Australian Institute of Professional Intelligence Officers
The peak representative body for all intelligence professionals

24 June 2020

Senate

Finance and Public Administration Legislation Committee

Australian Institute of Professional Intelligence Officers Inc. Submission
National Intelligence Enterprise: Oversight and Evaluation Arrangements

Thank you for the opportunity to provide a submission to the Committee considering the *Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020*. We have reviewed the Information about the bill, including the Explanatory Memorandum (EM) and provide the following submission.

A few brief comments about the National Intelligence Enterprise

The National Intelligence Enterprise (NIE) is critical to the ongoing protection of Australia and Australia's interests, and arrangements put in place to coordinate and optimize Australia's national intelligence effort should do just that. However, the 2017 Independent Review and references contained in the *Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020* EM refer only to agencies in the intelligence enterprise at the federal level, not those at the state and territory levels. Arguably, a national approach should incorporate the contributions of states and territories since we are referring to the protection of Australia and Australia's interests. There is no longer any safe clear separation between federal and state/territory intelligence responsibilities in meeting Australia's national security objectives. The NIE must truly be national.

While the 2017 Independent Intelligence Review and the EM suggest the NIE that supports Australia's national security is no longer limited to the six AIC agencies and that it should now include the Australian Federal Police, the Department of Immigration and Border Protection (DIBP), now the Department of Home Affairs and the Australian Border Force, the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian Criminal Intelligence Commission (ACIC) other federal agencies, and state and territory agencies also make a critically important and increasingly significant contribution to national security. There is little reason provided as to why other federal agencies are not included (let alone State and territory agencies).

The emphasis is around the threats faced by Australia and the role of the NIE in protecting our national interests and references are specifically to terrorism and irregular immigration; however, other issues likely will have an equally catastrophic impact, for example, the COVID-19 pandemic, should they be realized and those issues are the remit of agencies not considered in discussion about the enterprise. Food security, land security, water security, pandemic and other real and immediate threats fall significantly within the remit of state and territory government and federal government agencies not currently included in the NIE but likely to lead prevention, response and recovery efforts in the national interest. Those agencies also have a strong and increasing roles in the exchange of information and other assets with the ten mentioned agencies.

So, two questions arise immediately: one, is the NIE sufficiently different today to be considered a breakthrough in management of our national intelligence effort; and two, are arrangements now in place to effectively coordinate and optimize Australia's national intelligence effort?

The answer seems, on first blush, to be no and that suggests the national intelligence effort is solely the Commonwealth or Federal intelligence effort.

The 2017 Independent Intelligence Review

The 2017 Independent Intelligence Review ('Intelligence Review') found that because of transforming geopolitical, economic, societal, and technological changes, the national intelligence community will be faced with challenges that will intensify over the coming decade. The Intelligence Review's recommendations broadly cover four priority areas: the co-ordinating structures of the intelligence community, new funding mechanisms to address capability issues, the streamlining of legislative arrangements, and measures to further strengthen the state of trust between the intelligence agencies and the Australian community of which they are part.

The Intelligence Review, however, did not define the NIE and the lack of a precise definition may cause confusion in the short term but allows the concept to evolve amid complex dependencies between stakeholders and the tempo of intelligence activities at the national level. Key phenomena observed in social systems – competition, specialization, co-operation, exploitation, learning, growth, and several others – are likely to influence the evolution of the NIE. The Intelligence Review identified the desired end state for the NIE to become a global leader in the intelligence field. That goal is achievable given the international standing of Australian intelligence efforts, and the highly commended international liaison role the AFP has developed and the contribution it makes to law enforcement information sharing, capability building and operational coordination.

In this context, the oversight arrangements for the intelligence enterprise are critical in ensuring its implementation stays the course and that the enterprise achieves the goals set for it.

The AIPIO White Paper 2019

The recently published AIPIO White Paper 1-2019 described and explored four alternative futures for the NIE. Clearly, these alternative futures are not the only possible variations and an intermediate end state is entirely possible. They are not in the 'likely' context, but as scenarios resulting from polar states along two dimensions of greatest concern. What is likely is that the actual outcome will be somewhere in these four quadrants, rather than 'blending'. What all the alternatives expose is the importance of both effective oversight and effective evaluation of the work of the enterprise. The alternative futures are:

> Scenario 1 – Bureaucratic Enterprise. The NIE embraced incremental reform but remained weighed down by hierarchy, risk aversion, and the pursuit of efficiency. While intelligence agencies can point to solid processes and comprehensive metrics, there has been little or no performance improvement.
>
> Scenario 2 – Fractured Enterprise. The NIE reform agenda falters along deep cultural lines, fomenting an unhealthy struggle for influence and resources. Intelligence support became uneven as deep expertise became compartmented, and support was directed towards preferred clients.
>
> Scenario 3 – Obsolescent Enterprise. Initially, the NIE refused to acknowledge the need for transformative change, complacently believing their legacy would shield them from a changing world. Eventually the NIE was unable to build the momentum to change fast enough as the wider democratisation of intelligence rendered agencies obsolescent.
>
> Scenario 4 – Dynamic Enterprise. The NIE boldly pursued the 'enterprise model' and assisted by sustained investment has realised many of the benefits described in The Intelligence Review. Purposeful innovation has positioned the NIE as a global leader in the intelligence field, displaying a high level of collective performance and integration.

Improving coordination is a prevailing orthodoxy of intelligence reform in Australia. Intelligence reviews – both within Australia and overseas – have repeatedly identified that information sharing, interoperability and strong coordination among agencies are critical elements of an effective intelligence response to complex, transnational security challenges. The Intelligence Review also called for the strengthening of these elements in the contemporary intelligence reform agenda. Yet the intelligence reform agenda is not underpinned by a national intelligence strategy or long-term vision of the role intelligence will play in furthering Australia's national interests.

The enterprise model anticipates information sharing across partners in the enterprise; however, because agencies within the Australian Intelligence Community and the broader National Intelligence Community may tend to hoard information and find reasons not to share, rather than ways to share, intelligence reform will remain confined by fundamentally cultural boundaries. Of course, differing security classification levels, security clearances and capability to receive, store and handle classified information and operational security measures, play a part in this but these reasons also point to barriers to information sharing and highlight practical as well as cultural impediments that will likely also hold the NIE back.

Without a long-term intelligence strategy and vision, and with a continuing culture of information hoarding and isolation of the centre (AIC) from the remainder of those who could contribute to the national enterprise in a meaningful way, the role of oversight remains relatively straightforward. Evaluating the impact and effectiveness of the intelligence enterprise, however, emerges as a complex and fraught proposition. For example, oversight is anchored in the Commonwealth jurisdiction through legislation and beyond agreements between the

Commonwealth and State and Territory government, we likely have no legislation or a means to legitimise legislation for the national jurisdiction. A possible solution may be to replicate model legislation across all jurisdictions through the Council of Australian Governments and that would likely raise the need to add 'intelligence' and particularly the NIE to the COAG agenda.

Whereas Scenario 4, identified in the AIPIO White Paper, is the ideal, Scenario 1 is the most likely outcome for the NIE based on the approach that has been taken and the less than substantial reforming of the enterprise.

The AIPIO White Paper 1-2019 is attached to this submission at Annex A.

Proposed oversight arrangements

When considering the oversight of the intelligence enterprise we reviewed arrangements in place with Five Eyes partners to gain an appreciation of how the proposed arrangements in Australia compared to those within partner countries and across the partnership. A full extract of the comparative analysis is attached at Annex B of this submission.

Several questions arose as part of the analysis;

1. Are the existing and proposed arrangements intended by the legislative amendments consistent with those adopted by Five Eyes partners?

   The comparative analysis annexed to this submission suggests they are.

2. The proposed amendments to the legislation apply limits to oversight by certain bodies, but do the resulting arrangements expose gaps that could be detrimental to the oversight of the intelligence enterprise or will they enable effective scrutiny?

   We consider that the proposed arrangements will enable effective oversight and scrutiny of the agencies included in the intelligence enterprise. The deeper question is, if the enterprise was a Dynamic Enterprise (Scenario 4, above) and it harnessed all the capability across all Australian governments, would the proposed oversight arrangement meet the need, or would they run afoul of federation and the complexity that it invokes. Those observations do not mean an intelligence enterprise made up of 10 or 11 nominated federal agencies cannot be a Dynamic Enterprise; it will, however, be a compromise on what a NIE could be.

3. What oversight arrangements vest in the Office of National Intelligence?

   It is unclear from the EM and the *Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020* what, if any, oversight of the intelligence enterprise rests with the ONI.

   It is clear from Section 9 of the *Office of National Intelligence Act 2018* (C'th) that the ONI has a role in the evaluation of activities of an affected agency or agencies in respect of national intelligence priorities, and in 9(c) 'other aspects of an affected agency or agencies;'. Exclusions to the ONI's evaluation function are set out in section 10, but it remains unclear what 'activities' the ONI is expected to review.

   We therefore conclude that since there is no specific inclusion in the *Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020* referring to an oversight function for the ONI, that its responsibilities are limited to evaluating performance and other activities as specified in the *Office of National Intelligence Act 2018* (C'th). However, the use of the term 'activities' and the references to evaluation in respect of resource allocations, intelligence priorities, and effort in the ONI Act may be difficult to distinguish from an oversight role even if the evaluation of activities does not include evaluation of the methods used by an agency or agencies in the intelligence enterprise.

   Moreover, a question that remains unanswered is, will the ONI be able to substantively influence resource allocations between agencies given the many jurisdiction involved when the Director Generals mandate is anchored in the Commonwealth jurisdiction. The choice of performance metrics will be important here; for example, how do the outputs/prioritisation within individual agencies contribute to collective outcomes?

The explanatory memorandum states:

> 7.2 It is critical in a democracy that intelligence agencies are subject to strong oversight and accountability mechanisms. Indeed, oversight of intelligence services is a central tenet of the 'state of trust' between intelligence services and the community of which they are part.

Arguably, the Bill fails to achieve that goal if it limits the intelligence agencies, (or agencies with a remit that contributes to the protection of Australia and Australia's interest), to be included in the NIE and to be subject of the oversight arrangements set out in the Bill. This also

raises another question; is it in the national interest to exclude other Commonwealth and state and territory agencies from the NIE? Perhaps the point of the proposed amendments is that the agencies with the highest level of classified information will now be subject to the enhanced oversight arrangements, which can be justified to the public, in which case, the function of the proposed oversight mechanism should extent to understanding systemic failures in the NIE (due to siloed operations).

The NIE appears to miss an opportunity to change the culture of separation among the intelligence agencies, by selecting specific agencies for inclusion; also, the constant references to the "intelligence community" is an overreach if the independent oversight is not for the entire intelligence community contributing to the protection of Australia and Australia's interests.

Evaluation Arrangements

Running in parallel with oversight arrangements applied to the intelligence enterprise is the requirement for evaluating performance and what performance should actually be evaluated; what methods should be used: and what are the indicators of success (or performance measures to be applied). Additionally, a question about whether a monitoring mechanism is to be used and if so, what is to be counted and monitored; what key performance indicators are to be applied to an agency's or agencies' work; and when will an evaluation take place?

So, matters central to an evaluation process include:

1. Who is being evaluated?
2. What is being evaluated?
3. How often are the evaluations undertaken?
4. Who is conducting the evaluation?
5. What authority does the evaluator have to conduct the evaluation?
6. What methodologies are being used to evaluate performance?
7. What does success look like – what are the KPIs or Performance Measures?
8. Are inputs and outputs or impact and effectiveness the central elements of the evaluation?
9. How will the criminal and regulatory intelligence contributions of the states and territories be recognised in the overall evaluation of performance of the NIE where those contributions are of value in respect of serious and organised crime, terrorism, illegal migration and other crime which is the responsibility of state and territory governments but forms part of the national picture?
10. How will the contributions of other Commonwealth agencies (regulators and compliance agencies, environmental agencies, and others) be measured and included in an overall assessment of the impact and effectiveness of the NIE if they are not acknowledged as being part of the enterprise?
11. Is agency performance against intelligence priorities and collection requirements being monitored and if so, who is monitoring, what is being monitored and how is the monitoring being done?
12. Who evaluates the performance of the ONI in respect of its role coordinating the NIE?
13. Is there an independent evaluation framework, which includes an evaluation of the ONI, as part of the overall evaluation of the intelligence enterprise?
14. Would it be possible to include an assessment of the contributions made to the national intelligence picture or to collection against requirements associated with intelligence priorities by organisations in the private sector to recognise a strong partnering approach between the public and private sector?

It is unclear from the legislation whether any of these questions will be addressed in an evaluation process and most importantly, whether an independent evaluation of ONI and of the NIE will be undertaken at all. Could this role be assigned to the ANAO, which has strong evaluation capabilities and likely capacity or is an alternative body or committee the solution?

Assumptions

In preparing this submission, we have made a number of assumptions on the question of evaluating performance and evaluation arrangements including:

1. The ONI is bound by the *Office on National Intelligence Act 2018* (C'th) to evaluate the performance of the NIE.
2. Evaluation is distinguished from oversight insofar as evaluation refers to performance of an agency or agencies and not roles and functions, whereas oversight refers to roles, functions and governance arrangements.
3. The idea of 'mission management' (https://fas.org/irp/dni/icd/icd-900.pdf) rather than agency or functional responsibilities has likely been considered for the NIE.
4. Some form of independent evaluation of the NIE (including the ONI) will likely be undertaken periodically.

5. ONI will evaluate the efforts of an agency or agencies in the NIE, but only in respect of matters associated with national intelligence priorities and other specific matters set out in Section 9 of the *Office of National Intelligence Act 2019 (C'th).*

   This assumption becomes problematic when considering the role and function of the AFP, ABF, ACIC and AUSTRAC in particular and the nexus to national security for a significant part of the work undertaken by those agencies. This is likely also exacerbated by the wording used in the ONI Act relating to evaluation or resources and activities.

Conclusion

The oversight and evaluation of the work of the national intelligence enterprise is complex and requires careful consideration.

AIPIO remains very supportive of the intention of a NIE and is encouraged by some of the very early steps taken to expand the previous Australian Intelligence Community and National Intelligence Community; however, while tentative steps have been taken, the threat environment has moved and is moving quickly and our approach needs to be more dynamic and proactive. The time for taking small steps may have passed, the time likely is now for bold and innovative reforms. The implementation of the recommendations of the 2017 Independent Intelligence Review and of recommendations arising from the Hope Royal Commission, conducted some 40 years ago, see a tentative, steady as we go approach, rather than a future focussed one.

AIPIO has raised a range of issues in the comments above and we remain available to address them with the Committee should further exploration be considered desirable.

Dr Phil Kowalick
President, AIPIO

Annex A

WHITE PAPER | 1-2019

THE FUTURE OF THE

NATIONAL INTELLIGENCE ENTERPRISE

IN AUSTRALIA

DECEMBER 2019

PREFACE

The Australian Institute of Professional Intelligence Officers (AIPIO) Inc is committed to growing the intelligence body of knowledge through fostering scholarship, professionalization of practice, support to major intelligence research projects, and professional collaboration amongst practitioners at our events.

Each year, AIPIO promotes a theme to focus our investment in thought leadership. In 2019, the theme was 'An Emerging Intelligence Enterprise' – which aligns with the core proposition in the 2017 Independent Intelligence Review, and the many related initiatives now underway.

The changing nature of 21st century intelligence demands greater connectivity and collaboration. We need to move beyond the traditional concept of intelligence professionals and the intelligence 'community' to realise a strengthened, diverse intelligence 'enterprise' spanning jurisdictions, government agencies, business, finance, technology, and other partners. It is the sharing and integrating of individual capabilities and areas of excellence between these groups that will lead to strong collective performance and outcomes, to effectively leverage change and identify opportunities for collaboration.

Curating and supporting the burgeoning intelligence profession of tomorrow across multiple domains of practice requires strategic management and transformational change. AIPIO activities in 2019 — especially the national conference — explored this emerging landscape in Australia and beyond, especially what it means for capability planning, organisational development, and analytic rigour.

AIPIO has captured the insights generated during this year and given them a forward-looking focus. This White Paper (1-2019) entitled *'The Future of the National Intelligence Enterprise in Australia'* offers four alternate futures highlighting challenges and opportunities for all stakeholders in the intelligence profession over the longer term.

Dr Phil Kowalick, MAIPIO
President, Australian Institute of Professional Intelligence Officers (AIPIO) Inc

CONTENTS

EXECUTIVE SUMMARY

The 2017 Independent Intelligence Review (the 'Intelligence Review') found that because of transforming geopolitical, economic, societal, and technological changes, the national intelligence community will be faced with challenges that will intensify over the coming decade. The Intelligence Review's recommendations broadly cover four priority areas: the co-ordinating structures of the intelligence community, new funding mechanisms to address capability issues, the streamlining of legislative arrangements, and measures to further strengthen the state of trust between the intelligence agencies and the Australian community of which they are part.

This White Paper outlines four alternate futures for the national intelligence enterprise. The futures are exploratory and do not attempt to predict the future of the national intelligence enterprise but rather sketch out plausible dynamics and choices that could give rise to each of them. The four alternate futures do not represent all the futures for the national intelligence enterprise, but they offer a basis for challenging deeply held assumptions, and may assist in generating insights, or at least promoting a dialogue about a change agenda. The emerging future is likely to be messier – perhaps reflecting a combination of elements of the different scenarios outlined below.

- **Scenario 1 – Bureaucratic Enterprise.** The NIE embraced incremental reform but remained weighed down by hierarchy, risk aversion, and the pursuit of efficiency. While intelligence agencies can point to solid processes and comprehensive metrics, there has been little or no performance improvement.
- **Scenario 2 – Fractured Enterprise.** The NIE reform agenda falters along deep cultural lines, fomenting an unhealthy struggle for influence and resources. Intelligence support became uneven as deep expertise became compartmented, and support was directed towards preferred clients.
- **Scenario 3 – Obsolescent Enterprise.** Initially, the NIE refused to acknowledge the need for transformative change, complacently believing their legacy would shield them from a changing world. Eventually the NIE was unable to build the momentum to change fast enough as the wider democratisation of intelligence rendered agencies obsolescent.
- **Scenario 4 – Dynamic Enterprise.** The NIE boldly pursued the 'enterprise model' and assisted by sustained investment has realised many of the benefits described in The Intelligence Review. Purposeful innovation has positioned the NIE as a global leader in the intelligence field, displaying a high level of collective performance and integration.

This White Paper finds that transformational change will require sustained effort to create the environment for the enterprise approach to be successful. Innovation will be a key imperative to evolve the NIE. The White Paper also stresses that wider intelligence reform — whether in Australia or overseas — is fundamentally cultural. Accordingly, the consideration of challenges and opportunities arising from the scenarios, focus on their implications for intelligence management, intelligence practitioners, and the intelligence profession. The White Paper concludes with a discussion of how the Australian Institute of Professional Intelligence officers (AIPIO) could become a trusted partner in support of the evolving NIE.

INTRODUCTION

Background

The 2017 Independent Intelligence Review (the 'Intelligence Review') found that Australia's intelligence agencies are highly capable and held in high regard by their international partner agencies. The Intelligence Review also found that because of transforming geopolitical, economic, societal, and technological changes, the intelligence community will be faced with challenges that will intensify over the coming decade.

To address these challenges, the Intelligence Review made a series of recommendations to provide a pathway to an even higher level of collective performance. These recommendations broadly cover four priority areas: the co-ordinating structures of the intelligence community, new funding mechanisms to address capability issues, the streamlining of legislative arrangements, and measures to further strengthen the state of trust between the intelligence agencies and the Australian community of which they are part.

What is the National Intelligence Enterprise?

"The Intelligence Review identified the desired end state for the NIE was to become a global leader in the intelligence field."

The Intelligence Review does not define the National Intelligence Enterprise (NIE). The lack of a precise definition may cause confusion in the short term but allows the concept to evolve amid complex dependencies between stakeholders and the tempo of intelligence activities at the national level. Key phenomena observed in social systems – competition, specialization, co-operation, exploitation, learning, growth, and several others – are likely to influence the evolution of the NIE. The Intelligence Review identified the desired end state for the NIE was to become a global leader in the intelligence field.

Approach of the White Paper

"The White Paper adopts the scenario method – which is a core concept and one of the most widely used methods in foresight studies."

This White Paper addresses the focal question: 'What is the future of the National Intelligence Enterprise in Australia' with a time horizon of 2030. The White Paper adopts the scenario method – which is a core concept and one of the most widely used methods in foresight studies. This application of the scenario method is exploratory not predictive — positing that the future is neither predictable nor pre-determined but can be affected by individual choices and decisions leading to alternate futures. The scenario method also helps to stimulate creativity and to break from the conventional obsession with present and short-term problems.

Structure of the White Paper

This White Paper considers pertinent drivers of change over the next decade, outlines four scenarios for the future of the NIE, and the dynamics and choices that could give rise to each of them. The paper stresses that intelligence reform – whether in Australia or overseas - is fundamentally cultural. Accordingly, the consideration of challenges and opportunities arising from the scenarios, focus on their implications for intelligence practitioners, intelligence management, and the intelligence profession. The White Paper concludes with a discussion of how the Australian Institute of Professional Intelligence officers (AIPIO) could become a trusted partner in support of the emerging NIE.

Drivers of change are likely to create movement in the possibility space and influence the evolution of the NIE over the next decade. These illustrative drivers are neither equally important nor are their outcomes equally uncertain. The drivers may have multiple possible states in the different scenarios.

National Security Outlook

Australia's security environment is becoming more contested and will remain dangerous for the foreseeable future. The unprecedented change occurring in global geopolitical circumstances presents an increased likelihood that in the nearing years, the world could experience a series of massively transformative events — some of which will seemingly come out of the blue. Crowding of the national security agenda will make prioritisation more difficult – and with a tendency to focus on the intelligence problem du jour – could lead to over-concentration on a single threat.

Conflict in East Asia. The prospect of prolonged strategic competition between the US and China, and the potential for that competition to slide into military conflict, should directly shape Australian national security outlook over the coming decade.

Conflict in North East Asia. Tension on the Korean Peninsula will likely rise in the near term because of the collapse of diplomacy between the US and North Korea towards the goal of denuclearisation of North Korea. Renewed provocations from the North would pressure the Trump administration to reassert a new maximum pressure campaign without good prospects for a return to diplomacy.

Conflict in the Middle East. Tensions between the US and its partners in the Middle East arrayed against Iran continue to grow, and military conflict in the near term, perhaps stemming out of another military incident similar to the Iranian shooting down of a USAF Global Hawk UAV, or a direct Iranian attack on a US ally in the region, can't be dismissed.

Intelligence Reform Agenda

Improving coordination is a prevailing orthodoxy of intelligence reform in Australia. Intelligence reviews – both within Australia and overseas – have repeatedly identified information sharing, interoperability and strong coordination among agencies are critical elements of an effective intelligence response to complex, transnational security challenges. The Intelligence Review also called for the strengthening of these elements in the contemporary intelligence reform agenda. Yet the intelligence reform agenda is not underpinned by a national intelligence strategy or long-term vision of the role intelligence will play in furthering Australia's national interests.

Importantly, the Intelligence Review did not arise because of an existential threat to Australia and lacked the gravitas to shift the perception of national security and propel the Australian response. Historically, decisive action took place only after a disaster had occurred or specific weaknesses had been laid bare. Both the United States and the United Kingdom took bold steps after the attacks of 11 September 2001 and 7 July 2005 respectively to strengthen the co-ordination and integration of their intelligence communities. In Australia, between 2002 and 2010, successive federal governments promulgated 45 new security laws.

Indeed, the 'enterprise model' may not prove to be the panacea for reform. First, the volume of information is so vast that even with the continued rapid advances in data processing it cannot be collected, stored, retrieved, and analysed in a single database or even network of linked databases. However, this proposition may be challenged by growing investments in artificial intelligence and quantum computing. Second, legitimate security concerns limit the degree to which classified information can safely be shared, especially as more porous organisational boundaries increase the potential damage done by insider threats. And third, the different intelligence services and the subunits of each service tend, because information is power, to hoard it. Intelligence reform will remain fundamentally cultural.

DRIVERS OF CHANGE

"Crowding of the national security agenda will make prioritisation more difficult ..."

"... the intelligence reform agenda is not underpinned by a national intelligence strategy or long-term vision of the role intelligence will play in furthering Australia's national interests."

Public Sector Reform

The NIE is bureaucratic in character, comprising institutions and agencies often insulated by different cultural practices. The 2019 Independent Review of the Australian Public Service (the 'APS Review') echoed many of the enterprise design imperatives in the Intelligence Review, viz.:

> 'In a complex, changing world, the APS needs to work flexibly and nimbly across organisational boundaries. It needs to respond dynamically to change, and to harness the right APS expertise, perspectives, and resources to deliver seamless services and solve problems. It needs to empower people and teams to deliver outcomes, not deal with process and hierarchy. And in an era of continued fiscal pressure, the APS needs carefully prioritised investment in capital, including digital transformation, and needs to provide robust, evidence-based advice to inform government budget decisions.'

"This wave of public sector reform is likely to buoy the intelligence reform agenda."

Reforming the APS to achieve this change is ambitious. Partly this is because the APS itself is big and diverse, consisting of more than 190 separate entities and companies, hundreds of boards and committees, and many subsidiaries and other arrangements, all with an annual budget around $430 billion. But transformational change will be necessary to deliver an APS that is fit-for-purpose to meet the rising expectations of Australians and emerging opportunities and challenges – economic, social, technological, and geopolitical over the next decade and beyond. This wave of public sector reform is likely to buoy the intelligence reform agenda.

Intelligence Workforce

Technological enablement is a dominant feature of the intelligence reform agenda but integrating digital technologies that allow collaboration without adopting complementary social practices will diminish the benefits afforded by the new technologies. Notwithstanding technological enablement, intelligence will remain a 'people business' but the character of the workplace and management imperatives would change in response to the unprecedented presence of four 'generations' in the workplace, namely Baby Boomers, plus Generations X, Y and Z.

"... intelligence will remain a 'people business' but the character of the workplace and management imperatives would change ..."

Over the next decade, Generation X will dominate management levels of the intelligence community, with Generation Y providing the bulk of active practitioners. By 2030, the leading edge of millennials will be nearing 50, and they and Gen Z will make up most of the workforce. Two key challenges are the leaching of corporate knowledge in the wake of Baby Boomer decline, and the lack of innate, institutional loyalty by Generation Y.

More broadly, the intelligence workforce is likely to become a national asset, and more important in whole-of-nation security planning, as both foreign nation states and non-state actors resort to hybrid or grey-zone conflict. Increasing the diversity of the intelligence workforce beyond comprising multiple generations, to include varying cultural heritage, worldview, and career aspiration will evolve a 'different' national asset better able to comprehend and navigate the post-normal world.

Wild Cards

Wildcards are low-probability, high-impact events that happen very quickly, with potentially significant consequences for the focal question – the future of the NIE. For example, the COVID-19 pandemic, which began as a public health issue with deepening economic impacts could pose enduring national security concerns. Consideration of wild cards in the context of the scenarios helps surface new uncertainties and different approaches for future action that may not emerge from the more logical structure of a scenario framework.

Weakening of International Intelligence Cooperation. Five Eyes is one of the world's most successful intelligence gathering and sharing partnerships – at the core of Australia's national security strategy — now under new stress over Chinese participation in 5G telecommunications networks. The Fives Eyes partners are not (not yet, at least) unified on this 5G issue, with New Zealand, Canada and Britain having more nuanced and perhaps questionable positions. Huawei represents a significant challenge to the future of Five Eyes, which could lead to the weakening of international intelligence cooperation. Also, the intelligence-sharing deal between South Korea and Japan is a linchpin of trilateral security cooperation but is complicated by painful, wartime history.

Prioritisation of Domestic Threats in the National Security Outlook.
The management of threat could become more challenging with the emergence of new internal and intangible threats bearing upon national security and competing for scarce government resources. This growing threat complexity may dislocate an intelligence and security apparatus focused on the external environment and constrained by policy inertia. Under these circumstances, and in the absence of reliable means for measuring NIE effectiveness, political interest in external threats might weaken and constrain the intelligence reform agenda.

“Consideration of wild cards in the context of the scenarios helps surface new uncertainties and different approaches for future action ...”

ALTERNATE FUTURES

This White Paper outlines four scenarios for the future of the national intelligence enterprise, the dynamics and choices that could give rise to each of them, and their implications for intelligence managers, intelligence practitioners, and the intelligence profession. The four scenarios are exploratory and do not attempt to predict the future of the NIE but rather sketch out conceivable alternative futures and some of the implications for key stakeholders. The four scenarios do not represent the totality of NIE futures, but they offer a basis for challenging deeply held assumptions, and may assist in generating insights, or at least promoting a dialogue about a change agenda. The actual course of events is likely to be less contained – perhaps reflecting a combination of key elements of the different scenarios outlined in this White Paper.

Scenario One – Bureaucratic Enterprise

The Bureaucratic Enterprise has hastened slowly to embrace the intelligence reform agenda. Unable to break from the conventional obsession with present and short-term problems, the Bureaucratic Enterprise placed a strong emphasis on business planning rather than strategy. The Bureaucratic Enterprise is process and compliance driven offering little or no performance improvement. Limited performance improvement has been disguised by ambiguous performance metrics for the national security community – both at the intelligence agency level, and for the enterprise.

“... process and compliance driven offering little or no performance improvement.”

Still present in the Bureaucratic Enterprise architecture are the traditional hard functional and organisational boundaries – favoured for their contribution to efficiency. Efficiency is still considered a pre-eminent goal, but notions of simplifying tasks and centralising authority limits the Bureaucratic Enterprise from responding effectively to the rapidly changing environment created by technology. Efficiency fails to make room for adaptability in structures, processes, and mindsets.

Much of the Bureaucratic Enterprise capital budget has been consumed by addressing accumulated technical debt in legacy ICT systems deemed necessary to ‘keep the lights on’ within individual agencies but constraining enterprise solutions for improved collaboration, coordination, and digital transformation. Expanded scrutiny by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into capital expenditure increases competitive tension between agencies, which constrains inter-agency collaboration.

However, the Bureaucratic Enterprise did deliver some early demonstrable agency-level gains from incremental change but a poor shared understanding by agencies of the ‘intelligence enterprise’ concept have limited the impact of gains at the enterprise level. Despite a series of leaders’ best intentions, the Bureaucratic Enterprise remains bloated and dominated by a self-reinforcing culture that unintentionally rewards intelligence managers who suffocate more transformative innovative ideas that might threaten the established way of doing things.

“... plagued by ongoing barriers to improved coordination and collaboration ...”

The Bureaucratic Enterprise has also been plagued by ongoing barriers to improved coordination and collaboration, including security classification systems, poor ICT connectivity, and embedded cultural practices. The trialling of alternative options for Top Secret (PV) clearances – intended to alleviate Australian Government Security Vetting Agency (AGSVA) backlog — proved ineffective, and unsupported by Australia’s Five Eyes partners. Consequently, there has been token engagement of external expertise, and greater emphasis placed on APS-wide generalist skills than building specialist expertise in areas such as analytic methods.

Indeed, the more prominent place of intelligence in modern society has reinforced risk-averse behaviour especially where assessments can produce unintended effects on Australians. The dynamic threat environment, actionability, and risk has distorted the balance of production between current and estimative intelligence, emphasizing the former, and resulting in the loss of a strategic perspective across the Bureaucratic Enterprise.

Scenario Two – Fractured Enterprise

In past intelligence reforms, founded on existential threats such as 9/11, individual agencies in the enterprise grew simultaneously, avoiding hard questions about where funding should be prioritised. In the Fractured Enterprise, pursuing the intelligence reform agenda has sharpened distinctions between the resourcing, power, and influence of individual agencies and institutions in the enterprise. Individual agencies and institutions in the Fractured Enterprise were uncomfortable ceding control by thinking and acting outside of traditional boundaries – a mindset shift that was essential for an enterprise model to be successful.

The emergence of new and unfamiliar domestic threats required capabilities outside the Fractured Enterprise. The widespread use of the private sector to augment the enterprise led to a hollowing out of expertise in the public sector. Key areas of expertise were concentrated in individual agencies and institutions because contractual arrangements focused too heavily on competition and not enough on collaboration across the enterprise. Advancing the interests of individual agencies was given more weight in decision making rather than taking advantage of the intellectual capacity and administrative experience the enterprise had to offer.

“... sharpened distinctions between the resourcing, power, and influence of individual agencies and institutions in the enterprise.”

Despite new challenges, funding for strategic responses to technological change favoured specific agencies closer to issues at the core national security agenda. Individual agency heads sought to please key political clients in other ways, to demonstrate responsiveness by devoting resources to more tactical and immediate support than to strategic and longer-term advice, and intelligence activities with dubious domestic and international benefits. The ‘intelligence enterprise’ concept grew increasingly ambiguous and irrelevant.

Minimising political risk became a key concern for the Director of National Intelligence (DNI), but without the authority to direct resources across and between agencies the DNI lacked the clout to mitigate political risk. However, whistle-blower concerns about politicisation triggered expanded uncomfortable public scrutiny by the Inspector-General of Intelligence and Security (IGIS). Alignment with partisan concerns undermined the confidence of the Parliament and the public in the Fractured Enterprise as an apolitical institution.

“... the intelligence workforce became careerist – pursuing personal advancement without regard to the enterprise ethos and mission.”

In the Fractured Enterprise, the intelligence workforce became careerist – pursuing personal advancement without regard to the enterprise ethos and mission. Professional development became a means to outshine others rather than to improve the quality of intelligence collaboration, production, and service. Intelligence managers and practitioners kept a keen eye on the political agenda of their own agencies and institutions, regarding the professionalisation of intelligence practice as an abstraction and distraction from ruthless execution of assigned tasks.

Scenario Three – Obsolescent Enterprise

The Obsolescent Enterprise has been too slow to recognise and adapt to disruption arising from the external democratisation of intelligence, and growing contestability of intelligence assessment. There is now much more scope for constructive competition of ideas and many sources of expert advice on intelligence issues, but the Obsolescent Enterprise is more inward-looking and seemingly anonymous as it does a poor job recording, documenting, analysing, or distilling lessons from its own past experiences.

“... subscribed to the proposition that the work of tomorrow will be the same as the work of today.”

The Obsolescent Enterprise subscribed to the proposition that the work of tomorrow will be the same as the work of today. Decisions are top-down, and the intelligence workforce interactions are transactional and unlikely to lead to new opportunities or innovations. Within agencies, innovation is incremental using familiar approaches to help improve the existing system. Beyond agency boundaries, collaboration and coordination efforts become code for control, ensuring everyone ‘sings from the same song sheet’, promoting ‘groupthink’ and constraining transformation.

Intelligence managers, who have reached their position in the Obsolescent Enterprise by learning the intricacies of the current 'system,' openly or subversively resist efforts to change the system. The trajectory to this future is managerial in nature, as it represents a system in use, and managers who must keep it running, it is the way that things get done today. No one has great expectations of quality or public acceptance. Nothing is ventured, nothing is threatened. The level of intelligence support has remained desultory for so long that the Obsolescent Enterprise has settled into a comfortable rut.

The lack of interest and investment in professionalising intelligence practice across the Obsolescent Enterprise has led to great variation in the competence and skill of individual analysts, uncertainty regarding the very duties of intelligence practitioners and an overall diminution in the role that intelligence analysis could play in decision making. A doctrinaire embrace of the familiar 'intelligence cycle' production model has led to practices – and intelligence architectures — better suited to traditional 'complicated' settings rather than the prevalent complex settings confronted by the enterprise as the world moved from a 'data-poor world with relatively predictable settings' to a 'data-rich world with unpredictable settings.' The failure to hold intelligence practitioners accountable to formal professional standards prevents their services from being fully utilized. In the Obsolescent Enterprise, intelligence consumers have no assurance that intelligence analysis is consistently reliable.

"... intelligence practitioners concerned about the future of the enterprise, have chosen to leave for other opportunities, and others have become fearful and less engaged."

For the Obsolescent Enterprise, sustaining the level of funding for the enterprise has proven difficult in the absence of a major national security incident. Mounting legacy technical debt constrains investment for transformation and technical barriers to enterprise-wide collaboration prove intractable. The loss of political interest in intelligence transformation coupled with the Government's insistence that performance targets must be commensurate with the resources the Government makes available has constrained funding to keeping the lights on.

In the Obsolescent Enterprise, the long period of heightened uncertainty about the viability of the enterprise has taken a toll on workplace culture. Many of the best intelligence practitioners concerned about the future of the enterprise, have chosen to leave for other opportunities, and others have become fearful and less engaged. The wider lack of operational agility precludes the agencies and institutions of the enterprise from making the quick pivots necessary for surviving and thriving.

Scenario Four – Dynamic Enterprise

The Dynamic Enterprise moved boldly and decisively to implement the reform agenda outlined in the Intelligence Review. The impact of the intelligence reform agenda was not immediate or overly disruptive, but over time was transformational. The Dynamic Enterprise consciously leaned into changes and counterintuitive activities at the precise moments when it is most uncomfortable to do so, especially when the forces of inertia and gravity was pushing it toward a predictable outcome.

"... recognised that efficiency is necessary but no longer sufficient to be successful."

The Dynamic Enterprise stresses the importance of intelligence architecture over intelligence process, highlighting the limitations of traditional intelligence models in navigating a complex problem space. The Dynamic Enterprise has taken full advantage of new technologies to facilitate collaboration, allow more responsive service delivery to clients, as well as driving increased efficiency. Networks have become the main institutional design feature of the Dynamic Enterprise, allowing innovation to emerge from anywhere and ripple across the enterprise at the speed of relevance.

Absent from the Dynamic Enterprise are the traditional hard functional and organisational boundaries – favoured for their contribution to efficiency – because it is recognised that efficiency is necessary but no longer sufficient to be successful. For the millennials in the intelligence workforce, workplaces are now seen more as networks than as hierarchies. Intelligence practitioners are more likely to seek out the people they need to work with, at any level, to get their work done. Intelligence managers who are frustrated by anyone who does not work through proper channels are seen by millennials as a bad user experience. The best intelligence practitioners do not need to be managed - they need guidance, because they're already self-motivated and brimming with ideas.

Capability development across the Dynamic Enterprise becomes easier as its agencies and institutions stopped thinking in terms of 'owning' capability but rather considered that they are 'leasing' and 'leveraging' capability in a whole of nation context. Technological innovation and the rise of open source intelligence (OSINT) weakened the basis for longstanding information security protocols, especially as OSINT displaces traditional sources. These evident gains from joint capability development and systems integration on an enterprise-wide basis offered up a 'collaboration' dividend.

The Dynamic Enterprise has defined the knowledge, skills and abilities needed for each specialty related to intelligence production, providing more nuanced understanding of the education, training and professional development needed for each specialty. Over time, this investment in the intelligence workforce has led to greater consistency and reliability in intelligence production, and improvements in both individual and organisational performance.

"... stopped thinking in terms of 'owning' capability but rather considered that they are 'leasing' and 'leveraging' capability in a whole of nation context."

CHALLENGES AND OPPORTUNITIES

"The key recommendations of the Intelligence Review (are) probably insufficient to stimulate further information sharing, collaboration, and integration – which are all cultural in nature."

"Exaggeration of the challenges to reform is more often a managerial failure rather than an organisational one."

The four scenarios are differentiated based on how empathically the agencies and institutions in the NIE embraced the intelligence reform agenda outlined in the Intelligence Review. The scenarios highlighted that enterprise planning privileging efficiency will deprive organisational decision makers of a full range of alternatives. The key recommendations of the Intelligence Review — creation of the Office of National Intelligence (ONI), legislative reform, joint intelligence capability development, and strategic human resource management of the intelligence workforce are timely and appropriate but, by themselves, probably insufficient to stimulate further information sharing, collaboration, and integration – which are all cultural in nature.

For reform to be successful, the intelligence workforce needs to come along and ensure that change is deeply embedded in structures and systems. Otherwise, good ideas will inevitably be lost through poor implementation. The scenarios highlighted that many elements of capability – organisations, people, systems, and tradecraft — will need to change concurrently and yet remain synchronized. Capability development will become easier if organisations stop thinking in terms of 'owning' capability but rather consider that they are 'leasing' and 'leveraging' capability. The arrangements needed to effect coherent capability development will operate quite independently of individual organisational structures. The NIE will need to become less organisation-centric and more interdependent as pressure grows from self-organisation through the proliferation of collaboration channels. A longer-term perspective on strategic change is also needed to aid futureproofing of intelligence capability, especially through partnerships extending beyond the traditional intelligence community.

The key recommendations of the Intelligence Review should be only the beginning of a larger necessary reform. The likely novelty of future threats requires commensurate novelty by the NIE. But it is challenging to take effective action to mitigate the risk of something that hasn't occurred previously. The scenarios highlighted that a key challenge will be making the NIE more receptive to innovation in multiple dimensions — conceptual, organisational, process, and technological. In its most basic form, innovation is simply the act of introducing something new; however, if innovation is to have any real value for the NIE, it must have a purpose — introducing something new to achieve a specific change — and it must achieve its purpose to be successful.

Intelligence Managers

The Intelligence Review judged that the NIE 'would benefit from greater investment in the development of its current and future leaders.' Exaggeration of the challenges to reform is more often a managerial failure rather than an organisational one. The scenarios highlighted that issues beyond the characteristics of individual intelligence products or services, will determine the success of intelligence effort. The agencies and institutions within the NIE will require an intelligence effort more closely attuned to collective objectives. Organisational and functional barriers should be removed to allow the collective knowledge, skills, and behaviours of the entire NIE to be mustered into something that is greater than the mere sum of its parts. The intelligence management function will be core to achieving this synergistic effect.

Digital technologies will become more pervasive and integrative, making the agencies and institutions in the NIE more pliable and porous, and the intelligence workforce more questioning, assertive, and independent. The management imperatives of this 'new organisation' are to continually improve as part of its normal functioning; to be intelligent, critical, and open; and to be creative and capable of eternally transforming themselves while sustaining a sense of purpose and direction. Intelligence managers will need to ask, 'As technology frees us to do different work, what are the mindsets, tools, and capabilities we need in order to embrace the value that humans can bring to work, and what types of investment does the enterprise need to make to support that?' These investments should seek to create a work environment — which includes the physical and virtual spaces as well as the management systems and practices — that encourages (and requires) intelligence practitioners to use their human capabilities to find new sources of value for the NIE.

Reform objectives will be achieved by people. Traditionally, many management roles have involved defining individual tasks and even specific processes for completing them. Tomorrow, tasks that can be prescribed will be more often automated, ensuring that fewer employees perform repetitive tasks, and more are engaged in personalizing services, innovating offerings, and creatively solving problems. In the NIE, intelligence managers must set the conditions for a culture of innovation; a culture eager to adopt new ideas, and a culture committed to learning and improvement. Without an innovation culture, initiatives to create change and incorporate change will have no place to take root and grow.

Intelligence Practitioners

As the 9/11 Commission concluded, there is a risk that the practices used to succeed in the past will not serve intelligence so well into the future. The success of intelligence at any time depends on anticipation and adaptation to the opportunities and challenges posed by emerging conditions, technical possibilities, and information flows. Evolution of the NIE requires that innovation and problem solving become the products of teamwork, not a single architect. Yet, for example, intelligence practitioners currently do not experience high levels of individual autonomy due to involvement of management in approving the dissemination of most finished intelligence analysis.

“... innovation and problem solving become the products of teamwork, not a single architect.”

The future will punish intelligence practitioners committed to employing old methods to solve new problems. Old methods and mindsets need to incorporate knowledge from new domains, such as decision science, network theory and drama theory, if they are to better deal with emerging challenges and opportunities. For example, the pervasive employment of digital technologies and increased automation are changing how people work and what they can contribute to organisational success. Intelligence practitioners should use, develop, and adapt their new skills, tools, and techniques, and develop the capabilities to keep learning and adapting as conditions change.

The changing intelligence workforce – influenced by generational change — will likely relate to cross-community challenges rather than organisational loyalty, so accredited training will be necessary to ensure transportability of qualifications across the intelligence community. Systems standardization across the NIE is unrealistic; however, interoperability and complementarity are worthwhile and achievable design objectives. Innovation in tradecraft through partnerships beyond the NIE offers the only real sustainable competitive advantage in a dynamic threat environment.

“... accredited training will be necessary to ensure transportability of qualifications across the intelligence community.”

Intelligence Profession

Intelligence is a discipline that has not yet been widely accepted as a profession, perhaps due to its relatively small personnel base and lack of external scrutiny. Unlike other recognised professions, intelligence as practiced is unregulated, unstandardized, and lacking in key aspects of a profession. The failure to professionalise has led to great variation in the competence and skill of individual intelligence officers, uncertainty regarding the duties of intelligence officers, and an overall diminution in the role that intelligence could play in decision making. The APS Review calls for deploying a wider range of specialist talent and further investment in the skills, capability, and expertise of the APS workforce. Recognition of intelligence as a distinct discipline requiring a specialist workforce would accelerate the move towards intelligence as a profession.

“... great variation in the competence and skill of individual intelligence officers ...”

AIPIO as a Trusted Partner of the NIE

Professional practice is not immune from change, but the intelligence profession often struggles to give up the tried, tested, and familiar without stimulus. From its beginning in 1991, AIPIO has been committed to the professionalisation of intelligence across multiple domains of practice with the aspirational goal of establishing intelligence as a recognised profession in Australia. AIPIO also has advocated for keeping the practitioner central in intelligence practice. The central role of intelligence managers, intelligence practitioners, and the intelligence profession in intelligence reform makes AIPIO a natural partner in the evolution of the NIE in Australia.

In Australia's increasingly complex operational environment, the agencies and institutions of the NIE will not be able to go it alone. The Intelligence Review judged that the NIE 'generally would benefit significantly if external engagement was more systematic and better co-ordinated.' However, the proposed external engagement was narrowly defined in terms of 'appropriate and productive exchanges on science and technology issues with publicly funded research agencies, academia and industry within Australia.' This approach seems anchored to the agencies in the national security community, overly transactional, biased towards the technological dimension of innovation, and unlikely to achieve the desired end state of the Intelligence Review: making the NIE a global leader in the intelligence field.

"AIPIO envisages a partnership approach based on an ecosystem model."

Alternatively, AIPIO envisages a partnership approach based on an ecosystem model. The ecosystem would comprise a network of cross-industry players who work together to define, build, and execute innovative solutions across multiple dimensions - conceptual, organisational, process, and technological. The ecosystem would be defined by the depth and breadth of potential collaboration among a set of players, with each delivering a component of the solution, or contribute a necessary capability. The power of an ecosystem model is that no single player needs to own or operate all components of the solution, and that the value the ecosystem generates is larger than the combined value each of the players could contribute individually.

"AIPIO could make key contributions to improve intelligence performance."

Within the proposed ecosystem model, AIPIO could make key contributions to improve intelligence performance:

- Maintain a strategic focus on professionalisation of intelligence practice.
- Focus thought leadership on intelligence management – which is a poorly defined competency – and on analytic methods more appropriate to modern complex operating environments.
- Develop an authoritative formal knowledge base – an Intelligence Body of Knowledge (IBOK).
- Provide a virtual learning facility for the NIE, to support a systematic approach to professional development informed by good practice across multiple domains of intelligence practice.
- Manage an NIE certification program for intelligence managers and practitioners, including the capture of continuing professional development.
- Manage an open innovation network of skilled practitioners with a deep understanding of intelligence practice and able to operate across the innovation value chain.

REFERENCES

Agrell, W. (2002) "When Everything is Intelligence, Nothing is Intelligence." The Sherman Kent Center for Intelligence Analysis. Occasional Papers (1)4 (October) http://www.cia.gov/cia/publications/Kent_Papers/pdf/OPNo 4.pdf

Bates, R.W. (1982). The Intelligence Profession. *American Intelligence Journal*, (4)3, pp.19-23.

Best, R.A. (1996). *Proposals for Intelligence Reorganization 1949-1996.* Congressional Research Service: Washington, DC.

Hackman, J.R. (2011). *Collaborative Intelligence: Using teams to solve hard problems.* Berrett-Koehler Publishers: San Francisco.

Jones, D.M. (2018). Intelligence and the management of national security: the post 9/11 evolution of an Australian National Security Community. *Intelligence and National Security.* (33)1, pp.1-20.

L'Estrange, M., Merchant, S. and Lobban, I. (2017). *Independent Intelligence Review.* Department of the Prime Minister and Cabinet: Canberra.

Lowenthal, M.M. (2018). *The Future of Intelligence.* Polity Press: Cambridge.

McChrystal, S. (et.al.) (2015). *Team of Teams: New rules of engagement for a complex world.* Portfolio Penguin: St Ives.

Peppler, C.B. (2006). *The Future of Intelligence.* Australian Homeland security Research Centre: Canberra.

Pillar, P.R. (2011). *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and misguided reform.* Columbia University Press: New York.

Thodey, D. (et.al.) (2019). *Our Public Service Our Future.* Independent Review of the Australian Public Service. Department of the Prime Minister and Cabinet: Canberra.

Ungerer, C. (2010). Australia's National Security Institutions: reform and renewal, Special Report 34. Australian Strategic Policy Institute: Canberra.

LIST OF ACRONYMS AND TERMS

AGSVA	Australian Government Security Vetting Agency
AIC	Australian Intelligence Community
AIPIO	Australian Institute of Professional Intelligence Officers Inc
APS	Australian Public Service
ASPI	Australian Strategic Policy Institute
DNI	Director of National Intelligence
HUMINT	Human Intelligence
IBOK	Intelligence Body of Knowledge
ICT	Information and Communications Technology
IGIS	Inspector-General of Intelligence and Security
IIR	Independent Intelligence Review (2017)
NIC	National Intelligence Community
NIE	National Intelligence Enterprise
NSC	National Security Community
ONI	Office of National Intelligence
OSINT	Open Source Intelligence
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Scenario	A description of how the future may unfold according to an explicit, coherent, and internally consistent set of assumptions about key relationships and driving forces. The term 'scenario' was introduced by Herman Kahn in the 1950s in connection with military and strategic studies conducted by the Rand Corporation. Kahn used the term for issues related to US public policy, international development, and defence.
USIC	United States Intelligence Community
Wildcard	An early indication of a potentially important new event or emerging phenomenon that could become an merging pattern, a major driver, or the source of a new trend.

About AIPIO

Established in 1991, AIPIO is the peak representative body for the intelligence profession in Australia. Through leadership, advocacy, and innovation, AIPIO will advance the professionalisation of intelligence practice across all domains, ensuring the Institute remains relevant and attuned to the evolving nature of the intelligence professions, the needs of its members, and key stakeholders.

Author

Brett Peppler is the Managing Director of Intelligent Futures Pty Ltd, a management consulting practice providing intelligence-led approaches for managing uncertainty in strategic planning. Brett specialises in the creative application of strategic foresight to help clients frame and navigate complex strategic challenges. Brett has over 40 years of professional experience as an intelligence officer, and is a Fellow, Past President, and Life Member of AIPIO.

Acknowledgements

The author acknowledges contributions from John Schmidt, Travis Cunningham, Taylor Devlin, Riley Allen, and Kaitlyn Frazer.

Disclaimer

The Australian Institute of Professional Intelligence Officers (AIPIO) Inc does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select those vendors with favourable reviews or other designation. AIPIO research publications consist of the opinions of the authors and should not be construed as statements of fact. AIPIO disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Australian Institute of Professional Intelligence Officers (AIPIO)
Membership@aipio.asn.au | 1300 411 036
Web: aipio.asn.au

Annex B

Oversight arrangements in Five Eyes Countries compared

To enable a useful and detailed submission, AIPIO caused a comparative analysis of current oversight mechanisms of intelligence agencies in the Five Eye countries.

In a modern democracy it is essential intelligence agencies are subject to strong oversight and evaluation mechanisms. The oversight of intelligence agencies is a central part of the 'state of trust' between intelligence services and communities. A critical element of this 'state of trust' is that agencies are able to operate effectively to provide intelligence which contributes to the safeguarding of national interests and citizens in their country.[1] To balance the imperative accountability of intelligence agencies with the need to operate with a degree of secrecy, the oversight mechanisms in place need to ensure that those agencies act with propriety, legality, and are responsive and accountable for their activities.[2]

Current Oversight Mechanisms in Five Eye Countries

The intelligence communities and oversight framework in Australia, Canada, New Zealand, the United Kingdom and the United States have evolved to meet the needs of those countries and specific contexts in which they operate. In each country, there is a combination of executive, parliamentary/congressional, independent and judicial oversight in place.[3] For our purposes, there will be a focus on the parliamentary/congressional and independent oversight mechanisms.

Australia

The Australian Intelligence Community (AIC) is comprised of six agencies including Australian Secret Intelligence Service (ASIS), Australian Security Intelligence Organisation (ASIO), Defence Imagery and Geospatial Organisation (DIGO), Defence Intelligence Organisation (DIO), Defence Signals Directorate (DSD) and the Office of National Assessments (ONA). The AIC is part of the broader national security community including law enforcement, border protection and policy agencies.[4]

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Inspector-General of Intelligence and Security (IGIS) undertake complementary roles in the oversight of the AIC.[5]

The PJCIS oversight of the AIC includes:

- review the administration and expenditure of the AIC agencies, including their annual financial statements
- review any matter in relation to an AIC agency referred to it by the responsible minister or a House of Parliament and
- report its comments and recommendations to each House of Parliament and the responsible minister[6]

The IGIS provides independent oversight over the AIC operational activities by reviewing the agencies to ensure they act legally and with propriety, comply with ministerial guidelines and directives, and respect human rights.[7] These IGIS oversight functions include AIC agency inquiry functions, intelligence and security matter inquiry functions, AIC agency inspection functions and public interest disclosure functions.[8]

Canada

The National Security and Intelligence Committee of Parliamentarians (NSICOP) was created in 2017 as a committee of parliamentarians. NSICOP has a broad government mandate to provide oversight to the Canadian National Security and Intelligence Community (CNSIC) as a whole including at least 17 federal agencies.[9] The government body therefore can review any national security or intelligence matters including:

- the legislative, regulatory, policy, administrative and financial framework for national security and intelligence

---

[1] Commonwealth of Australia, 2017, p.111

[2] The Parliament of Australia, 2020, p. 2; Barker, C., Petrie, C., Dawson, J., Godec, S., Porteous, H., & Purser, P, 2017, p.9

[3] Barker et al., 2017, p. 9

[4] Commonwealth of Australia, 2017, p.46-47

[5] Barker et al., 2017, p. 12

[6] Intelligence Services Act 2001 (Australia), section 29; Commonwealth of Australia, 2017, p. 112

[7] Commonwealth of Australia, 2017, p. 114

[8] Inspector-General of Intelligence Act 1986 (Australia), section 8 & 9

[9] Barker et al., 2017, p. 36

- any activity carried out by a department that relates to national security or intelligence, unless the activity is an ongoing operation and the appropriate Minister determines that the review would be injurious to national security
- any matter relating to national security or intelligence that a minister of the Crown refers to the Committee[10]

The National Security and Intelligence Review Agency (NSIRA) was created in 2019 as an independent agency to review all national security and intelligence activities carried out by the Canadian Government. NSIRA has unrestricted access to classified information including any and all information held by, or under the control of departments and agencies.[11] The NSIRA has a statutory mandate to:

- review the activities of the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE)
- review any activity carried out by a department that relates to national security or intelligence
- review any matter that relates to national security or intelligence that a minister of the Crown refers to the Agency; and
- investigate complaints as well as the national security and intelligence activities of all other federal departments and agencies[12]

In practice, the NSICOP and NSIRA will complement each other and provide comprehensive and multi-faceted scrutiny over the Government's activities in all national security and intelligence matters.[13]

New Zealand

New Zealand has two intelligence and security agencies. The Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS).[14]

Parliamentary oversight of the two agencies policies, administration and expenditure is undertaken by the Intelligence and Security Committee (ISC). The functions of the ISC include:

- to examine the policy, administration and expenditure of each intelligence and security agency
- to consider any bill, petition or other matter in relation to an intelligence or security agency referred by the House of Representatives
- to receive and consider the annual reports of GCSB and NZSIS
- to conduct each year, following receipt of the annual report of the agencies, an annual review of the agencies
- to request the Inspector-General to conduct an inquiry into:
- any matter relating to an intelligence and security agency's compliance with New Zealand law, including human rights law
- the propriety of particular activities of an intelligence and security agency
- to consider any matter (not being a matter relating directly to the activities of an intelligence and security agency) referred to the Committee by the Prime Minister because of that matter's intelligence or security implications
- to consider and discuss with the Inspector-General his or her annual report[15]

The IGIS is a statutory officer providing independent external oversight and review of the intelligence and security agencies. The IGIS is responsible for reviewing issues of legality and propriety and provides an independent determination of complaints about GCSB and NZSIS conduct.[16] The Inspector-General's work involves:

- investigating complaints about the intelligence and security agencies
- conducting inquiries into the activities of the intelligence and security agencies
- reviewing all warrants and authorisations issued to the intelligence and security agencies
- reviewing the intelligence and security agencies' compliance procedures and systems, and
- receiving protected disclosures ('whistle-blower' disclosures) relating to classified information or the activities of the intelligence and security agencies[17]

---

[10] National Security and Intelligence Committee of Parliamentarians Act 2017 (Canada)

[11] Security Intelligence Review Committee, 2019

[12] National Security and Intelligence Review Act 2019 (Canada)

[13] Security Intelligence Review Committee, 2019

[14] New Zealand Intelligence Community, 2017

[15] Intelligence and Security Act 2017 (New Zealand), part 6; New Zealand Intelligence Community, 2017

[16] Inspector-General of Intelligence and Security, 2019; New Zealand Intelligence Community, 2017

[17] Intelligence and Security Act 2017 (New Zealand), part 6; Inspector-General of Intelligence and Security, 2019

United Kingdom

The Intelligence and Security Committee of Parliament (ISC) is the committee of Parliament with statutory responsibility for the oversight of the United Kingdom Intelligence Community (UKIC).[18] The function of the ISC is to examine the expenditure, administration, policy and operations of the UKIC which includes:

- MI5 (the Security Service)
- MI6 (the Secret Intelligence Service)
- GCHQ (Government Communications Headquarters)
- Defence Intelligence in the Ministry of Defence
- the Joint Intelligence Organisation (JIO) in the Cabinet Office
- the National Security Secretariat (NSS) in the Cabinet Office and
- the Office for Security and Counter terrorism (OSCT) in the Home Office[19]

The Investigatory Powers Commissioner (IPC) provides an independent oversight of the use of intrusive powers by the Agencies. By conducting robust, evidence-based inspections of the use of investigatory powers, the IPC ensures that those public bodies authorised to use investigatory powers are doing so lawfully and in line with best practice. In addition to its inspection duties, the IPC carries out ad hoc investigations into potential non-compliance. The Commissioner makes an annual report to the Prime Minister, which is then published and laid before Parliament.[20]

United States

The United States Intelligence Community (USIC) is comprised of 17 executive military and civilian intelligence-related entities including defence, signals, security and foreign intelligence, energy, drugs, diplomatic and financial intelligence.[21] The Congressional oversight refers to the responsibility of the legislative branch to monitor and indirectly supervise intelligence programs, agencies and policies.[22] The Congress's authority is ingrained in the Constitutions implied powers, and the necessary and proper clause.[23]

The Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) are the primary intelligence oversight bodies responsible for the review of the USIC.[24]

The US government-wide system employs Inspectors-General (IGs), which oversees specific intelligence agencies and an IG of the Intelligence Community with cross-agency jurisdiction[25]. The IGs for specific agencies and the IG of the Intelligence Community may conduct audits of, and investigations into, the programs and operations of agencies they oversee.[26]

The President's Intelligence Advisory Board (PIAB) and the Privacy and Civil Liberties Oversight Board (PCLOB) serve the President in an advisory capacity within the executive branch but employ external experts to ensure a degree of independence.[27]

The PIAB is responsible in reviewing the legality and propriety of intelligence activities, the Board advises the President on intelligence activities that the Board believes may be unlawful or contrary to Executive Order or Presidential Directive.[28]

The oversight functions of the PCLOB include continually reviewing the implementation of Executive Branch policies, procedures, regulations, and information-sharing practices relating to efforts to protect the nation from terrorism, in order to ensure that privacy and civil liberties are protected[29]. The advice functions include reviewing proposed legislation, regulations, and policies related to efforts to protect the nation from terrorism, the implementation of new and existing policies and legal authorities, in order to advise the President and Executive Branch agencies on ensuring that privacy and civil liberties are appropriately considered in their development and implementation.[30]

---

[18] Intelligence and Security Committee of Parliament, 2020

[19] Justice and Security Act 2013 (United Kingdom), part 1; Intelligence and Security Committee of Parliament, 2020

[20] Investigatory Powers Act 2016 (United Kingdom), part 8; Investigatory Powers Commissioner's Office, 2019

[21] Barker et al., 2017 p. 58

[22] Baker, J., 2008, p. 199-208

[23] Congressional Research Service, 2018, p.4)

[24] Office of the Directory of National Intelligence, 2020; Congressional Research Service, 2018, p. 4

[25] Office of the Directory of National Intelligence, 2020

[26] Barker et al., 2017, p. 66

[27] President's Intelligence Advisory Board, 2020; Privacy and Civil Liberties Oversight Board, 2020

[28] President's Intelligence Advisory Board, 2020; Officer of the Director of National Intelligence, 2020

[29] Privacy and Civil Liberties Oversight Board, 2020

[30] Office of the Directory of National Intelligence, 2020; Baker, 2008, p. 199-208

Comparative Analysis of Five Eye Countries

Despite differences in the oversight mechanisms taken by the Five Eye countries, each of the countries has developed a framework that includes checks and balances that spans over branches of government and independent reviews. Each of these mechanisms aim to ensure that the intelligence agencies are accountable for both their administration and expenditure, and the legality and propriety of their activities.[31]

Jurisdiction of Oversight Mechanisms

The Jurisdiction and mandate of almost all the intelligence agencies in the Five Eye countries are now largely governed by statute. Legislation to put intelligence agencies on a statutory footing ensure that the existence and work of agencies is subject to parliamentary/congressional debate.[32] However, the key parliamentary/congressional committees and independent oversight differ on whether their mandate is based around specific agencies or specific activities as can be seen in Table One.[33]

Table 1: Oversight mechanisms jurisdictions

	Parliamentary/congressional	Independent
Australia	PJCIS: limited matters relating to AIC agencies	IGIS: all AIC agencies
Canada	NSICOP: activities relating to National Security or Intelligence	NISRA: all CNSIC agencies
New Zealand	ISC: NZSIS and GCSB excluding operational activity	IGIS: limited to matters relating to the NZSIS and GCSB
United Kingdom	ISC: all UKIC agencies as agreed upon with Prime Minister	IPC: statutory function, direction by Prime Minister
United States	Congress, under the advisement of SSCI and HPSCI: all USIC agencies	IG, PCLOB and PIAB: all USIC agencies

Basing mandates around specific activities means that it automatically keeps pace if additional agencies become involved in those activities. However, this also means that the oversight body cannot look deeply at the way an agency operates broadly.[34]

Basing mandates around specific agencies allows the oversight bodies to scrutinise the full range of operations by agencies but can also means the jurisdiction to examine issues that extends beyond those agencies is limited.[35]

Parliamentary/Congressional Oversight

The US was the first country of the five to establish a separate committee that focused solely on intelligence related activities. The establishment of the SSCI and the HPSCI had the purpose to better integrate the interests, responsibilities and depth of intelligence expertise and respond to the limited accountability of certain intelligence agencies. While each of the relevant committees has some limits on what they may examine, there are no official limits on what these committees, taken collectively, may inquire into in terms of the intelligence-related activities of the US Government.[36]

The UK ISC was originally set up to cover MI5, MI6 and GCHQ with a relatively limited mandate to oversee the expenditure, administration and policy. However, since the 2013 reform of the Justice and Security Act, the United Kingdom made the ISC a Committee of Parliament with a broadened mandate covering organisational and functional oversight of all agencies and departments. The UK ISC now has the power to examine the intelligence activity on a wider range including the Ministry of Defence, the Cabinet office and the Home office.[37]

The Australian, New Zealand and Canada parliamentary oversight have established similar committees by the way of statue however they have a more limited mandate than the UK ISC and the US Congress as noted above.

In Australia, the PJCIS was expanded by legislation in 2001 and 2005 so that the oversight role encompasses six agencies responsible for intelligence activities. Following the 2017 Independent Intelligence review, it is recommended that oversight should be extended to

---

[31] Barker et al., 2017, p.2

[32] Defty, A., 2020, p. 368

[33] Table 1 adapted from Barker et al., 2017, p. 59-61

[34] Barker et al., 2017, p. 59-60; Defty, A., 2020, p. 375

[35] Barker et al., 2017, p. 59-60; Defty, A., 2020, p. 375

[36] Congressional Research Service, 2018, p. 4; Office of the Director of National Intelligence, 2020; Barker et al., 2017, p. 63-64

[37] Defty, A., 2020, p. 376; Barker et al., 2017, p.50

encompass up to ten agencies.[38] However, PJCIS is limited to reviewing only the administration and expenditure of the intelligence agencies, with an extensive list of areas that the PJCIS may not inquire.[39]

In New Zealand, the ISC is permitted to review the administration, expenditure and policies of the NZSIS and GCSB, among other matters referred by parliament or Prime Minister. The ISC is however not permitted to review any operational matters of the agencies.[40]

In Canada, NSICOP mandate does not refer specifically to any intelligence or security agency but refers to the CNSIC as a whole. NSICOP has the powers to review in relation to policy, administration and expenditure of the CNSIC, mimicking those oversights by the ISC in New Zealand. NSICOP can review any activity carried out by an agency or department that relates to national security or intelligence unless the activity is an ongoing operation, similar to the UK ISC. However, NSICOP is a committee of parliamentarians and remain part of the Executive.[41]

Independent Oversight

In Australian and New Zealand, the independent oversight is carried out by the IGIS, while the United Kingdom has the IPC and Canada has NSIRA. The US has a government wide system of IG and two boards to form independent oversight.

The IGIS in Australia and New Zealand share a similar mandate. The IGIS is responsible for reviewing the operational activities of their intelligence agencies to ensure those agencies act with propriety and legality. They are empowered by their mandates to conduct inquires and carry out inspections. Given the relatively strict limitation on parliamentary oversight in Australia and New Zealand, the IGIS play a vital role in holding agencies accountable.[42]

The UK IPC differs from the IGIS in Australia and New Zealand as the IPC is mandated to review certain statutory function as opposed to reviewing the general activities of intelligence agencies. The IPC specifically may audit, inspect and investigate communications, acquisition and retention of communication data, equipment interference, as well as the acquisition, retention and use of bulk datasets.[43]

In Canada, prior to NSIRA, only specific agencies had independent expert review bodies, and these bodies could not collaborate or share classified information. The NSIRA, by contrast, is mandated to review all Government of Canada national security and intelligence activities in an integrated manner, without regard for the department or agency the activities fall under.[44]

In the US, IGs for specific agencies and the IG of the Intelligence Community may conduct audits of, and investigations into, the programs and operations of agencies they oversee. The PIAB oversees the US intelligence community's compliance with applicable laws, Executive Orders and Presidential Directives, while the PCLOB is tasked with ensuring 'that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.[45]

Conclusion

This comparative analysis demonstrates the current oversight mechanisms in place throughout the Five Eye countries intelligence communities and compares the parliamentary/congressional and independent oversight. The oversight mechanisms reflect each of the nation's political structure and therefore differ across areas. However, all countries include a system of checks and balances that ensure intelligence agencies and departments are accountable for their administration and expenditure, and the legality and propriety of their activities.

---

[38] Commonwealth of Australia, 2017, p. 113

[39] Defty, A., 2020, p. 376

[40] Barker et al., 2017, p. 64; Defty, A., 2020, p. 376

[41] Security Intelligence Review Committee, 2019; Defty, A., 2020, p. 376; Barker et al., 2017, p. 64

[42] Barker et al., 2017, p. 66

[43] Intelligence and Security Committee of Parliament, 2020; Barker et al., 2017, p. 66-67

[44] Security Intelligence Review Committee, 2019; Barker et al., 2017, p. 67

[45] President's Intelligence Advisory Board, 2020; Privacy and Civil Liberties Board, 2020; Barker et al., 2017, p. 66

References

Baker, J. (2008). Intelligence oversight. *Harvard Journal on Legislation*, *45*(1), 199–208.

Barker, C., Petrie, C., Dawson, J., Godec, S., Porteous, H., & Purser, P. (2017). Oversight of intelligence agencies: a comparison of the 'five eyes' nations. Parliamentary Library. https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/Others/PDF/ISSN_2203-5249-e.pdf

Commonwealth of Australia. (2017). *2017 Independent intelligence review.* Department of the Prime Minister and Cabinet. https://www.pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf

Congressional Research Service. (2018). *Congressional oversight of intelligence: background and selected options for further reform.* CRS Report for Members and Committees of Congress. https://fas.org/sgp/crs/intel/R45421.pdf

Defty, A. (2020) From committees of parliamentarians to parliamentary committees: comparing intelligence oversight reform in Australia, Canada, New Zealand and the UK. *Intelligence and National Security*, *35*(3), 367-384, https://doi.org/10.1080/02684527.2020.1732646

Inspector-General of Intelligence Act 1986 (Australia)

Inspector-General of Intelligence and Security. (2019). *About IGIS.* Retrieved April 8, 2020, from http://www.igis.govt.nz/about/

Intelligence and Security Act 2017 (New Zealand)

Intelligence and Security Committee of Parliament. (2020). *How the committee works.* Retrieved April 8, 2020, from http://isc.independent.gov.uk/how-the-committee-works

Intelligence Services Act 2001 (Australia)

Investigatory Powers Act 2016 (United Kingdom)

Investigatory Powers Commissioner's Office. (2019). *IPC what we do.* Retrieved April 8, 2020, from https://www.ipco.org.uk/

Justice and Security Act 2013 (United Kingdom)

National Security and Intelligence Committee of Parliamentarians Act 2017 (Canada)

National Security and Intelligence Review Act 2019 (Canada)

New Zealand Intelligence Community. (2017). *Oversight.* Retrieved April 8, 2020, from https://www.nzic.govt.nz/oversight/#

Office of the Director of National Intelligence. (2020). *Oversight and partners.* Retrieved April 8, 2020, from https://www.intelligence.gov/how-the-ic-works#oversight

President's Intelligence Advisory Board. (2020). *Intelligence oversight and advisory board.* Retrieved April 8, 2020, from https://www.whitehouse.gov/piab/

Privacy and Civil Liberties Oversight Board. (2020) *What is the privacy and civil liberties oversight board?* Retrieved April 8, 2020, from https://www.pclob.gov/about/

Security Intelligence Review Committee. (2019). *All government of Canada national security and intelligence activities now subject to independent expert review.* News Wire. https://www.newswire.ca/news-releases/all-government-of-canada-national-security-and-intelligence-activities-now-subject-to-independent-expert-review-858523391.html

The Parliament of Australia. (2020). Intelligence and security legislation amendment (implementing independent intelligence review) bill 2020 explanatory memorandum. https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fs1256_ems_a99cd29d-5571-45ea-b5d6-c9e30ed67d8c%22