

13.36 This can only be achieved if the NIC is working to agreed objectives through a well-designed technology strategy. The NIC needs a technology strategy that:

- defines how the NIC will use technology to deliver its core intelligence mission for government and clarifies the strategic vision for how the ecosystem should operate
- considers the current and future challenges that will affect this goal. Examples of challenges raised with us include: the need to operate at, and across, multiple classifications; adoption and deployment of new technologies at scale in a classified environment; data interoperability; and AI
- prioritises where and how the enterprise will focus resources, including funding, to address the challenges identified
- articulates a process for evaluation and review to enable proactive, enterprise-level management of risks that could impede delivery of technical projects.

Recommendation 37: That the NIC develop a technology strategy to articulate the enterprise-level vision, requirements, priorities, and risks regarding the current and future technological environment.

Regulatory considerations

AI legislation and the intelligence community

13.37 The 2019 Comprehensive Review of intelligence legislation (2019 Comprehensive Review) considered whether legislative controls were needed to govern the use of AI in intelligence agencies. It found that the use of AI capabilities for intelligence purposes had the potential to raise novel legal, policy and ethical issues, and that early use of AI in the intelligence community was evolving organically under laws that were likely not designed with AI in mind.

13.38 The 2019 Comprehensive Review observed that use of AI by intelligence agencies raised a number of potential risks, including the introduction of bias, mistakes made by AI tools at speed and scale, and the possibility that AI tools would reach conclusions or judgements that were not ‘explainable’ – that is, agencies would not be able to understand themselves on what basis such conclusions were reached.

13.39 Ultimately, the 2019 Comprehensive Review concluded that legislation would be premature, favouring instead reliance on institutional mechanisms to ensure that the development of the capabilities of NIC agencies was subject to regular review, including by the IGIS and future independent intelligence reviews.

13.40 As recommended by the 2019 Comprehensive Review, we have considered current use of AI in the intelligence community. In our judgement this has not changed sufficiently since 2019 to warrant legislative oversight specific to intelligence agencies. Broader, nationwide regulatory controls on 'high-risk' AI have, though, been foreshadowed by the Government, and we discuss below the possible implications of this development for NIC.

13.41 We agree that the governance and control of AI use in the intelligence community will require regular future review. We endorse an important role for the IGIS. In addition, we recommend, that at an appropriate time, the Independent National Security Legislation Monitor (INSLM) undertake a review into the legislative dimensions of the NIC's use of AI.

13.42 Finally, while we argue that strong governance and oversight of intelligence agency use of AI is necessary and important, we accept that government must find a balance that does not discourage agencies from taking up AI. This is a mistake Australia cannot afford to make.

Recommendation 38: That the Independent National Security Legislation Monitor undertake a review of the legislative context around the NIC's current use of artificial intelligence to inform legislative and policy changes.

13.43 As noted above, the governance of AI in the intelligence community is just one component of a larger national, indeed global, debate about ethical use of AI. Some of Australia's close partners – for example the United Kingdom – have decided not to legislate national-level obligations or principles at this point. Others, such as the European Union, are doing so. The US has also favoured non-legislative approaches to guide the design, use and deployment of AI. Some states in the United States have introduced legislation to control specific departments' use of AI.

13.44 The Government is exploring options for regulating 'high risk' AI applications, which will provide general guidance for intelligence communities. At the same time, some controls might inadvertently affect the ability of agencies to conduct otherwise lawful intelligence activities. Close consultation with intelligence agencies in the development of nationwide regulatory responses to AI is essential.

Technology and privacy

13.45 The nature and capability of the NIC's technological ecosystem could have broader implications for privacy. Intelligence agencies hold, or have access to, a range of information including, where appropriate, personally identifiable information (PII) of Australian citizens. Some public submissions expressed concern about the NIC's use of PII. The Law Council of Australia, for example, raised privacy concerns around intelligence agencies' use of bulk personal datasets – particularly where the majority of individuals whose information is captured by the datasets are not of interest to the agency.[22] Others

[22] Law Council of Australia submission, p 16.

highlighted government's responsibility to ensure adequate measures are in place to protect this information in the event of a data breach.[23]

13.46 Similarly, the 2019 Comprehensive Review raised the potential for capability to progress to a point where agencies could begin 'detecting' or 'discovering' criminal or security-relevant activities. Such activity would also likely lead to public concerns about privacy, particularly with regards to reference information.[24]

13.47 There is no legislation in Australia that expressly and holistically regulates the use of reference information. However, NIC agencies' ability to obtain and use reference information is regulated to some extent by the *Privacy Act 1988* or by agencies' privacy rules, as well as legislative controls applying to specific datasets.[25] In light of public concerns, the 2019 Comprehensive Review recommended that future independent intelligence reviews examine whether additional statutory controls were needed to safeguard the collection, retention and use of reference information.

13.48 We judge there is currently no need for additional statutory controls on the use of reference information by NIC agencies. The intelligence community uses reference information to quickly answer basic intelligence questions such as a person's name, their address, or vehicle information. In our view, there has been no substantive change to either the nature of the data or the way that NIC agencies are collecting, using, retaining or destroying reference information since 2019.

13.49 We note that some agencies have yet to implement recommendations 139 and 140 from the 2019 Comprehensive Review, which relate to updating the ASIO guidelines and the privacy rules for the Australian Secret Intelligence Service, Australian Signals Directorate, the Australian Geospatial-Intelligence Organisation, ONI, the Defence Intelligence Organisation and the Australian Criminal Intelligence Commission to better articulate how reference information is used. We heard that, in some cases, this was because the *Intelligence Services Act 2001* (IS Act) application of privacy rules does not include agencies' use of reference information. We agree with the intent of recommendations 139 and 140, which supported greater transparency, and so recommend the IS Act be amended to enable this.

Recommendation 39: That the *Intelligence Services Act 2001* be updated to expand the application of agency privacy rules to include reference information.

13.50 In the future, AI will change the way agencies use data – including, but not limited to, Australian PII. In addition to bolstering traditional methods of investigation and operations, AI could support greater data integration and search capability across the intelligence enterprise.

[23] CPSU submission, p 2; Olivia Shen submission, supplementary material, *Walking the talk on citizen data*, p 2; United States Studies Centre submission, pp 7, 11.
[24] The 2019 Comprehensive Review defined reference information as a set of information that 'agencies obtain or retain for the purposes of assisting the performance of their intelligence functions, generally, rather than for the purpose of a specific investigation, operation or matter'. Reference information contains personal information that identifies, or could reasonable identify, a person; for example, name, address, credit card information, photographs or internet protocol address.

13.51 We acknowledge moving to more proactive use of NIC data raises complex legal, privacy and potentially human rights concerns. One agency told us that current legislation when it comes to using AI to search across its data holdings to identify new links or leads was unclear. Combining multiple datasets, some which include reference information, could have a mosaic effect. Where a single dataset might contain minimally intrusive information, in combination they could reveal potentially sensitive information about a person's identity, location or affiliations. Respecting the privacy of Australians must remain one of the community's highest priorities.

13.52 It is our view that NIC agencies should be able to utilise data in new or enhanced ways. The technology is now at a point where this is possible. It is therefore important that these complexities be considered now to ensure government and public expectations of privacy for Australians are maintained.

Recommendation 40: That the Attorney-General's Department consider what, if any, regulation would be required to enable NIC agencies to combine and interrogate multiple datasets (including reference information) for the purposes of proactively identifying criminal and national security concerns.

Chapter 14. Insight and advantage through open source

14.01 Australia's decision-making advantages will rest more and more on the intelligence community's ability to quickly gain actionable and accurate insight from open source intelligence – also known as OSINT.

14.02 We judge the foundations to achieve this are present. Through its OSINT leadership of the community, the Office of National Intelligence (ONI) has supported other agencies to establish their own open source capabilities. Nonetheless, given the pace and scale of change, stronger collective action is required to help intelligence agencies future-proof OSINT as an intelligence specialisation.

14.03 We also assess the National Intelligence Community (NIC) needs to invest more in its ability to deal with misinformation and disinformation.

The OSINT landscape

14.04 Today's online environment is awash with data that offers a unique intelligence advantage. OSINT is no longer merely the collection and analysis of news media and public-facing websites. The OSINT revolution now encompasses social media, satellite and other geospatial imagery, and the growth of commercial entities collecting and aggregating vast amounts of data for purchase.

14.05 A simple web search will only reveal some of what is potentially on offer. While the information landscape continues to expand and evolve at rapid speed, new technologies and tradecraft are required to exploit it for intelligence advantage.

14.06 In some areas, civilian OSINT investigators, think tanks and commercial providers are pacesetters. These groups are expertly navigating the contours of the increasingly complex information landscape to derive intelligence insights by leveraging artificial intelligence and machine learning technologies (see *Box 5*).

14.07 Technology can also obfuscate. Generative AI is creating more sophisticated, harder to detect disinformation. As generative AI technology continues to rapidly advance – and other technologies are developed over time – these tools will increase disinformation and pollute data in unprecedented ways.

14.08 Open societies are only just beginning to grapple with this increasingly grave challenge. Disinformation can, for example, incite violence, spark communal unrest, manipulate political systems and corrode democracy. Disinformation makes getting to the truth of things quickly much harder for intelligence agencies.

Implications for the NIC

14.09 OSINT is a vital collection pathway. It enables other covert collection, investigative and operational activity within the intelligence community. It also informs all source assessment and delivers unique standalone intelligence insight at a low classification. In a crisis, open

source information, backed by analytical expertise, can help governments make sense of fast-moving events even in the absence of classified intelligence.

14.10 The imperative for the intelligence community to fully harness OSINT is more acute than ever. Government expects its intelligence community to provide accurate, actionable and timely insights to inform its decision making. Translating open source data into intelligence insight is a critical component.

14.11 Other countries are making significant investments in the open source domain. To compete, the intelligence community must have an integrated and agile approach to OSINT. As the *United States Intelligence Community Data Strategy 2023–2025* observes:

> *Strategic competition is no longer just about the volume of data, it is about who can collect, access and gain actionable insight the fastest, as they will have the decision and intelligence advantage.*

14.12 The foundations to achieve this exist. ONI plays an important functional leadership role to ensure intelligence agencies are able to build open source capabilities to service their missions.

14.13 This 'functional leadership' role is consistent with ONI's broader leadership role of the NIC. Since the 2017 Review, ONI has focused on adding value with respect to common challenges and opportunities, for example, by coordinating the delivery of open source training for the community and providing leadership on governance issues.

14.14 The 'federated model' importantly recognises the production of OSINT is not a generic process. To have impact, OSINT needs to be tailored to different problem sets and to different decision makers. Tactical OSINT to identify leads for covert collection is entirely different to strategic OSINT to inform an all source intelligence assessment. Decentralising the 'doing' of OSINT so that it is housed within each agency enables the efficient and effective production of insights to serve respective missions.

Delivering capability

Enhanced functional leadership

14.15 We judge ONI's functional leadership of a decentralised OSINT ecosystem across the NIC to be the right model for the community. It is clear from our consultations that intelligence agencies derive benefit from ONI's advice, guidance and advocacy on open source governance and training to help support their own OSINT missions.

14.16 But we also judge more needs to be done to uplift the NIC's capability on OSINT, particularly noting the speed at which the online environment is changing. This uplift is needed to bring all agencies to the same level of ability in terms of leveraging private expertise, technology and access to data, and also to set up the community collectively to innovate and ensure adequate protections are in place.

14.17 The increasing volume and diversity of data coupled with greater use of technology to derive insight will mean that intelligence agencies will also need to take greater care to ensure the proportionality and legality of their OSINT activities. Consultations suggest that agencies are cognisant of this reality and are taking steps to ensure adequate governance

and policies are in place specific to their contexts. Still, in our view ensuring adequate protections for the rights of Australians will become more complex as the information landscape evolves. We note that in the United States, important policy work has recently been undertaken in response to the rise of commercially available information to ensure the community can maximise the intelligence value of these datasets while also protecting the privacy and civil liberties of citizens.[26] We judge similar work will need to take place in Australia.

14.18 Ensuring the safe and secure collection of OSINT so that Australia's most sensitive intelligence priorities remain protected from adversaries will also require dedicated effort. While rapidly evolving technologies offer the community an intelligence advantage if harnessed, they also provide similar opportunities to adversaries. This includes improved adversary capabilities to detect and analyse the digital footprints of competitors to reveal their secrets. Strong leadership is needed to ensure all NIC agencies are cognisant of risks and are equipped to minimise risk and harm.

14.19 ONI must, in our view, be postured to provide leadership in the following key areas:

- drive a collective approach to the adoption of cutting-edge technology, including to safeguard secrets
- identify and pursue new ways for the NIC to partner with OSINT expertise in industry, think tanks and academia
- coordinate the acquisition of open source datasets of common value and enable sharing where possible
- provide expert governance advice to ensure proportionality and legality while protecting the rights of Australians
- innovate to improve OSINT tradecraft
- undertake horizon scanning to future-proof OSINT capabilities and to ensure that legislative settings keep pace with the evolving information environment.

14.20 There is scope for ONI to build on its current endeavours to deliver a more integrated OSINT community of practice across the NIC.

Recommendation 41: That the NIC's federated approach to open source intelligence under the functional leadership of the Office of National Intelligence continue. The Office of National Intelligence's leadership role be strengthened by additional investment in the skills and capabilities needed to build an integrated community of practice.

A dedicated open source intelligence agency?

14.21 We carefully considered other models for lifting the NIC's open source capabilities, including a dedicated open source intelligence agency sitting within the NIC. An argument put to us in favour of a new agency was that it would accelerate the transition to best-

[26] Office of the Director of National Intelligence, *Intelligence community policy framework for commercially available information,* 2024.

practice use of open source, including because it could operate without the constraints of secrecy.

14.22 Nonetheless, for several reasons, we judge that at this time the disadvantages of a new OSINT agency outweigh any possible benefits. First, OSINT requirements are too diverse and too discrete to be serviced effectively and efficiently by a centralised entity, so a new enterprise could not replace individual agency-level efforts. Second, open source analysis has little value for government if it is simply repackaged news – some value-add is required. This does not necessarily have to come from classified intelligence but it must at least come from subject-matter expertise. This would be expensive to build at a time of scarce resources and would duplicate ONI's analytical teams. Third, a new agency inevitably would introduce a competitive dynamic between open source analysis and classified all-source analysis from ONI and the Defence Intelligence Organisation (DIO). In our view, this is unlikely to be productive or helpful to ministers, especially if such analysis produces competing judgements. Finally, the establishment of a new OSINT agency would need to be carefully weighed against the competing budget priorities of the government of the day.

14.23 The approach we recommend is consistent with the way in which the United States intelligence community organises its own open source efforts under the functional leadership of the Central Intelligence Agency's Open Source Enterprise. The *IC OSINT Strategy 2024–2026* offers a similar call to action for the United States intelligence community to ensure it can fully harness the potential of open source.

14.24 Building advanced OSINT capabilities must be a first order priority for the NIC. Set and forget approaches will be overwhelmed by the pace of change in the open source information landscape. Full implementation of the changes recommended in this report is essential, along with regular reviews of their effectiveness. And a further holistic review by the next independent intelligence review would be timely and appropriate.

Recommendation 42: That the next independent intelligence review consider how open source intelligence functions are best organised across the intelligence community to ensure optimal intelligence outcomes for government.

Increased disinformation expertise

14.25 Given the large volume of information to draw upon in open source when a crisis occurs, there is potential for adversaries to exploit situations by using misinformation and disinformation. Determining the veracity of publicly available information is crucial to ensure government is given the best possible information to make a decision, particularly in a rapidly evolving crisis.

14.26 Misinformation and disinformation are becoming increasingly sophisticated and harder to detect. Coverage of the Israel–Gaza conflict has highlighted this trend. For example, the aftermath of a blast at the Al-Ahli Hospital in Gaza on 17 October 2023 led to different 'authoritative' claims as to who was at fault. Civilian OSINT experts, journalists and think tanks played an important role in using their disinformation tradecraft to inform judgements regarding the veracity of claims.

14.27 As the scale and complexity of misinformation and disinformation continues to grow, expertise to identify it quickly will become essential. We have provided separate advice to government on these matters.

Partnerships

14.28 The intelligence community must always have the ability to produce its own OSINT. This is critical to ensuring that the most sensitive intelligence requirements are protected through specialised OSINT collection practices and safeguarded by infrastructure designed to minimise the digital footprint of intelligence agencies.

14.29 However, by sheer necessity, the NIC's efforts need to be augmented by the capabilities and expertise of the commercial sector.

14.30 The volume of publicly available data means it is not possible for one entity – be it an intelligence agency or a think tank – to have the expertise, technology and bandwidth to derive insight from it all. Knowing when to harness the analytical insights of others not only creates efficiencies, it also results in better intelligence. Engagement with the private sector is essential to ensuring the NIC's in-house OSINT capabilities are supported by the most up-to-date technology and tradecraft. The growth of commercially available information – that is, publicly available data that is collected, aggregated and sold by one commercial entity to a third party – means that NIC agencies will require the services of others to fully exploit OSINT's potential.

14.31 We welcome current agency-level engagement with the private sector to enhance their OSINT efforts. It is important this is well coordinated across the intelligence community and carefully designed to maximise collective advantage – particularly regarding technology and data acquisition.

Open source and covert collection

14.32 The 2019 Comprehensive Review of intelligence legislation (2019 Comprehensive Review) recommended future independent intelligence reviews consider the roles of ONI, DIO and the Department of Home Affairs in collecting open source information. The 2019 Comprehensive Review was concerned to ensure the boundary between open source and covert collection was not being crossed. We judge there is currently no requirement for assessment or policy agencies to use covert techniques to maintain platform legitimacy when collecting open source information. However, this may change within the next few years given the pace and scale of change in the online environment. The NIC will need to navigate the governance and legislative complexities which may arise as a result.

Box 5. Russia–Ukraine OSINT case study[27]

Researchers at the Turing Institute's Centre for Emerging Technology and Security collated examples of OSINT activity in the lead-up to and during the early months of the Russia–Ukraine conflict. These include:

- Private investigators analysed commercial imagery to track the build-up of Russian military forces before the invasion was officially announced.
- The Ukrainian military used Instagram and TikTok video content to identify the location of Chechen forces it sought to target.
- A private-sector OSINT provider used machine-augmented tools to identify Kremlin-aligned communities on Telegram and VKontakte who were engaged in a systemic campaign to damage perceptions of Ukrainian refugees across Europe.

[27] Turing Institute, Centre for Emerging Technology and Security, *Artificial intelligence, OSINT and Russia's information landscape – expert analysis*, February 2023. Available at https://cetas.turing.ac.uk/publications/artificial-intelligence-osint-and-russias-information-landscape.

Chapter 15. Collective action on people and skills

15.01 A highly skilled and committed workforce is one of the National Intelligence Community's (NIC) greatest assets. Sustaining this advantage is no easy task. Still, any erosion of the community's attractiveness as an employer will weaken its ability to manage the high demands of the era, those present and those clearly evident on the horizon. This is especially so given the growth trajectories of some agencies.

15.02 In a tight national labour market, the NIC is not alone in having to work hard at recruitment and retention. But the intelligence profession poses some unique challenges, especially in meeting the interests of younger workers. These include the need to work for the most part in secure locations, long lead times for security clearances, and the dominance of Canberra-based jobs. These factors reduce options for job flexibility and mobility, including working from home.

15.03 Nor are intelligence jobs for everyone. NIC employees confront the sobering, hard-edged realities of today's world, whether the risk of great-power war, terrorism, serious and organised crime, or espionage and foreign interference. The stakes are high.

15.04 One of the enterprise management functions envisaged for the Office of National Intelligence (ONI) in the 2017 Review was responsibility for a strategic approach to the NIC's workforce. Since then, ONI has led a number of workforce initiatives on behalf of the NIC and the intelligence community is working hard to adapt to new workforce realities. Agencies are recruiting in different and innovative ways. Multi-classification offices allow work to be done at lower security clearance levels. The TOP SECRET-Privileged Access (TS-PA) Vetting Authority will, over time, provide a central clearance authority for all TS-PA security clearances.

15.05 These initiatives are welcome and delivering results. They can be reinforced through stronger collective action by the NIC on workforce analysis and planning, recruitment and retention to complement individual agency strategies.

Attraction and retention

15.06 Intelligence agencies are using new and innovative approaches to recruit their employees, often with considerable success (see *Box 6*). Even so, NIC recruitment and retention face some specific and growing challenges, among which are:

- a widening gap between the employment benefits the NIC can offer and those offered by the broader Australian Public Service (APS)
- improving, but still below average, workforce diversity
- a lack of data on workforce trends
- a mixed record on encouraging mobility within the NIC
- a competitive national employment market for some skill sets.

Box 6.The Australian Signals Directorate's approach to workforce growth

ASD is undertaking a number of recruitment activities to grow its workforce including:

- raising the profile of ASD through public engagement, including media and public-speaking appearances
- expanding multi-classification facilities so that staff can work in the organisation while waiting for higher-level security clearances
- streamlining recruitment processes to speed up the path from application to employment
- supporting skills-based training programs, including research and university programs, partnerships with TAFEs and relevant industry workforce initiatives
- new learning and development programs, more flexible and family-friendly work arrangements and a payment framework to recognise essential skills.

Employment offering

15.07 The widening gap on employment offerings is a difficult challenge for the intelligence community.

15.08 As a point of comparison, enterprise bargaining in the broader APS in 2023 secured the right for all APS employees to request work-from-home arrangements with no caps and a requirement for managers to 'bias' towards supporting staff requests. Proponents of the changes argued they were necessary to increase attraction and retention of staff across the service.

15.09 Intelligence agencies working primarily at lower classifications can offer hybrid work arrangements not so dissimilar from those of the wider APS and in the private sector. For many agencies, however, work at the PROTECTED level or below is the exception rather than the norm.

15.10 It was put to us during our consultations that, where this is the case, increased or additional allowances could help with recruitment and retention. In our view, new workplace realities mean there is a reasonable case for looking at allowance structures in the NIC. This would need to be done on a community basis and in conjunction with the Australian Public Service Commission (APSC). Some NIC agencies already offer service allowances and the rates at which these are applied vary considerably. While individual agencies might benefit, it is not in the NIC's interest as a community to have these disparities widen further. A common increase would be preferable but not necessarily easy to implement given differences in work and work practices across the NIC.

15.11 Agencies are innovating elsewhere, for example by strengthening in-house capabilities and targeting talent earlier in the pipeline, including for STEM jobs. ASD has a cadetship program that includes analyst, cyber, data and technologist streams. The Defence Intelligence Organisation has a similar STEM recruitment stream.

15.12 Several recommendations in this Review are broadly relevant to ICT and STEM recruitment. These include: enhanced brand identity for the NIC highlighting its unique value proposition; efficiencies to clearance processes; the potential growth of the

community into larger labour markets via an enhanced presence outside Canberra; and increased private–public talent exchanges for knowledge and capability sharing.

Promoting the NIC value proposition

15.13 Younger workers, particularly Generation Z (born 1997–2012), often want more than a good salary and a flexible workplace. Some will also consider the culture and purpose of their employer.

15.14 There is good evidence that organisations with strong employee value propositions (EVPs) can significantly reduce staff turnover – so long as they reflect lived experience in the workplace rather than an aspiration.[28] The NIC's mission to support Australia's ongoing security and prosperity should be an attractive proposition for individuals wanting to contribute to national goals. A NIC-wide EVP could therefore help raise the profile of the intelligence community and appeal to younger employees wanting work with a strong purpose. To have full effect, a NIC-specific EVP would need to be well designed and prominent in community advertising and branding. This would complement – not replace – individual agency brands and the APS employee value proposition.

Recommendation 43: That a NIC-wide employee value proposition be developed to inform branding and recruitment campaigns.

Diversity

15.15 A more diverse NIC workforce will attract more employees. The business case is strong and now well established – diversity improves organisational performance.

15.16 NIC leaders are committed to a workforce that reflects the modern face of Australia. ONI leads diversity initiatives on behalf of the community, among which are NIC diversity priorities and articulating shared commitments towards First Nations peoples, women, and culturally and linguistically diverse (CALD) groups. Many individual agencies also have their own diversity initiatives and staff-led networks, including in support of LGBTIQA+ and neurodivergent staff.

15.17 Diversity representation across all recorded categories has improved since the 2017 Review. Notably, at the time of this Review, five of the 10 agency heads are women (the first time this has been achieved). Despite this, the community continues to lag somewhat behind the rest of the APS, particularly in the overall rate of female representation.

15.18 Publishing aggregated diversity statistics from across the community in the public domain would increase transparency and accountability, while providing an opportunity to engage prospective employees. We heard support for this in public submissions.[29] In line with APSC diversity principles, where possible, this should account for representation in leadership roles and diverse job families, not just raw representation percentages. This is an important measure of inclusion.

[28] Gartner, 'Employee value proposition', *HR insights*. Available at: https://www.gartner.com/en/human-resources/insights/employee-engagement-performance/employee-value-proposition.
[29] Yun Jiang submission; Elise Stephenson and Susan Harris Rimmer, Global Institute for Women's Leadership and Griffith University Law Futures Centre submission.

Recommendation 44: That the Office of National Intelligence publish aggregated NIC diversity statistics and gender pay gap data annually.

Separation

15.19 Some turnover is inevitable and healthy. But separation in the NIC can have an outsized impact compared to other workplaces. Shortened tenure can diminish the return on costly on-boarding investment, creating additional burden in the vetting pipeline. And some specialised intelligence roles have long lead times to competency, including in-house training requirements.

15.20 The risk for intelligence agencies if separation rates become too high is a constant drain on the skills and hard-won experience that are especially important at times of high threat and crisis. Quality can be affected when too many experienced employees leave, and so too can workplace culture. This is particularly the case for those intelligence job families that are not readily available in the job market. Leaders need to plan for a period of vulnerability as new staff are brought up to speed.

15.21 In our judgement the NIC would benefit from more consistent, centralised workforce data collection to analyse which skills are being lost, where shortages might be anticipated and to understand workforce sentiment. A shared exit survey process and standardised staff surveys, could better illuminate workforce trends and inform workforce planning. Our consultations with several large Australian companies reinforced the importance of rigorous data in workforce planning.

15.22 The capability review process we recommend in *Chapter 6* is an additional opportunity to consider organisational culture and the role it plays in recruitment, retention and diversity.

Recommendation 45: That the Office of National Intelligence work with NIC agencies to develop a more consistent approach to data collection on NIC workforce trends.

Mobility

15.23 Mobility in the broader public service is now encouraged and regarded as an important component of developing public service professions. Broad experience in government is an asset. It allows employees to develop new skills, expand networks and improve their understanding of the APS. And it is valued for promotion to the Senior Executive Service.

15.24 NIC leaders accept the principle, but worry about losing staff with rare skills even to other intelligence agencies. They are conscious of higher than average recruitment costs and lead times. They understandably want return on the investment in a new officer, particularly where a Positive Vetting clearance is involved.

15.25 While we sympathise with these concerns, we are not convinced limiting movement within the NIC is healthy. Younger generations will move more – this is the case for all workplaces. And there are advantages to retaining experienced and cleared staff within the NIC rather than losing them from the community entirely given recruiting costs and times.

15.26 Encouraging mobility within the community won't on its own stop people leaving. But in our view, a formal mobility scheme could provide opportunity for NIC officers while also allowing agencies to plan for periods of extended absence.

15.27 We also consider there are broad benefits to greater cross-community experience. This provides opportunities for individual professional growth. At the enterprise level, experience in other NIC agencies may help strengthen a culture of collaboration at leadership level. As an example, in the United States, with some limited exceptions, experience in more than one United States intelligence agency via a 'Joint Duty' program is a general condition of promotion to senior executive.[30]

15.28 Linking talent management to mobility opportunities could have some advantage in both retaining and attracting talent. Facilitated opportunities for high performers to move around the NIC could be an attractive proposition and enhance the NIC's appeal as a prospective employer.

Recommendation 46: That the Office of National Intelligence lead the development of a program to support intra-community mobility.

Clearances

15.29 Robust security clearance and psychological testing processes are essential to the integrity and performance of the intelligence community. It is clear from our consultations they also still weigh on the NIC's ability to recruit efficiently and quickly. They can also act as a barrier to mobility within the NIC.

15.30 As we discuss in *Chapter 6*, the shift from a federated vetting model to the TS-PA capability, comprising the TS-PA Vetting Authority in the Australian Security Intelligence Organisation (ASIO) and the Quality Assurance Office in ONI, will create efficiencies through scalable delivery and improve workforce mobility over the long term. We recognise the importance of this initiative and strongly urge government to commit the necessary resources to ensure the success of the new model.

Recommendation 47: That adequate investment and resources be provided for the TOP SECRET-Privileged Access Vetting Authority to achieve a single high-assurance vetting standard, enable staff mobility in the NIC and harden the community against compromise.

15.31 It may be possible over time to achieve efficiencies in the clearance process. Each clearance – Negative Vetting 1, Negative Vetting 2, Positive Vetting and TS-PA – is currently a discrete process within both the TS-PA Vetting Authority and Australian Government Security Vetting Agency (AGSVA), with access to prior records or assessments sometimes limited. There is scope to better leverage records from Negative Vetting 1 or Negative Vetting 2 clearances that may already be held.

[30] Office of the Director National Intelligence, *Joint Duty - FAQs*, www.dni.gov/careers/joint-duty/faqs.

15.32 There are technical barriers to integrating these approaches. And for the time being, the new TS-PA capability must be the priority. Still, as the TS-PA Vetting Authority evolves and as AGSVA digitises more processes, we assess there is opportunity for optimisation.

Recommendation 48: That security clearance processes at different levels be optimised via a phased approach, leveraging efficiencies from the TOP SECRET-Privileged Access Capability.

Organisational suitability assessments

15.33 Organisational suitability assessments (OSAs) and psychological testing allow agencies to make informed decisions about a candidate's capability and fitness to work in an intelligence environment. Done early, this reduces the risk of investing in a costly vetting process only to find an employee not suitable.

15.34 Individual agency OSAs can, however, be a barrier to intra-NIC mobility, slowing down recruitment and career advancement. We commend recent efforts by some intelligence agencies to harmonise processes. Taking further steps down the harmonisation path will complement the design of the TS-PA security clearance as a single standard to be recognised across the NIC.

Recommendation 49: That NIC agencies utilising organisational suitability assessments continue to identify opportunities to harmonise processes to facilitate intra-community mobility, including leveraging of TOP SECRET-Privileged Access clearances.

Talent management, leadership and culture

15.35 The APS is progressively improving its mechanisms for talent management and succession planning. The goal is a consistent, transparent approach to developing high performing officers and to 'build strong and diverse pipelines for leadership and other critical roles.'[31]

15.36 The NIC has access to senior leadership talent management programs led by the APSC, and we understand that most agencies use these programs, albeit to varying extents. We propose all NIC agencies regularly put their leaders through the assessment processes for talent management programs.

15.37 APSC-led succession planning for potential agency heads is currently limited to ONI. It would be good practice to extend this process to all NIC agencies, to support the development of a larger pool of future intelligence community leaders. That some NIC agencies are not part of the APS should not be a barrier to succession planning. Similarly, leadership skills should be considered in NIC selection processes as much as they are now for senior roles in the APS.

15.38 We understand government is considering extending the APS values to include all agencies covered by the *Public Governance, Performance and Accountability Act 2013*. This would

[31] APSC, *APS Talent management programs and initiatives*. Available at: www.apsc.gov.au/initiatives-and-programs/aps-talent-management.

include those parts of the NIC not covered by the *Australian Public Service Act 1999*.[32] We support this proposal. Connecting all NIC agencies to a broader set of values will reinforce expectations in relation to standards of conduct and behaviour. The high level nature of the values means they can be applied while recognising the unique work of NIC agencies.

Recommendation 50: That current leaders and staff with potential to become future leaders in the NIC be identified, independently assessed and nurtured via Australian Public Service Commission talent programs.

Recommendation 51: That, in consultation with secretaries and agency heads, a regular succession scan for NIC agency leadership be commenced as part of the Australian Public Service–wide enterprise succession scans led by the Secretaries Talent Council.

Training

15.39 Collective training in the intelligence community is improving. The National Intelligence Academy (NIA), established in 2022, builds on the former National Centre for Intelligence Training and Education to accommodate the changing needs of the NIC. The NIA offers a combination of self-paced e-learning modules and courses (both virtual and face to face). Many are offered in partnership with contractors such as the Australian National University's National Security College and the Australian Strategic Policy Institute.

15.40 While the NIA won't and can't provide all the training needs of the community, there are clear benefits in a central NIC training function. Shared foundational training is valuable to generate common standards and platforms for analytical tradecraft. This includes collective understanding of the history and culture of the intelligence community as well as methodology.

15.41 In our judgement, the NIA is an asset for intelligence agencies and the broader national security community and should be supported with appropriate funding. With new investment the NIA could increase its offerings to foster greater understanding in the policy community of intelligence and its uses.

Recommendation 52: That the National Intelligence Academy continue in existence and be funded accordingly.

A Chief People Officer

15.42 To lead the cross-NIC initiatives outlined in this section, we recommend the establishment of a NIC Chief People Officer (CPO) as a central senior coordinator. This initiative will place people – as they should be – at the centre of NIC enterprise strategic planning and decision making.

[32] APS Reform, *APS Reform outcomes and initiatives – Stage 2*. Available at: https://www.apsreform.gov.au/about-aps-reform/our-focus-areas-stage-2.

15.43 The CPO function would not encroach on individual agency decision making or workforce planning but would facilitate the programs that run across the whole of the NIC, including work in support of branding, mobility and data collection. They would be responsible for anticipating strategic trends likely to impact the community's workforce – such as skills shortages – and working with the community to respond accordingly.

15.44 We suggest the CPO should sit in ONI, be a senior, highly experienced human resources professional, and have regular access to NIC agency heads and senior leadership. The position should build linkages with relevant APS forums and best-practice organisations outside of government. A NIC CPO should be supported by a small team.

Recommendation 53: That a NIC Chief People Officer be established in the Office of National Intelligence.

Chapter 16. Partnerships

16.01 The threats targeting Australia are complex and global in nature. Australia cannot effectively meet them on its own. Strong partnerships are an essential national asset.

16.02 Partnerships are force-multipliers for the National Intelligence Community (NIC) – creating opportunities to enhance capability, intelligence insights and strategic warning. Similarly, in many cases, NIC intelligence can help partners respond to, and mitigate, threats directly. Healthy partnerships are built on two-way collaboration and information sharing.

16.03 Here we consider domestic partnerships, such as with state and territory governments, the research sector and Australian industry, as well as international partnerships with foreign governments and their intelligence, military and law enforcement agencies.

Domestic partners

16.04 A more diverse and complex body of security challenges is driving more frequent and better coordinated NIC engagement with domestic partners. This is both welcome and essential – Australia's industry and research sectors and state and territory governments sit at the centre of many challenges to national security and prosperity. Critical infrastructure, defence capability, and critical and emerging technologies are all subject to a range of security threats including cyber attacks, foreign interference, intellectual property theft and espionage, and physical threats from sabotage and terrorism. Domestic partners want and need advice from intelligence agencies to manage these threats and build resilience.

16.05 There will always be limits to the ability of agencies to share intelligence insights at an unclassified level. Even so, the NIC's domestic partners want more than just broad messaging around security risks. Based on our discussions, deeper, reciprocal engagement on threat and response options will support domestic partners to manage national security issues.

States and territories

16.06 Since the 2017 Review, the NIC has worked with Commonwealth policy agencies to provide more regular and structured advice for state and territory partners on the threat environment. For example, intelligence agency leaders brief senior state and territory government representatives through the Department of the Prime Minister and Cabinet–led First Secretaries Group.

16.07 Australia needs efficient communication between its intelligence enterprise and states and territories. In many situations, the roles are complementary. The NIC's subject-matter expertise and unique capabilities can enhance state and territory partners' responses to threats occurring within their jurisdictions. Similarly, these partners provide unrivalled local knowledge and alternative sources of information to inform the broader threat picture. Such collaboration is particularly important in the context of preparedness.

16.08 The number of complex of national security issues demanding close cooperation between state and territory governments and the Commonwealth will only grow, including in relation to preparedness for, and resilience in the face of, a major crisis or conflict. While this is a

matter for state governments, we would observe that maintaining a strong cadre of state and territory officials with high-level security clearances is part of an essential broader national adjustment to a world in which Australia is managing diverse security risks.

Research sector

16.09 The security of Australia's research sector has long-term implications for the nation's interests. Government research and university partners confront cyber attacks, foreign interference and espionage targeting sovereign research. Research entities and universities use intelligence from the NIC to inform policies on international engagement and collaboration, improve situational awareness and mitigate threats.

16.10 The research sector also possesses data and expertise that is beneficial to the NIC. This includes information related to cyber and foreign interference incidents detected on their networks and premises. Collaboration with the research sector can assist agencies to solve hard problems and innovate. The Australian Signals Directorate (ASD) and the Australian Federal Police, for example, have established formal relationships with universities to collaborate on priority issues. The Office of National Intelligence (ONI)-led National Intelligence and Security Discovery Research Program has funded national security- and intelligence-focused research projects.

16.11 While NIC outreach is welcomed, some research partners we consulted would like more support to respond to cyber and foreign interference threats. Classification of information and the cost and availability of secure infrastructure impose some barriers. Some research centres sought tailored intelligence at lower classifications.

16.12 One research institution proposed the establishment of a due-diligence centre to support better integration between the NIC and the university sector on foreign interference and related matters. Canada, for example, has a Research Security Centre that provides tailored advice and guidance to the research sector.

16.13 This is a model Australia may wish to adopt in the future. In the meantime, we recognise the importance of NIC support for the work of the University Foreign Interference Taskforce housed within the Department of Home Affairs. We also judge that more proactive and regular outreach and, where relevant, consultation between agencies and the research sector could improve engagement on this issue and invite greater information sharing.

Private industry

16.14 Like the research sector, private industry represents a force-multiplier for the NIC. It is also an increasingly important vector in mitigating and neutralising threats at the source.

16.15 Several private sector entities told us they most frequently engaged with the ASD's Australian Cyber Security Centre (ACSC), ASIO and ONI. Those with long-term relationships with agencies, and more regular access to Sensitive Compartmented Information Facilities, reported greater and deeper information sharing. Those with less established relationships would welcome more detailed advice to support risk-focused decision making.

16.16 The desire for a reciprocal relationship was particularly strong in the context of cyber security. While some partners described strong relationships with ASD's ACSC, others felt

they would benefit from timelier advice and more actionable data. Who does what in the cyber system, especially the respective roles and responsibilities of the ASD's ACSC and the National Cyber Security Coordinator within the Department of Home Affairs, remains unclear to some. We note the coordinator function is relatively new, but more could be done to clarify how the various functions can assist industry and citizens.

16.17 We see value in the NIC and its research and industry partners gaining greater exposure to each other's ways of working. An industry partner said 'there needs to be more cross-pollination of people between the NIC and the private sector'. We agree and therefore recommend that greater flows of people between the NIC and industry via a private–public talent exchange would help strengthen engagement between sectors.

Recommendation 54: That the NIC establish a public–private talent exchange to deepen partnerships with private industry through knowledge and capability sharing.

International partners

16.18 The Five Eyes arrangement remains the cornerstone of the intelligence community's international partnerships. Through these relationships, Australia has access to intelligence and cutting-edge tradecraft and technology. Five Eyes partnerships also provide warning of threats and support intelligence operations. But these relationships are not one-sided – the NIC is a respected partner and contributes unique intelligence and operational capability, especially in our near region.

16.19 Australia's intelligence relationships within the Five Eyes continue to deepen in response to changing strategic circumstances. The Combined Intelligence Centre – Australia, for example, was established in the Defence Intelligence Organisation in mid-2023 to produce intelligence on strategic issues relating to the Indo-Pacific.

16.20 The NIC works with partners well beyond the Five Eyes community. Partnerships across the Asia Pacific and Europe, for example, remain vital to Australia's capability to understand Indo-Pacific geopolitical trends, to support Australian diplomacy, and to counter terrorism and transnational and serious organised crime.

16.21 We heard many examples of operational engagement resulting in successful security outcomes, including by law enforcement and criminal intelligence agencies. This should continue as these partnerships strengthen the NIC's ability to generate national security outcomes.

Chapter 17. Legislation

17.01 Australia's intelligence agencies operate in accordance with a considered and comprehensive legislative framework. This framework establishes a careful balance, simultaneously promoting the collective right to security and protecting individual freedoms. It empowers agencies to perform their functions, including by conducting activities that would otherwise be unlawful, while ensuring agencies are accountable for their conduct and operate within the rule of law.

17.02 The community's legislative framework is premised on well-established foundational principles, including distinctions between foreign and security intelligence, onshore and offshore activities, and the collection of intelligence on Australians and non-Australians. These distinctions were first enunciated by Justice Hope and continue to underpin the design of intelligence legislation, as outlined in *Chapter 5*.

17.03 The 2019 Comprehensive Review of intelligence legislation (2019 Comprehensive Review) provides a relatively recent deep dive into the legislation governing the intelligence community. Many of its recommendations are currently being, or have only recently been, implemented. As such, we have primarily confined our consideration of legislation to matters raised in submissions to our Review. We consider below the need to progress holistic electronic surveillance reform as well as several targeted legislative amendments proposed by agencies.

Electronic surveillance reform

17.04 The centrepiece recommendation of the 2019 Comprehensive Review was that Australia's electronic surveillance laws be repealed and replaced with a single new Act.[33] The 2019 Comprehensive Review made a further 57 recommendations concerning the design of this new electronic surveillance framework.[34]

17.05 The 2019 Comprehensive Review found Australia's electronic surveillance framework to be 'highly inconsistent', based on 'outdated technological assumptions' and 'complex to the point of being opaque'.[35]

17.06 Government commenced work on the electronic surveillance reform project in July 2021. This is a major reform, involving complex policy, legal and technological issues, as the 2019 Comprehensive Review itself acknowledged. The reforms must be given due consideration and undergo extensive consultation. Still, several agencies and oversight bodies submitted to our Review that the need for a new Act was becoming more urgent. Some agencies argued that the issues identified by the 2019 Comprehensive Review are posing increasing operational challenges.

17.07 We agree that developments in communications technology will make the technological assumptions underpinning the current framework increasingly outdated.

[33] 2019 Comprehensive Review, recommendation 75.
[34] 2019 Comprehensive Review, recommendations 76–132.
[35] 2019 Comprehensive Review, Volume 3, [26.68]–[26.71].

17.08 For example, developments in communications technology, including since 2019, mean there are a broader range of entities involved in the delivery of telecommunications services. The role played by these entities could not have been contemplated when the current legislative framework was being developed and it is not always clear what electronic surveillance obligations apply to them.

17.09 This is just one example of the increasing challenges in applying Australia's electronic surveillance laws to modern communications technologies that need addressing through holistic electronic surveillance reform.

Recommendation 55: That the 2019 Comprehensive Review of intelligence legislation's recommendation for holistic electronic surveillance reform be implemented as a matter of priority.

Recommendation 56: That, as part of the electronic surveillance reform project, government revise the range of communications providers subject to electronic surveillance obligations in order to provide clarity and better reflect the entities involved in the modern telecommunications system.

Urgent electronic surveillance amendments relating to groups

17.10 ASIO submitted that some urgent amendments to electronic surveillance legislation are required in advance of holistic reform. Specifically, ASIO argued that it is increasingly urgent to implement the 2019 Comprehensive Review's recommendation that agencies be permitted to obtain warrants in relation to a group of actors. The review heard convincing evidence to support this change on national security grounds.

17.11 Under the *Telecommunications (Interception and Access) Act 1979* (TIA Act), security intelligence warrants to intercept communications can only be issued in relation to a particular telecommunications service or, if that would be ineffective, a particular named person.[36] Similarly, warrants to access data on computers in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) must be issued in relation to a particular computer, a computer on a particular premises, or a computer associated with a particular person.[37]

17.12 As a general rule, amendments to electronic surveillance legislation made in advance of holistic reform should be as targeted as possible to address immediate operational challenges. Such amendments should be consistent with the commentary, principles and recommendations of the 2019 Comprehensive Review. The 2019 Comprehensive Review recommended that group warrants only be available where the common activities of the group would justify the issue of a warrant and it would be 'impractical or ineffective' for an agency to obtain a warrant in relation to individual members of the group.[38] These safeguards, as a minimum, should be included in the proposed urgent amendments.

[36] TIA Act, ss 9, 9A.
[37] ASIO Act, s 25A(2) and (3).
[38] 2019 Comprehensive Review, recommendation 83.

Recommendation 57: That the *Telecommunications (Interception and Access) Act 1979* and *Australian Security Intelligence Organisation Act 1979* be amended urgently, and in advance of holistic electronic surveillance reform if necessary, to enable the Australian Security Intelligence Organisation to obtain interception and computer access warrants against particular groups. If progressed ahead of holistic reform, it would be appropriate that these amendments implement relevant safeguards recommended by the 2019 Comprehensive Review of intelligence legislation.

Other legislative changes

17.13 Several agencies argued for various targeted legislative amendments. These requests can be grouped into two categories:

- those that sought legislative change to provider greater operational flexibility in light of changes in the strategic environment
- those relating to agency requirements in a conflict or a period of intense grey-zone activity.

17.14 Though we do not detail them in this Review, in our view, some of these proposals lacked sufficient justification. However, there were several proposals that we consider warrant legislative amendments or further exploration. These are considered below.

17.15 We sought to impose a relatively high evidentiary bar for legislative proposals. We were willing to support proposals for legislative change only where agencies could provide considerable legal and operational justification, supported by case studies and data where relevant.

Legislative change to provide greater operational flexibility in light of changes in the strategic environment

17.16 Several agencies submitted that the strategic environment has changed such that existing legislative settings are not fit for purpose. These submissions related to a diverse range of legislative provisions, considered in turn below.

Definition of 'foreign power' for the purposes of the *Intelligence Services Act 2001*

17.17 Agencies with foreign intelligence mandates must obtain a ministerial authorisation to produce intelligence on an Australian person.[39] One of the grounds for which foreign intelligence agencies can obtain a ministerial authorisation is that the Australian person is acting for, or on behalf of, a 'foreign power'.[40] 'Foreign power' is defined to include 'an entity that is directed or controlled by a foreign government'.[41]

17.18 There is nothing in the IS Act that expressly states that a company must be *formally* or *legally* controlled or directed by a foreign government. It is possible that indirect control or direction may be sufficient. However, the absence of formal or legal control or direction will often make it very difficult to establish that a company is subject to control or direction.

[39] *Intelligence Services Act 2001* (IS Act), ss 8 and 9.
[40] IS Act, s 9(1A)(a)(ii).
[41] IS Act, s 3 (which provides that 'foreign power' has the same meaning as in the ASIO Act); ASIO Act, s 4.

Perhaps more significantly, it is clear that the definition requires actual control or direction. Influence or obligation, however strong, is unlikely to be sufficient.

17.19 The *Criminal Code Act 1995* (Criminal Code) provides a legislative precedent for a broader understanding of foreign government control of a company. The definition of 'foreign public enterprise' in the Criminal Code, used in relation to various espionage offences, contemplates various ways in which a foreign government may exercise control or influence. Most notably, it contemplates that a company's directors may be 'accustomed or under an obligation (whether formal or informal) to act in accordance with the directions, instructions or wishes' of the foreign government.[42]

17.20 We do not believe that the definition of foreign power in the IS Act excludes companies that are effectively, but not formally, controlled by a foreign government. However, the definition does exclude companies that are obliged to act in accordance with the instructions of a foreign government in circumstances that fall short of control or direction. We assess that there is no clear justification for the different treatment of these companies.

17.21 In light of the above, we consider there is a case for amending the IS Act to enable intelligence agencies with foreign intelligence mandates to obtain intelligence on Australians working for companies that are not controlled by a foreign government, but that are subject to influence or an obligation to act on that government's behalf. We consider this could be achieved by amending the IS Act to reflect the broader range of companies that fall within the definition of 'foreign public enterprise' in the Criminal Code.

Recommendation 58: That the *Intelligence Services Act 2001* be amended to enable NIC agencies to obtain ministerial authorisations in relation to Australians working for a broader range of companies that are acting on behalf of a foreign government, but that are not subject to actual control or direction. This could be done by adopting the definition of 'foreign public enterprise' in the *Criminal Code Act 1995*.

Legislative implications of changing onshore foreign intelligence activities

17.22 An agency proposed numerous other targeted legislative amendments that it assessed were required because of changes in the technological and strategic environment. We assess that many of these legislative challenges raised by this agency flow from the same underlying cause: the increasing need for some foreign intelligence activities to be conducted within Australia. We received case studies establishing a compelling case for certain foreign intelligence activities to be conducted onshore. Those case studies also demonstrated that this shift raises complex legal and policy issues. However, we do not propose to individually address the legislative issues raised by the agency with this Review. Instead, we consider that the legislative settings for increasing foreign intelligence activities within Australia should be the product of holistic consideration by government.

17.23 Intelligence agencies with foreign mandates have limited powers and immunities within Australia. Those agencies are not prohibited from collecting foreign intelligence onshore. But they have no general immunity from criminal or civil liability in Australia.[43] In addition,

[42] Criminal Code, s 70.1 (definition of *foreign public enterprise*).
[43] The staff and agents of ASIS, ASD and AGO are immune from criminal and civil liability for activities conducted onshore that are preparatory to, in support of, or otherwise directly connected to offshore activities (IS Act, s 14(2)). Staff and agents of ASIS, ASD and

intelligence agencies with foreign mandates are not able to obtain warrants authorising otherwise unlawful activities within Australia. Instead, foreign intelligence warrants are issued by the Attorney-General to ASIO.[44] This contrasts with the broad immunity from civil and criminal liability that applies to staff members and agents of intelligence agencies with foreign mandates for acts done outside Australia.[45]

17.24 These legislative settings reflect the foundational distinction between onshore and offshore activities, discussed earlier in this Review. This distinction was first outlined by Justice Hope, who stressed that the ability to break Australian laws, including for the purpose of obtaining foreign intelligence, should be available only under warrant issued to ASIO and authorised by the Attorney-General. We assess that this distinction remains sound and, as the 2019 Comprehensive Review outlined, enhances the consistency, accountability and control of covert and intrusive intelligence activities conducted onshore.

17.25 Nevertheless, we accept that there are increasing operational imperatives for certain foreign intelligence activities to be conducted onshore. Noting that there is no prohibition on intelligence agencies with foreign mandates acting onshore, we consider that this trend is not necessarily inconsistent with the principle underlying the distinction between onshore and offshore foreign intelligence. But changes in the volume and nature of those operations may require some reconsideration of the way in which that distinction is reflected in the legislation.

17.26 It is important that government consider this issue holistically. Though the immediate operational challenges could be addressed through piecemeal amendments, we anticipate similar challenges will continue to arise in the future. More importantly, the legislative settings for foreign intelligence operations within Australia should reflect a considered analysis of those agencies' role onshore rather than an ad hoc reaction to specific legislative barriers. As such, we recommend that the government review the appropriate legislative settings for the conduct of certain foreign intelligence activities onshore, having regard to the principles underlying the foundational distinction between onshore and offshore collection of foreign intelligence.

Recommendation 59: That government review the appropriate legislative settings for foreign intelligence requirements onshore, having regard to the principles underlying the foundational distinction between onshore and offshore collection of foreign intelligence.

Limited-use provisions

17.27 We heard during our Review that Australian companies increasingly are concerned that information provided to the Australian Signals Directorate (ASD) on major cyber breaches will be used against them in regulatory action. This limits the ability of ASD to respond to such incidents. In response, government has proposed the creation of a 'limited-use obligation'. This would mean that information provided to ASD relating to a cyber incident could be used only for a limited set of cyber security–related purposes, to be defined in

AGO are also immune from civil and criminal liability for conduct undertaken onshore or offshore on the reasonable belief that it is likely to cause a computer-related act, event, circumstance or result to take place outside Australia (Criminal Code, s 476.6).

[44] See ASIO Act, s 27A; TIA Act, ss 11A–11C.

[45] IS Act, s 14(1).

legislation. There appears to be broad support, particularly from industry, for a limited-use obligation.[46]

17.28 We agree that a limited-use obligation of the kind proposed by government would be a useful mechanism to encourage industry to disclose information and to assist ASD in the performance of its cyber security functions.

Disclosing ASIO information to ONI

17.29 ASIO submitted that current information sharing provisions in the ASIO Act prevent it from effectively sharing certain information with ONI for the purposes of ONI's strategic assessment function.

17.30 There are provisions that would allow ASIO to disclose information to ONI on a targeted basis.[47] However, these narrow sharing provisions contrast with the broad powers for ASIO to share information with ASIS, ASD and AGO,[48] as well as powers to share information when assisting or cooperating with law enforcement agencies and the Department of Defence.[49] There is no similar ability to share information for the performance of ONI's functions, even when ASIO is formally assisting or cooperating with ONI under the ASIO Act. There is no indication in the explanatory material for relevant provisions as to why ONI is treated differently from other agencies. Nor can we identify a clear principle justifying this different treatment.

17.31 We agree that expanding ASIO's ability to share information with ONI would be of significant benefit to ONI's assessments function. It is clear that information ASIO could share would likely include material relating to matters of political, strategic or economic significance to Australia.

17.32 This proposal would require amendments to the ASIO Act to enable ASIO to share information with ONI where relevant to the performance of ONI's functions. It would likely also require amendments to the TIA Act. It would be appropriate for amendments to the TIA Act to be progressed as part of holistic electronic surveillance reform.

17.33 It would also require ONI to establish controls and compliance mechanisms to appropriately restrict access to, and use of, this information and to ensure that irrelevant information is not retained.

[46] See e.g. Amazon Web Services, *Australian Cyber Security Strategy: legislative reforms, Amazon Web Services submission*, p 4; Business Council of Australia, *Australian Cyber Security Strategy: legislative reforms*, March 2024, p 6; Optus, *Response to government consultation paper: Cyber Security Strategy legislative reforms*, March 2024, [14]–[15].
[47] For example, ASIO could share such information if it were in the national interest (ASIO Act, s 18(3)). See also TIA Act, ss 64(2) and 65.
[48] ASIO Act, s 184A.
[49] ASIO Act, s 19A(4) (see also *Australian Security Intelligence Organisation Regulation 2016*, reg 6, which prescribes the Department of Defence as a department with which ASIO can cooperate).

Recommendation 60: That the *Telecommunications (Interception and Access) Act 1979* and the *Australian Security Intelligence Organisation Act 1979* be amended to enable the Australian Security Intelligence Organisation to share raw foreign intelligence information with the Office of National Intelligence.

Agency requirements in a conflict or a period of intense grey-zone activity

17.34 The question of whether or not Australia's intelligence laws would allow agencies to meet government requirements effectively in a conflict or major military crisis was a theme during our consultations. Agencies identified a number of potential legislative obstacles arising under various Acts.

17.35 To identify all potential legislative barriers in a conflict situation would be a substantial undertaking that is beyond the scope of this Review. We also recognise that complex legal issues are involved and that, even in a conflict, governments must be mindful of the appropriate limits of legislative power for intelligence agencies.

17.36 Nonetheless, in line with our other recommendations on preparedness, we recommend these issues be considered now. We propose a body of work to identify legislative barriers and consider potential mitigations in advance of any potential conflict.

Recommendation 61: That relevant policy agencies, in consultation with NIC agencies, lead a body of work to identify whether there are legislative barriers that may prevent the intelligence community from effectively responding to a conflict. Consideration is to be given to what legislative reform may be required in advance of, and in the event of, conflict.

Chapter 18. Oversight

18.01 Effective oversight sustains public and government confidence in Australia's intelligence community. A strong oversight architecture ensures that the intelligence community acts with integrity and in strict compliance with the law. It provides public assurance that agencies are accountable for their actions. Oversight is a necessary counterpart to the strong covert powers vested in agencies.

18.02 Australia's oversight architecture contains numerous independent specialist bodies that collectively oversee a broad range of matters, from the legality and propriety of agency activities through to the effectiveness and proportionality of the intelligence legislative framework. This includes the Inspector-General of Intelligence and Security (IGIS), the Commonwealth Ombudsman (the Ombudsman), the Independent National Security Monitor (INSLM), the Parliamentary Joint Committee on Intelligence and Security (PJCIS), the Parliamentary Joint Committee on Law Enforcement, the Independent Reviewer of Adverse Security Assessments, the Auditor-General and the National Anti-Corruption Commission.

18.03 The IGIS is a notable feature of the Australian oversight model. It has a broad jurisdiction and strong compulsory information-gathering powers. The Australian oversight model vests these strong, intrusive powers in the IGIS rather than a parliamentary committee. The work of the IGIS helps hold agencies accountable to their responsible ministers.

18.04 In our view, this model remains fit for purpose. Australia's oversight architecture and institutions are strong. We see no evidence of any failure of oversight. We endorse the judgements of the 2017 Review and the 2019 Comprehensive Review of intelligence legislation (2019 Comprehensive Review) that Australia's oversight architecture is sound and fulfils the characteristics of effective oversight. These characteristics include the existence of numerous oversight bodies that are independent, have clear mandates and powers, and collectively provide comprehensive oversight of agencies' activities, administration and legislative frameworks.

18.05 There have been a range of changes to the operation of Australia's oversight system since the 2017 Review and the 2019 Comprehensive Review.[50] In this chapter, we confine ourselves to three thematic issues where change has introduced complexity or where we consider additional reform is warranted – the operation of the Intelligence Services Legislation Amendment Bill 2023 (ISLAB), powers and information sharing, and resourcing.

The jurisdiction of the IGIS and PJCIS – Intelligence Services Legislation Amendment Bill 2023

18.06 ISLAB was introduced to Parliament on 22 June 2023 and is currently subject to review by the PJCIS. The Bill includes a range of oversight-related amendments.

18.07 Most significantly, ISLAB expands the jurisdiction of the IGIS and PJCIS to the entire intelligence community. This would mean the IGIS and PJCIS would oversee the Australian Criminal Intelligence Commission (ACIC) and the intelligence functions of the Australian

[50] This includes amendments to the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act), the creation of the National Anti-Corruption Commission and the appointment of the first full-time Independent National Security Legislation Monitor.

Federal Police (AFP), the Department of Home Affairs (Home Affairs) and the Australian Transaction Reports and Analysis Centre (AUSTRAC), in addition to the six 'Australian Intelligence Community' agencies that already fall under the jurisdiction of the IGIS and PJCIS.[51]

18.08 The 2017 Review and the 2019 Comprehensive Review partially disagreed on this matter. The 2017 Review considered the IGIS should oversee the entire intelligence community, with oversight of the AFP, ACIC and Home Affairs limited to their intelligence functions.[52] In contrast, the 2019 Comprehensive Review recommended that the IGIS and PJCIS not oversee the AFP or Home Affairs.[53] The 2019 Comprehensive Review considered there was no gap in the oversight of these agencies and that their intelligence functions significantly differed from the intelligence functions of other agencies that the IGIS oversees. Both reviews agreed that the IGIS and PJCIS should oversee AUSTRAC and the ACIC.

18.09 The explanatory material relating to ISLAB does not explain why the 2017 Review's approach concerning the AFP and Home Affairs was preferred by government. However, there are benefits to providing the IGIS with oversight of the intelligence functions of the entire community. This would give the IGIS holistic oversight of all intelligence functions and provide consistent oversight of intelligence activities.

18.10 Nonetheless, the change embedded in ISLAB does introduce some complexities and potential inconsistencies. Submissions to our Review, for example, noted the following:

- Particularly in relation to the AFP, the integration of law enforcement and intelligence functions means the boundaries between the oversight responsibilities of the IGIS and the Ombudsman could be unclear.
- Currently, the majority of the ACIC's covert, intrusive and coercive powers have the same thresholds and can be used for the same purposes as the powers used for the law enforcement functions of the AFP. There is a risk of inconsistency in oversight given that the IGIS will oversee the former while the Ombudsman will oversee the latter.
- Government proposes to take a 'structural approach' to defining oversight of Home Affairs by providing the IGIS with oversight of Home Affairs' Intelligence Division.[54] There is a risk that this approach could cause oversight gaps.

18.11 Though there is weight to the concerns raised in submissions and by the 2019 Comprehensive Review, the challenges with this approach are not insurmountable. They can be overcome through effective cooperation and coordination between the IGIS and the Ombudsman.

18.12 It is too early to properly evaluate the effectiveness of the proposed changes to the oversight framework. It will be important for the next independent intelligence review to consider the effectiveness and consistency of these arrangements.

[51] The IGIS and PJCIS currently have some oversight of specific AFP and ACIC powers, such as their use of network activity warrants in the *Surveillance Devices Act 2004* (SD Act) (see IGIS Act, ss 3 (definition of *intelligence function*), 8(3A)).
[52] 2017 Review, recommendation 21 and [7.18]–[7.21].
[53] 2019 Comprehensive Review, recommendation 168.
[54] Attorney-General's Department, *Submission to the PJCIS Review of the Intelligence Services Legislation Bill 2023,* August 2023, p 15.

Recommendation 62: That, subject to Parliament's consideration of relevant legislation, the next independent intelligence review consider the effectiveness of expanding the oversight jurisdiction of the Inspector-General of Intelligence and Security and the Parliamentary Joint Committee on Intelligence and Security to include the Australian Criminal Intelligence Commission and the intelligence functions of the Australian Federal Police, Department of Home Affairs and Australian Transaction Reports and Analysis Centre.

18.13 Recent and proposed legislative amendments have sought to improve cooperation between oversight bodies. Given the importance of effective cooperation and coordination to the oversight framework created by ISLAB, we consider more could be done to support the IGIS and Ombudsman to work together.

18.14 The Ombudsman's oversight of the use of various covert, intrusive and coercive powers by agencies is limited to considering the legality of agency activities.[55] The Ombudsman has limited capacity to consider broader issues of propriety or proportionality. In contrast, the IGIS has a broad remit to oversee the legality *and propriety* of the activities of agencies under its jurisdiction.

18.15 The Ombudsman's limited remit in relation to these powers makes it difficult for the Ombudsman to advise agencies on best practice and to support agencies to identify the root causes of non-compliance. The differences between the IGIS's and the Ombudsman's remits may also limit their ability to share information[56] and coordinate oversight of cross-cutting issues relating to the propriety of agency activities.

18.16 As such, we consider the Ombudsman should be empowered to oversee matters going to propriety or proportionality in the use of covert, intrusive and coercive powers for the law enforcement functions of the AFP, Home Affairs and AUSTRAC. This would generally enhance the Ombudsman's oversight of these agencies and would improve coordination and cooperation with the IGIS.

18.17 In considering this change, we have had regard to existing oversight mechanisms applying to these agencies. We assess that expanding the Ombudsman's remit as recommended would not result in duplicative oversight.

Recommendation 63: That the Commonwealth Ombudsman be empowered to oversee the propriety and proportionality of the use of covert, intrusive and coercive powers by the Australian Federal Police, Department of Home Affairs and Australian Transaction Reports and Analysis Centre.

[55] For example, in its oversight of controlled operations under Part IAB of the *Crimes Act 1914* and various warrants and authorisations in the SD Act and the TIA Act, the Ombudsman's oversight is limited to periodically inspecting agency records to ascertain compliance with certain legislative provisions.
[56] Section 32AF of the IGIS Act enables the IGIS to disclose information to the Ombudsman only if the information is relevant to the Ombudsman's functions.

Proposed changes to oversight powers, information sharing and resourcing

Changes to oversight bodies' powers and information sharing

18.18 For the most part, we assess that oversight bodies' legislative functions and powers are sufficient and appropriate. However, some oversight bodies raised discrete legislative issues that we consider should be addressed. In particular:

- there are limitations on the INSLM's ability to commence own-motion reviews
- the Auditor-General is not able to share some confidential performance audit reports with the PJCIS.

18.19 These matters are considered further below. We received other submissions proposing amendments to components of the oversight architecture. Having regard to the strength of Australia's oversight system and the range of recent amendments to oversight legislation, we were not convinced that broader changes were required.

The INSLM's own-motion remit

18.20 The *Independent National Security Monitor Act 2010* (INSLM Act) includes a defined list of 'counter-terrorism and national security legislation' in relation to which the INSLM can conduct an own-motion inquiry.[57] The list excludes much of the legislation governing intelligence agencies' functions, powers and duties, such as the *Australian Security Intelligence Organisation Act 1979*,[58] the *Intelligence Services Act 2001* (IS Act), the *Office of National Intelligence Act 2018*, the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997*, the *Surveillance Devices Act 2004*,[59] the *Australian Crime Commission Act 2002* and the *Australian Federal Police Act 1979*.

18.21 The INSLM's own-motion remit was designed to focus on specific terrorism-related laws enacted after 11 September 2001. This was modelled on the United Kingdom Independent Reviewer of Terrorism. Notably, the United Kingdom Independent Reviewer has recently been given additional scope to review certain secrecy, espionage and foreign interference offences.[60]

18.22 The INSLM's own-motion remit is an important element of its independence. It provides the INSLM with discretion to conduct the reviews that it, rather than government, identifies as a matter of priority for oversight. Having regard to the importance of this function, the range of relevant intelligence legislation excluded from the INSLM's remit because of the passage of time, the changes to the United Kingdom Independent Reviewer's role, and the greater capacity of the current INSLM as a full-time appointee, we consider the INSLM's own-motion jurisdiction should be updated. The INSLM Act should be amended to enable the INSLM to conduct own-motion inquiries into the full range of contemporary legislation

[57] *Independent National Security Monitor Act 2010*, ss 4 (definition of *counter-terrorism and national security legislation*), 6(1)(a).
[58] With the exception of those parts dealing with ASIO's compulsory questioning powers.
[59] With the exception of the powers introduced by the *Surveillance Legislation (Identify and Disrupt) Act 2021,* which must be reviewed within three years after that Act received royal assent.
[60] National Security Act 2023 (UK), ss 63–64.

relevant to counterterrorism and national security, including the core legislation governing the community.

Recommendation 64: That the *Independent National Security Legislation Monitor Act 2010* be amended to ensure the Independent National Security Legislation Monitor is able to conduct own-motion inquiries into any Commonwealth legislation relating to counterterrorism or national security. At a minimum, this should include the IS Act, the entirety of the ASIO Act, the ONI Act and provisions relating to intelligence agency powers in the TIA Act, Telecommunications Act and SD Act.

PJCIS access to confidential Auditor-General reports

18.23 In its 2020–21 review of intelligence agencies' administration and expenditure, the PJCIS recommended that government amend the *Auditor-General Act 1997* (Auditor-General Act) and the IS Act for the purpose of improving information sharing between the Auditor-General and the PJCIS.[61] The Government's response to that recommendation noted that the matter would be reconsidered following our Review.

18.24 The PJCIS's recommendation has two limbs, which we consider separately.

18.25 The first limb seeks to encourage the Auditor-General to conduct performance audits of intelligence agencies by creating a mechanism for the Auditor-General to table classified reports confidentially in the PJCIS. The Auditor-General can and does conduct financial statement and performance audits of intelligence agencies. In that context, it is not clear that the mechanism proposed by the PJCIS is necessary to encourage audits of the community.

18.26 The second limb is a more limited amendment that would enable classified reports relating to the intelligence community to be disclosed to the PJCIS. This is not possible under current legislation[62] and in our view limits the reasonable interrogation by the PJCIS of intelligence community administration and expenditure.

18.27 The PJCIS's recommendation is closely related to a recommendation of the Joint Committee of Public Accounts and Audit (JCPAA). The JCPAA previously recommended that the JCPAA be able to receive confidential Auditor-General reports.[63] Given the JCPAA's various statutory responsibilities relating to the Auditor-General,[64] it would be unusual if confidential Auditor-General reports could be provided only to the PJCIS and not to the JCPAA. As such, any amendments to enable the disclosure of confidential Auditor-General reports to the PJCIS should be considered alongside the broader reform recommendations made by the JCPAA.

[61] PJCIS, *Review of Administration and Expenditure No. 20 (2020–2021) – Australian Intelligence Agencies,* June 2023, recommendation 1.
[62] See *Auditor-General Act 1997*, s 37.
[63] Joint Committee of Public Accounts and Audit, *Report 491 – Review of the Auditor-General Act 1997,* March 2022, recommendation 7.
[64] For example, the JCPAA is required to review all reports tabled in parliament and to report to parliament on its deliberations *(Public Accounts and Audit Committee Act 1951,* ss 8(1)(c) and (d)).

Recommendation 65: That, in the context of broader reform to the *Auditor-General Act 1997*, government consider amending the Act to enable confidential information relating to an agency overseen by the Parliamentary Joint Committee on Intelligence and Security to be disclosed to the committee.

Oversight resourcing

Oversight implications of intelligence agencies' funding proposals

18.28 Having regard to additional funding for oversight provided in the 2023–24 Budget, and subject to our later comments about PJCIS staffing, we assess resourcing for oversight bodies is adequate.

18.29 For the IGIS, this additional funding will increase its staffing level. We assess this increase is likely to be sufficient. But the IGIS will continue to face challenges in recruiting to fill these additional positions and retaining staff.

18.30 Though we do not assess additional oversight funding is required, it is notable that several recent large investment proposals from the intelligence community failed to take account of downstream implications, most notably for oversight bodies but also for other stakeholders such as policy departments. For example, a department submitted to this review that several recent funding proposals which significantly increased agency powers and workforce did not include any funding for relevant oversight bodies.

18.31 It would be best practice for agencies to consider possible oversight imposts and consult oversight bodies, the Attorney-General's Department and other relevant policy departments early in the development of funding proposals. This will allow government to consider the downstream effects of large new intelligence community investments on Australia's oversight system and on the ability of policy departments to absorb and effectively use new lines of intelligence.

Support to the PJCIS

18.32 Like other parliamentary committees, the PJCIS is supported by a secretariat staffed by parliamentary service employees. Unlike other parliamentary committees, there are limits on the extent to which committee members' electorate or personal staff can assist with PJCIS-related functions.

18.33 The IS Act contains secrecy offences limiting how certain information obtained, held or made by the PJCIS can be used.[65] These provisions are underpinned by written agreements between the PJCIS and intelligence agencies about the use of such information. The practical effect of the legislation and related agreements is that large amounts of PJCIS-related information can be disclosed to, and used by, PJCIS members and secretariat staff only.

18.34 The PJCIS has a substantial workload. That workload will increase after the passage of ISLAB. There is nothing to suggest the PJCIS secretariat does not provide strong support to the PJCIS. The PJCIS secretariat has also been allocated additional funding in the

[65] See particularly IS Act, Schedule 1, cl 9, 12 and 22.

2023–24 Budget to support its expanded functions under ISLAB. However, it is notable that PJCIS members are not able to use personal staff to supplement support from the secretariat, and that the chair and deputy chair of the PJCIS carry additional workloads in relation to the drafting and finalisation of reports.

18.35 In our view, there is a strong case for additional support for the chair and deputy chair of the committee. We have considered several models to achieve this, including further resourcing for the secretariat and a role for personal political staff. In our view, the former will not achieve the direct support the committee is looking for and the latter raises significant legislative and administrative issues, including in relation to the sharing of committee information.

18.36 A simpler solution would be to allocate an additional staff member each to the chair and the deputy chair of the PJCIS, with these roles to be filled by positively vetted intelligence agency or public service officers. This option would provide the chair and deputy chair with staff in their personal offices, ideally with a professional intelligence background. The sole function of these staff members would be to support the chair and deputy chair in the performance of PJCIS functions.

18.37 This option would require changes to the written arrangements between agency heads and the PJCIS to enable the secondees to access and use PJCIS information. The secondees would also require access to appropriate facilities in Parliament House to draft, store and handle highly classified information.

18.38 Finally, we note that the secrecy offence in the IS Act only binds members of the PJCIS and 'members of staff' of the PJCIS, which is not defined. There is some risk that the secondees may not be bound by the secrecy offence if they are not considered 'members of staff'.

18.39 It is likely that this risk could be reduced through the drafting of the secondees' employment arrangements. For example, those arrangements could specify that the secondees are employed to perform duties as members of staff of the PJCIS and for the sole purpose of assisting the chair and deputy chair with their PJCIS duties. The risk may be reduced further if secondees were employed as part of the parliamentary service and sat within the PJCIS secretariat. However, we consider this option would be less effective in providing the direct support that the committee seeks.

Recommendation 66: That the chair and the deputy chair of the Parliamentary Joint Committee on Intelligence and Security be allocated an additional staff member each to assist in the performance of their functions. These roles should be filled by positively vetted secondees from either the intelligence or policy community.

Impacts of technology

18.40 Much as they will for the intelligence community, ongoing rapid technological developments will have significant implications for oversight bodies. More could be done to support oversight bodies in this context.

18.41 The increasing complexity of the technological landscape will make it progressively more difficult for oversight bodies to understand the nature and operation of agencies' capabilities

and the technological context in which agencies operate. The nature of these challenges will differ between oversight bodies. However, we consider all oversight bodies are increasingly likely to require greater technological expertise in order to effectively perform their functions, whether to oversee agency activities or to assess the appropriateness of the governing legislation.

18.42 In practice, agencies can often provide some technological advice. There is nothing to suggest that agencies have not been forthright and thorough in doing so. However, an oversight body relying wholly on the agencies it oversees for technical advice raises questions about that body's actual or perceived independence.

18.43 To address this issue for the IGIS, the 2019 Comprehensive Review recommended that an independent panel be established to provide technical expertise and assistance to the IGIS. However, the IGIS has submitted that its preferred solution would be to hire an on-staff technical adviser.

18.44 This approach has some advantages over a panel arrangement, particularly in the ease with which oversight staff can access targeted technical advice. However, the challenges in recruiting and retaining technical experts are well established. Further, the scale of technical advice required by some oversight bodies would not warrant a full-time on-staff adviser. And as mentioned, the increasingly complex technological landscape means that the technical advice required by agencies is likely to grow beyond the expertise that could reasonably be expected of a single on-staff adviser.

18.45 As such, we recommend that government establish a panel of experts that can be drawn on to provide technological advice to any oversight body. This panel would supplement, rather than replace, any on-staff technical advisers. The panel should be available to all oversight bodies on an as-needed basis. It should comprise highly cleared technology experts, with a mix of academic and industry backgrounds.

Recommendation 67: That government establish a panel of technological advisers to provide advice to intelligence oversight bodies on an as-needed basis.

Appendix A: Media release

Friday 22 September 2023

The Australian Government has commissioned an Independent Review into Australia's intelligence agencies.

The work of our intelligence agencies underpins Australia's national security objectives, including safeguarding Australia's sovereignty in an increasingly uncertain security environment. Our intelligence agencies help protect Australia's security, prosperity and values in complex and changing circumstances.

The National Intelligence Community (NIC) has undergone significant structural and transformational changes in recent years. The Review will ensure that our intelligence agencies remain well-placed to serve Australia's national interest.

The Review will be co-led by Dr Heather Smith PSM and Mr Richard Maude.

Dr Smith is currently a professor at the Australian National University National Security College and has served as Secretary of the Department of Industry, Innovation and Science, and Deputy Director-General of the Office of National Assessments. In April 2023, Dr Smith was appointed the National President of the Australian Institute of International Affairs. Dr Smith has nearly 20 years' experience in the public service at senior levels.

Mr Maude is currently Executive Director of Policy at Asia Society Australia and a Senior Fellow at the Asia Society Policy Institute. He is a former senior Australian Government official with 30 years' experience in foreign policy and national security, including as the former Director-General of the Office of National Assessments. In May this year, Mr Maude was appointed to the External Advisory Panel to oversee the implementation of the Defence Strategic Review.

The reviewers will consult widely, and welcome public submissions. The findings of the Review will be provided to Government in mid-2024.

Independent Reviews of the intelligence community have been commissioned periodically, with the last completed in 2017.

Public submissions on matters included in the Review's Terms of Reference can be made to IIR2024@pmc.gov.au, or by post to '2024 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 24 November 2023.

Further information, including the Terms of Reference, can be found here: 2024 Independent Intelligence Review.

Appendix B: Terms of Reference

The 2024 independent review of Australia's National Intelligence Community (NIC) will prepare findings and recommendations on the NIC 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 2024 and will focus on the ten agencies of the NIC (Australian Criminal Intelligence Commission, Australian Federal Police, Australian Geospatial-Intelligence Organisation, Australian Secret Intelligence Service, Australian Security Intelligence Organisation, the Australian Signals Directorate, Australian Transaction Reports and Analysis Centre, Defence Intelligence Organisation, Department of Home Affairs and the Office of National Intelligence).

The work of the NIC underpins Australia's national security objectives, including safeguarding Australia's sovereignty in an increasingly uncertain security environment. The NIC is required to respond, in complex and changing circumstances, to protect Australia's security, prosperity and values.

The NIC has undergone significant structural changes since the last Independent Intelligence Review in 2017. Further transformative changes to the NIC are also mid-implementation following the 2019 Comprehensive Review of the Legal Framework of the National Intelligence Community (2019 Comprehensive Review).

The 2024 Independent Intelligence Review will consider:

- The impact of the implementation of the recommendations of the 2017 Independent Intelligence Review and the 2019 Comprehensive Review, including the benefits of the establishment of the Office of National Intelligence, the expansion to create the NIC, and the effectiveness and outcomes of the Joint Capability Fund;
- How effectively the NIC serves, and is positioned to serve, national interests and the needs of Government, including in response to the recommendations of recent reviews relevant to defence and security, and the evolving security environment;
- The status, risks and potential mitigations of major investments in the NIC since 2017;
- Topics identified by the 2019 Comprehensive Review for consideration by future reviews, and whether further legislative changes are needed;
- Whether workforce decisions by the NIC at both the agency and community levels reflect a sufficiently strategic response to current and future workforce challenges, anticipate future capabilities of other states so we are best positioned to counter threats, are in line with the Australian Public Service commitments to diversity and inclusion and offer options if recruitment targets cannot be met;
- NIC preparedness in the event of regional crisis and conflict;
- Whether the use of the classification system by the NIC achieves the right balance between protecting sensitive information and providing decision making advantages to policy makers and operators;

- Whether current oversight and evaluation mechanisms are effective and consistent across the NIC.

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 cooperate fully with the review and provide assistance as requested. Ministers will also be asked to meet and assist the review team. The review team is to consult widely, including seeking submissions publicly.

Appendix C: List of interviews and submissions

Interviews[66]

Government ministers

- The Hon Anthony Albanese MP, Prime Minister
- The Hon Richard Marles MP, Deputy Prime Minister and Minister for Defence
- Senator the Hon Penny Wong, Minister for Foreign Affairs and Leader of the Government in the Senate
- The Hon Dr Jim Chalmers MP, Treasurer
- The Hon Chris Bowen MP, Minister for Climate Change and Energy
- The Hon Mark Dreyfus KC, MP, Attorney-General and Cabinet Secretary
- The Hon Clare O'Neil MP, Minister for Home Affairs and Minister for Cyber Security
- Senator the Hon Katy Gallagher, Minister for Finance, Minister for Women, and Minister for the Public Service
- The Hon Pat Conroy MP, Minister for Defence Industry and Minister for International Development and the Pacific
- The Hon Madeleine King MP, Minister for Resources and Minister for Northern Australia

Parliamentarians

- The Hon Peter Dutton MP, Leader of the Opposition
- The Parliamentary Joint Committee on Intelligence and Security

Senior officials

- Andrew Shearer, Director-General National Intelligence
- Heather Cook, Chief Executive Officer, Australian Criminal Intelligence Commission
- Matt Rippon, A/g Chief Executive Officer, Australian Criminal Intelligence Commission
- Reece Kershaw APM, Commissioner, Australian Federal Police
- Kathryn McMullan, Director, Australian Geospatial-Intelligence Organisation
- Rachel Noble PSM, Director-General, Australian Signals Directorate

[66] Positions are accurate at time of interview.

- Mike Burgess AM, Director-General Security
- Kerri Hartland, Director-General, Australian Secret Intelligence Service
- Brendan Thomas, Chief Executive Officer, AUSTRAC
- Peter Soros, A/g Chief Executive Officer, AUSTRAC
- Lieutenant General Gavan Reynolds AO, Chief of Defence Intelligence
- Professor Glyn Davis AC, Secretary, Department of the Prime Minister and Cabinet
- Jenny Wilkinson PSM, Secretary, Department of Finance
- Dr Steven Kennedy PSM, Secretary, Department of the Treasury
- Greg Moriarty AO, Secretary, Department of Defence
- General Angus Campbell AO DSC, Chief of the Defence Force
- Jan Adams AO PSM, Secretary, Department of Foreign Affairs and Trade
- Katherine Jones PSM, Secretary, Attorney-General's Department
- David Fredericks PSM, Secretary, Department of Climate Change, Energy, the Environment and Water
- Stephanie Foster PSM, Secretary, Department of Home Affairs
- Meghan Quinn PSM, Secretary, Department of Industry, Science and Resources
- Lieutenant General Greg Bilton AO CSC, Chief of Joint Operations, Australian Defence Force
- The Hon Christopher Jessup KC, Inspector-General of Intelligence and Security
- Dr Gordon de Brouwer PSM, Australian Public Service Commissioner
- Iain Anderson, Commonwealth Ombudsman
- Grant Donaldson SC, Independent National Security Legislation Monitor
- Jake Blight, Independent National Security Legislation Monitor
- Kaylene Dale, Deputy Commissioner, Australian Border Force
- Dr Cathy Foley AO PSM FAA FTSE, Chief Scientist
- Richard Windeyer, Deputy Secretary, Department of Infrastructure, Transport, Regional Development, Communication and the Arts.
- Lieutenant General John Frewen AO DSC, Chief of Joint Capabilities, Australian Defence Force
- Graham Fletcher, Deputy Secretary, Department of the Prime Minister and Cabinet
- Roxanne Kelley PSM, Deputy Secretary, Department of the Treasury

- Luke Yeaman, Deputy Secretary, Department of the Treasury
- Hugh Jeffrey, Deputy Secretary, Department of Defence
- Sophie Sharpe, Deputy Secretary, Department of Home Affairs
- Duncan Grove, Deputy Director General, Office of National Intelligence
- Ewan Macmillan, Deputy Secretary, TOP SECRET-Privileged Access Vetting Authority
- Peter West, First Assistant Secretary, Australian Government Security Vetting Agency

Other interlocutors

- Justin Bassi and Chris Taylor, Australian Strategic Policy Institute
- Andrew Dowse, RAND
- Rosemary Huxtable AO PSM
- Major General Duncan Lewis AO, DSC, CSC, National Preparedness Taskforce
- Professor Rory Medcalf AM, Australian National University
- Peter Ford, Ben Scott and Olivia Shen, National Security College, Australian National University
- Steve McFarlane
- Stephen Merchant PSM
- Dennis Richardson AC
- Major General Paul Symon AO
- Peter Varghese AO
- Nick Warner AO PSM
- Greg Wilson
- *Meetings were also conducted with officials in the United States of America, the United Kingdom, Canada, New Zealand and Japan.*
- *We also met with the Business Council of Australia and several of its members.*

Submissions

Government agencies

- The Office of National Intelligence
- The Australian Criminal Intelligence Commission
- The Australian Federal Police
- The Australian Geospatial-Intelligence Organisation
- The Australian Signals Directorate
- The Australian Security Intelligence Organisation
- The Australian Secret Intelligence Service
- Australian Transaction Reports and Analysis Centre
- The Defence Intelligence Organisation
- The Department of the Prime Minister and Cabinet
- The Department of Foreign Affairs and Trade
- The Attorney-General's Department
- The Department of Climate Change, Energy, the Environment and Water
- The Department of Home Affairs
- The Inspector-General of Intelligence and Security
- The Commonwealth Ombudsman
- The Department of Infrastructure, Transport, Regional Development, Communication and the Arts
- The Commonwealth Scientific and Industrial Research Organisation
- The Australian Taxation Office
- The Department of Agriculture, Forestry and Fisheries

States and Territories

- The Department of Premier and Cabinet (Queensland)

Public

- Anywise
- BlackSky LLC
- Honorary Professor Bob Breen OAM
- Dr Peter Corkeron
- Commonwealth Public Sector Union
- Emeritus Professor Paul Dibb AM & Honorary Professor Richard Brabin-Smith AO
- Dr Alan Dyer
- Michael Gately, Trellis Data
- Helen Glazebrook CF, Visual Analysis
- Kate Grayson
- Paul Hadden
- Dr Miah Hammond-Erry & Tom Barrett, The United States Studies Centre
- Brendon Hawkins
- Yun Jiang
- Air Commodore Rick Keir AM CSC GAICD, Stirling Advisory
- Dr Phil Kowalick MAIPIO, The Australian Institute of Professional Intelligence Officers
- KPMG Australia
- Law Council of Australia
- Regenesis Lawyers
- Dr James Renwick AM CSC FRSN FAAL SC
- RSL Australia
- Dr David Schaefer
- Dr Elise Stephenson, Global Institute for Women's Leadership ANU and Professor Susan Harris Rimmer , Law Futures Centre Griffith University
- Jeremy Stredwick, Arc Professional Services
- Chris Taylor, Australian Strategic Policy Institute
- Professor Patrick F Walsh & Ausma Bernot, Charles Sturt University

Appendix D: Glossary

TERM	DEFINITION
ACIC	The Australian Criminal Intelligence Commission
ACSC	The Australian Cyber Security Centre
ADF	The Australian Defence Force
AFP	The Australian Federal Police
AGO	The Australian Geospatial-Intelligence Organisation
AI	Artificial Intelligence
APS	The Australian Public Service
APSC	The Australian Public Service Commission
ASD	The Australian Signals Directorate
ASIO	The Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
ASIS	The Australian Secret Intelligence Service
AUKUS	A trilateral security partnership between Australia, the United Kingdom, and the United States of America.
AUSTRAC	Australian Transaction Reports and Analysis Centre
CCTIC	The Cyber and Critical Technology Intelligence Centre (within ONI)
CPO	Chief People Officer
DFAT	The Department of Foreign Affairs and Trade
DGNI	The Director-General of National Intelligence
DIG	The Defence Intelligence Group
DIO	The Defence Intelligence Organisation
GEOINT	Geospatial intelligence
ICT	Information and communications technology
IGIS	The Inspector-General of Intelligence and Security
INSLM	The Independent National Security Legislation Monitor
INSLM Act	*Independent National Security Legislation Monitor Act 2010*
IQT	In-Q-Tel
IS Act	*Intelligence Services Act 2001*
ISLAB	Intelligence Services Legislation Amendment Bill 2023
JCF	The Joint Capability Fund
JCPAA	Joint Committee of Public Accounts and Audit

TERM	DEFINITION
NIA	The National Intelligence Academy
NIC	The National Intelligence Community
NSC	The National Security Committee of Cabinet
NSSIF	National Security Strategic Investment Fund
NV	Negative Vetting
ONI	The Office of National Intelligence
ONI Act	*Office of National Intelligence Act 2018*
OSINT	Open source intelligence
PJCIS	The Parliamentary Joint Committee on Intelligence and Security
PM&C	The Department of the Prime Minister and Cabinet
REDSPICE	A capability program within the Australian Signals Directorate covering resilience, effects, defence, space, intelligence, cyber and enablers.
SAT	Structured Analytic Techniques
SD Act	*Surveillance Devices Act 2004*
SIGINT	Signals intelligence
STEM	Science, technology, engineering, mathematics
TIA Act	*Telecommunications (Interception and Access) Act 1979*
TS	TOP SECRET
TS-PA	TOP SECRET-Privileged Access