A Comparison of Australian and Thai National Intelligence Accountability Frameworks

By

Colonel Stephen Fomiatti
Australian Defence Attaché to the Kingdom of Thailand
Australian Defence Force

Student of the National Defence College
The National Defence Course : Class 62
Academic Year 2019-2020

Certificate of Research Paper

National Defence College. National Defence Studies Institute has approved Colonel Stephen Fomiatti' s the individual research paper titled “A Comparison of Australian and Thai National Intelligence Accountability Frameworks” as a subject in the field of Strategy, and as part of the study of the College curriculum Class 62 Academic year 2019 – 2020

Lt.Gen.

(Pisan Pathom-ame)
Superintendent
National Defence College

Abstract

Title : A Comparison of Australian and Thai National Intelligence Accountability Frameworks

Field : Strategy

Name : Colonel Stephen Fomiatti, Australian Army

Course : NDC **Class :** 62

As part of a more general trend in government, greater degrees of scrutiny and oversight in corporate governance and accountability have developed within the Australian National Intelligence Community (NIC), along with increased attention to citizen rights. The continuum of accountability relationships developed between the public, the Parliament, the Government and the various agencies of the NIC has resulted in a high degree of transparency in NIC activities, ensuring agencies act legally and with propriety, comply with ministerial guidelines and respect human rights.

Thailand's recent political history has been rather more unsettled than Australia's, with coups in 2006 and 2014. This has led to periods of military government and internal instability, a situation that doesn't necessarily lend itself to increased transparency and enhanced accountability. Thai support for security sector reform has traditionally been temporary and poorly organised, and there are no Thai civil society groups who regularly monitor the agencies of the Thai Intelligence Community (TIC).

This is not to say however, that all NIC and TIC activity is, should or must be conducted completely in the open. The purpose of secrecy is to facilitate the proper functioning of government, but it needs to be

balanced against other competing public interests including the public's right to know. It is the role of both internal and external accountability frameworks to ensure this balance is maintained, minimising community apprehension pertaining to national intelligence activities and damage to the trust relationship between the Government and its constituency.

The internal accountability framework residing within the Australian governmental departments that NIC agencies belong to is implemented on three levels: individual, committee and organisational. External accountability is implemented through legislation; the Parliamentary Joint Committee on Intelligence and Security; committees of Cabinet including the National Security Committee of Cabinet and the Secretaries' Committee on National Security; courts, tribunals and ombudsmen; and an oversight body in the Inspector General of Intelligence and Security.

As in other regional countries, several Government departments and the military control TIC agency operations. Although TIC agencies prioritise operational effectiveness and the maintenance of national security over being held accountable to the public, there are clear accountability frameworks in place that are similar in nature to the Australian intelligence accountability system, both internal and external, if not as well defined as the Australian system. Internal accountability is implemented through clear and unambiguous command and control structures, with their responsibilities and obligations detailed by legal and regulatory contexts. External accountability is implemented through legislation; parliamentary committees and commissions; courts, tribunals and ombudsmen.

A comparative analysis of the two accountability frameworks reveals scope for enhancement of the Thai system through clearly defining and implementing the intelligence accountability framework, strengthening it through broader organisational remits and the establishment of an independent oversight body, publicising the system and developing it further over time.

Preface

During my thirty years of service in the Australian Army, mostly as an intelligence officer, I have witnessed significant change in the natures of society, democracy, government and national security, both in Australia and abroad. The nature and use of intelligence, too, has undergone much transformation in this period. Much of the work I have done has been done in secret with restrictive caveats on sourcing, sharing and using information to achieve tangible outcomes in support of the objectives of the Government of the day. Reconciling this work with democratic ideals, although sometimes difficult, has actually become easier and less ambiguous over time with the development and implementation of a robust accountability framework governing the work of Australia's intelligence agencies.

At the same time, Australian public trust in, and understanding of our intelligence agencies and their work has improved remarkably. The benefits derived from this support should not be understated. I have felt it provides me a solid mandate to undertake my work, sometimes distasteful, with the backing of the people I am ostensibly working for – the Australian public. Although Thailand and Australia have very different cultures and systems of government, and the nature of our geopolitical circumstances sometimes demand divergent approaches to national security, I believe there is significant upside in doing so with the backing of those whom we indirectly serve: the general public.

To that end, my hope is that this paper assists in facilitating change that helps develop greater public trust in Thailand's intelligence system, while at the same time enhancing the capability of Thailand's national security apparatus.

Colonel Stephen Fomiatti
Student of National Defence College
Course NDC Class 62

Acknowledgement

I would like to acknowledge the amazing opportunity provided to me as only the second Australian to attend Thailand’s National Defence College. The friendships and professional relationships I have made and developed during my time here will remain with me for the rest of my life. At the beginning of the course, both the Superintendent and the Deputy Superintendent said to me about being a student at National Defence College : “Pii Joey, you will never walk alone”. This resonated very closely with me, and has been borne out in practice throughout my time at the College. It is clearly one of the major strengths and benefits of being a student at this institution.

The distinguished staff at National Defence College have been a constant source of inspiration for me, in addition to providing me much needed guidance and assistance on a regular basis. Thanks to their patience and demeanour, I have never felt like an international student on course, and have been afforded the flexibility to work around the demands of my Attaché obligations and responsibilities. I wish to thank them all for their leadership, support, adaptability and collegiate approach.

Many people assisted me in production of this paper, and I thank each and every one of them. In particular, I would like to single out Lieutenant General Nopadon Mungdalaton who provided the direction, drive and academic support when I most needed it. Colonel Akradej Prateapusanond and Lieutenant Colonel Chalermpol Saributra helped me with academic guidance and direction that was also very much appreciated. And clearly, a huge thank you goes to those wonderful people who provided their time and open hearts to assist me with interviews, discussions, conversations and questions on the sometimes-tricky subject matter. I would like to especially thank Lieutenant General Natee Wongissares, Director of Joint Intelligence, Royal Thai Armed Forces; Lieutenant General Wichai Chucherd, Director General, Armed Forces Security Centre, Royal Thai Armed Forces; Lieutenant General Terdsak Dumkhum, Director General of Intelligence, Royal Thai Army; Air Marshal Punpakdee Pattanakul, Director of Intelligence, Royal Thai Air Force; Vice Admiral Wuttichai Saisatien, Director General, Naval Intelligence Department, Royal Thai Navy; Police Major General Saksira Pheuak-um, Deputy Commissioner Royal Thai Police Special Branch Bureau; Mr Krissada Aksornsong, Director Counter-Terrorism and Trans-National Crime, National Intelligence Agency, and Major General Pongtep Gaewchaiyo, Deputy Director General Border Affairs, Royal Thai Armed Forces.

A big thank you also goes to the Australian Ambassador to the Kingdom of Thailand, His Excellency Mr Allan McKinnon PSM, who took the time and exercised the necessary patience to advise me on this paper. As former Australian National Security Advisor, he has significant expertise in this area and was also responsible for the creation and development of Australia's National Intelligence Community in its current guise.

And finally, I wish to acknowledge my fellow course mates in Class 62 who have been simply incredible. They are an amazing set of people with whom I have had the great honour and pleasure to serve alongside. It is an absolute privilege to count them all as my friends, who never once, let me walk alone.

Colonel Stephen Fomiatti
Student of National Defence College
Course NDC Class 62

Contents

Contents (cont.)

Contents (cont.)

List of Figures

List of Figures (cont.)

Figure No. **Page**

List of Abbreviations

National Intelligence	ONI
Australian Secret Intelligence Service	ASIS
Australian Security Intelligence Organisation	ASIO
Defence Intelligence Organisation	DIO
Australian Signals Directorate	ASD
Australian Geospatial-Intelligence Organisation	AGO)
Australian Criminal Intelligence Commission	ACIC
Australian Federal Police	AFP
Australian Transaction Reports and Analysis Centre	AUSTRAC
Australian Intelligence Community	AIC
National Intelligence Agency	NIA
Armed Forces Security Centre	AFSC
Intelligence Divisions of the Royal Thai Armed Forces	RTArF
Royal Thai Army	RTA
Royal Thai Navy	RTN
Royal Thai Air Force	RTAF
Royal Thai Police Special Branch Bureau	RTPSBB

List of Tables

Chapter 1
Introduction

Background and Significance of Problem

Australia is a society characterised by strong notions of individual freedom and personal rights. With the advent and proliferation of social media in particular, its citizens today are probably more conscious of their rights than at any time in the past. The past 30 years has seen significant reform designed to enhance governance and accountability practices of the Government, its departments and agencies at the Federal level. This has had significant ramifications for Australia's National Intelligence Community (NIC) in particular. As part of a more general trend in government, greater degrees of scrutiny and oversight in corporate governance and accountability have developed within the NIC, along with increased attention to citizen rights. The continuum of accountability relationships developed between the public, the Parliament, the Government and the various agencies of the NIC has resulted in a high degree of transparency in NIC activities, ensuring agencies act legally and with propriety, comply with ministerial guidelines and respect human rights.

This is not to say however, that all NIC activity is, should or must be conducted completely in the open. The purpose of secrecy is to facilitate the proper functioning of government, but it needs to be balanced against other competing public interests including the public's right to know. It is the role of accountability frameworks to ensure this balance is maintained, minimising community apprehension pertaining to NIC activities and damage to the trust relationship between the Government and its constituency.

Perhaps the most difficult aspect of this accountability framework is reconciling democratic practices with maintaining organisations that necessarily work in secrecy. Balancing the concepts of ‘need to know’ and ‘right to know’ is central to the NIC accountability framework, which itself is the cornerstone to reconciling secrecy with democratic principles. Would such a framework be useful or successful in Thailand, a very different kind of political entity to Australia, but one which shares similar concerns and faces common challenges within the context of rapid regional geo-strategic change?

Given this context, it is appropriate to examine the apparent paradox of secrecy within a democratic society and explore how in Australia, a multi-faceted accountability framework has been designed to overcome this to the satisfaction of both the Government and the public. Furthermore, and despite significant institutional and architectural differences between Australia’s and Thailand’s national intelligence frameworks, it is interesting to examine which parts, if any, of the Australian intelligence accountability framework may contain useful insights for Thailand’s various intelligence agencies and the Government departments / institutions / entities to whom they necessarily answer. This is particularly so in light of the April 2019 publication of Thailand’s new National Intelligence Act and its impact on the Thai National Intelligence Strategy (2015-22).

Objectives of Research

The need to strike a balance between national security and human security is laying at the centre of the subject. Here is where 'accountability' comes in as an essential principle of security force's operations. However, different cultures may not have identical views of accountability; in many cases, these views are diverse, similar in concept to individual nations' approaches to the concept of 'human rights'. The concept of accountability will be discussed, as will its place as a practical norm in the Australian National Intelligence Community. The paper outlines the Australian 'accountability' structure within its legal framework, explains what its objective is and how it works in detail. It examines the role of oversight agencies, Parliamentary committees and ombudsmen in ensuring intelligence agencies in Australia maintain an appropriate balance between the public's right to know and the need of such agencies to maintain appropriate levels of security. It addresses intelligence oversight in an Australian setting within the context of extant legislation. As Australia's principal oversight body for NIC activity, the Inspector General of Intelligence and Security (IGIS) is explored in depth to provide a further degree of clarity and understanding in this regard.

This research will also examine the NIC's equivalent agencies in Thailand, their intelligence oversight mechanisms and discusses these within the context of security sector reform and governance, specifically the concepts of civil supremacy, rule of law, accountability and effectiveness. Finally, it will compare the two systems and identify elements of Australia's system able to be reconciled with Thailand's national context. It summarises the paper's findings and recommends elements of Australia's system that may be considered for adoption, in whole or in part, in Thailand over time.

Specific objectives of this research paper are to :

1. **study** concepts pertinent to intelligence accountability to provide a degree of context for the research (chapter 3);

2. **describe** the Australian system of intelligence accountability, both internal and external, through the use of intra-departmental governance and accountability practices, relevant legislation, Parliamentary committees, committees of Cabinet, courts, tribunals, ombudsmen and oversight agencies (chapter 4);

3. **describe** the current Thai system of intelligence accountability for NIC-equivalent agencies in a similar manner to that done for the Australian system (chapter 5); and

4. **compare** the two frameworks and **recommend** potential enhancements for Thailand's national intelligence accountability framework (chapter 6).

Scope of Research

The scope of research will comprise an examination of existing literature with findings and recommendations based on analysis of this material and the Australian National Intelligence Community experience of the author. In support of this will be interviews with a range of experienced Thai intelligence practitioners and the heads of various Thai intelligence agencies regarding their experiences with intelligence accountability and potential scope for further development of this issue in the Thai framework. Data for this paper was sourced over the period December 2019 to July 2020 (secondary data), with interviews conducted in May, June and July 2020 (primary data).

Methodology

This research is a qualitative research, conducted by gathering relevant data, researching literature pertinent to intelligence accountability concepts and the actual accountability frameworks themselves, the experience and knowledge of the author from working in the Australian National Intelligence Community, and the information obtained from interviews with representatives from Thai intelligence community. The primary methodology utilised in addressing the research objectives is necessarily descriptive and analytical in nature – first setting the scene through examining the apparent paradox of secrecy within a democratic society; followed by describing the current Australian National Intelligence Community accountability framework and where it came from; detailing observations from analysis of current pertinent literature and legislation; and discussing case studies of intelligence accountability within the Australian context. From this examination of the Australian setting, expert points of view from Thai Intelligence Community helped shape understanding of the Thai context. This data was then analysed and the two systems compared in order to obtain recommendations for development for the TIC's intelligence accountability framework.

Limitations and Delimitations

Limitations:

1. Classification. This paper is written at the unclassified level. Much data and information exist at the Australian and Thai classified level or individual agencies' respective levels of security classification. This data, however, is unavailable for the conduct of this analysis.

2. Australian scope. This paper will only consider the accountability framework for the NIC comprising the six traditional intelligence agencies that formally made up the Australian Intelligence Community (AIC) - the Office of National Intelligence (ONI), the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO), and the Defence intelligence agencies consisting of the Defence Intelligence Organisation (DIO), the Australian Signals Directorate (ASD) and the Australian Geospatial-Intelligence Organisation (AGO). The other four agencies that currently make up the NIC : the Australian Criminal Intelligence Commission (ACIC) and the intelligence functions of the Australian Federal Police (AFP), Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Department of Home Affairs, are beyond the scope of this paper. Accountability frameworks for other Australian Government intelligence bodies, intra-departmental and private intelligence sources and agencies are considered beyond the remit of this paper.

3. Thai scope. From the Thai perspective, this paper will only consider intelligence agencies with approximate NIC equivalence. Security agencies and organisations are beyond the scope of this paper. Operational, tactical, intra-departmental and private intelligence sources and agencies are likewise not considered. To that end, for the purposes of this paper, the following Thai organisations and agencies will be considered the ‘Thai Intelligence Community (TIC)’ from an accountability framework perspective :

3.1 the National Intelligence Agency (NIA),

3.2 the Armed Forces Security Centre (AFSC), 3.3 the Intelligence Divisions of the Royal Thai Armed Forces (RTArF), Royal Thai Army (RTA), Royal Thai Navy (RTN) and the Royal Thai Air Force (RTAF), and

3.4 the Royal Thai Police Special Branch Bureau (RTPSBB).

4. Assumed knowledge. A working knowledge of the roles and tasks, characteristics, organisation, capabilities and limitations of the above agencies is assumed. Additionally, an understanding of the structure and workings of Australian federal government departments is assumed. In fact, they don't differ all that much from their equivalents in Thailand.

5. Nomenclature. This paper refers to agencies and departments by their current names (as of 2020) and does not use historical nomenclature except when required for purposes of clarity.

6. Access to Thai sources and agencies. Related to classification limitations, access to Thai sources and agencies related to intelligence is restricted. The resultant knowledge gaps are necessarily mitigated through assumptions and extrapolation. The nature of the topic is a closed subject under legal restrictions in Thailand so that the sources of official information could not be disclosed nor elaborated in details; and literature on this topic has not been widely available except unclassified information which limits a more in-depth investigation and analysis. That said, the Thai intelligence agencies have been extremely generous with their time and access, as evidenced by interviews conducted for this paper with the directors and staff of each of the military intelligence agencies, access to senior National Intelligence Agency staff and the Deputy Commissioner of the Royal Thai Police Special Branch Bureau.

7. COVID 19 Restrictions. During the research for and writing of this paper, the COVID 19 pandemic struck around the world, forcing many agencies to shut down or severely limit services. Additionally, the limits placed on meetings and social interactions have negatively impacted the extensive interview program with Thai subject matter experts planned for this paper. However, several interviews were able to be conducted both face to face and by using virtual means such as video calls or through social media chats. Although not the same as face to face interviews, video interviews and social media discussions have proved to be an adequate means of obtaining insight into issues pertaining to oversight and accountability in Thailand.

8. Finally, discussion of this issue is closely linked with the concepts of Security Sector Governance (SSG) and Security Sector Reform (SSR). However, an extensive review of SSG and SSR in Thailand is beyond the scope of this paper. Any discussion of these topics is contextual in nature only.

Research Results for Utilisation

This examination of the Australian and Thai intelligence accountability frameworks aims to highlight the differences between Australia's and Thailand's national intelligence accountability architecture and provide useful insights for the continued development of Thailand's National Intelligence Strategy. Over time, these insights may be able to be used to:

1. reduce the organisational insulation created by 'stovepipe effect' in intelligence oversight in Thailand (enhancing efficiency and therefore effectiveness),

2. develop a central agency responsible to parliament for detailed intelligence oversight and accountability of the TIC (creating a degree of consistency currently lacking in the Thai system), and

3.increase transparency of intelligence agencies for the public (within practical, operational and security limitations) thereby increasing the level of trust in government and public support for the national intelligence institutions from their current levels.

Definitions

Accountability means is defined in the Macquarie Dictionary as 'liable to be called to account; responsible (to a person, for an act, etc.)'[1]. Accountability is one of the core concepts in a democratic order. Accountability means to have an obligation to explain and justify one's actions. When referred to in this paper, it is within the context of 'intelligence accountability' whereby a nation's intelligence system and agencies are bound by legal and regulatory frameworks and subject to scrutiny to ensure appropriateness of actions, methods and outcomes.

[1] Delbridge, A., Bernard, J.R.L., Blair, D., Butler, S., Peters, P., and Yallop, C., (eds), 1997, The Macquarie Dictionary, 3rd Edition, The Macquarie Library Pty Ltd, Sydney, p 13.

Transparency means it is defined in the Cambridge Dictionary as 'the quality of being done in an open way without secrets'[2]. In the intelligence context where secrets are a huge part of daily business, transparency refers to operating in such a way that it is easy for others to see what actions are performed and for what purposes (within the limits of national security). Transparency implies openness, communication, and accountability.

Public Sector Governance

means Public Sector Governance is 'the process by which organisations are directed, controlled and held to account. It encompasses authority, accountability, stewardship, leadership, direction and control exercised in the organisation'.[3]

Security Sector Governance

Means Security sector governance (SSG) refers to the 'process by which accountable security institutions transparently supply security as a public good via transparent policies and

[2] https://www.dictionary.cambridge.org/dictionary/english/transparent

[3] Australian National Audit Office, 1999, Corporate Governance in Commonwealth Authorities and Companies, Commonwealth of Australia, Canberra, p1.

practices. Security sector governance reinforces the rule of law'[4]. It is a subset of public sector governance and describes how the principles of good governance apply to public security provision.

Security Sector Reform

Means Security sector reform (SSR) is the process by which 'security institutions are subordinated to oversight mechanisms, vetting, and lustration in order to deliver transparent and accountable public services as a public good'[5].

Signals Intelligence (SIGINT)

means Signals intelligence is intelligence gained through the interception of signals, whether communications between people or from electronic signals not directly used in communication[6].

[4] Geneva Centre for Security Sector Governance website accessed via the internet on 19 January 2020 at https://www.issat.dcaf.ch/Learn/SSR-Overview

[5] ibid.

[6] https://www.en.wikipedia.org/wiki/Signals_intelligence

Imagery Intelligence (IMINT)

means Imagery intelligence is an intelligence gathering discipline which collects and processes information via satellite, aerial and other photography or image capture[7].

Human Intelligence (HUMINT)

means Human intelligence is intelligence gathered by means of interpersonal contact, as opposed to the more technical intelligence gathering disciplines such as signals intelligence and imagery intelligence[8].

[7] https://www.en.wikipedia.org/wiki/Imagery_intelligence

[8] https://www.en.wikipedia.org/wiki/Human_intelligence_(intelligence_gathering)

Chapter 2
Related Literature Review

Over the last thirty years, quite a bit has been written in Western academia about the nature of intelligence and its accountability to the governments it serves. This is not necessarily the case in other nations where systems of government and governance, and indeed the nature of national intelligence systems and organisations, differ significantly from those in the West. One could almost say this is a direct reflection of the need for accountability and oversight in Western liberal democracies, and the exact opposite in many other societies. This paper examines the concepts of reconciling secrecy with democracy, and the nature of accountability in the intelligence context. It moves from concepts to implementation and looks at both the Australian NIC and the Thai Intelligence Community and the nature and structure of their accountability systems, the latter taking into account the influence of security sector governance and reform.

From the Western perspective on intelligence accountability concepts, Thompson (1987) explores the fundamental paradox of intelligence work within democratic systems, and suggests three key methods for reconciling secrecy with democracy that remain extant to this day (retrospection, generalisation and mediation)[1]. These concepts are widely practiced in the West, although to varying degrees and with variable degrees of success. Cimbala (1987) also explores the reconciliation of

[1] Thompson, D., 1987, Political Ethics and Public Office, Harvard University Press, Harvard, p 24.

intelligence in democracies, helping to further define the context for this paper[2]. Mendel (1999) explored the concept of balancing principles of 'right to know' versus 'need to know', which effectively drives the paradox, competing tensions and vast differences in intelligence accountability regimes across the world[3]. McComas (2002) got to the heart of the issue in asking 'who will guard the guardians?'[4]

Dubnick (1998) lays out the four pillars of accountability (legal, organisational, professional and political) that are largely accepted in the West today, and certainly underpin Australia's national intelligence accountability framework[5]. These four pillars form the basis by which the intelligence accountability frameworks of Australia and Thailand can be broadly compared. Born and Leigh (2007) provide an excellent overview specifically focused on accountability of Western intelligence agencies, although they consider three pillars (executive oversight, parliamentary

[2] Cimbala, S., 1987, Intelligence and Intelligence Policy in a Democratic Society, Transnational Publishers Inc., New York.

[3] Mendel, T., 1999, The Public's Right to Know: Principles on Freedom of Information Legislation, accessed via the internet on 19 January 2020 at https://www.article19.org/data/files/pdfs/standards/righttoknow.pdf.

[4] McComas, H., 2002, 'Quis custodies custodiet?' Who Will Guard the Guardians? Accountability in Intelligence, The Journal of the Australian Institute of Professional Intelligence Officers, Vol. 10, No. 2, 2002, AIPIO, Canberra.

[5] Dubnick, M., 1998, 'Clarifying Accountability – An Ethical Framework' in Sampford, C. and Preston, N. (eds), Public Sector Ethics, The Federation Press, Sydney, p 77.

oversight and oversight by independent bodies) as opposed to Dubnick's four. In line with virtually all western writing on the topic, the concept of oversight is seen as a means of ensuring the accountability of the decisions and actions of security and intelligence agencies[6].

From the Thai perspective on intelligence accountability concepts, the majority of literature related to intelligence accountability and oversight pertains to Security Sector Governance and Reform (SSG/SSR). SSG/SSR themselves have been written about *ad nauseum*, with definitive sources including the Geneva Centre for Security Sector Governance[7] and Geneva Centre for the Democratic Control of Armed Forces[8]. In the literature, Thai perspectives on SSG/SSR seem to have fallen away in recent years, although in the past, these issues and their relevance to Thailand and its system of government were frequently discussed. Despite not being Thai, Paul Chambers has been one of the more vocal contributors covering the issue in Thailand. In 2014, he wrote that 'The May 22, 2014 coup marked the death knell to any possible

[6] Born, H. and Leigh, B., 2007, Democratic Accountability of Intelligence Services, Policy Paper No. 19, Geneva Centre for the Democratic Control of Armed Forces, Geneva.

[7] Geneva Centre for Security Sector Governance website accessed via the internet on 19 January 2020 at https://www.issat.dcaf.ch/Learn/SSR-Overview

[8] Karkoszka, A., 2003, The Concept of Security Sector Reform, Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva, accessed via the internet on 19 January 2020 at https://www.un.org/ruleoflaw/files/Karkoszka.pdf

progress toward security sector reform in Thailand'[9]. He covers the history of SSR in Thailand in depth[10] and bemoans the Thai security sector's lack of transparency and accountability under ostensibly civilian-created rule of law[11]. His arguments are supported by Kocak and Kode (2014) in discussing systemic and political obstacles to SSR in Thailand[12].

With regards to Thai authors and writers, most seem to agree with Chambers, Kocak and Kode. Chongkittavorn (2016) called for a revamp of Thai intelligence agencies[13] through SSR, although the article mostly discussed the effectiveness of Thai operational intelligence rather than accountability issues. Various Prachathi articles source multiple Thai authors in calling for what is effectively a rather extreme version of SSR

[9] Chambers, P., 2014, A Dearth of Demilitarization, Centre for Security Governance, accessed via the internet on 19 January 2020 at https://secgovcentre.org/2014/07/32847/

[10] Chambers, P., 2016, Civil-Military Relations in Thailand since the 2014 Coup: The Tragedy of Security Sector "Deform", Peace Research Institute, Frankfurt, accessed via the internet on 19 January 2020 at https://www.jstor.org/stable/resrep14467.7

[11] Chambers, P., 2014, op cit.

[12] Kocak D., and Kode J., 2014, 'Impediments to Security Sector Reform' in Thailand in Heiduk F. (ed), Security Sector Reform in Southeast Asia, Critical Studies of the Asia Pacific Series, Palgrave Macmillan, London.

[13] Chongkittavorn, K., 2016, Thai Intelligence Agencies Need a Revamp, accessed via the internet on 20 January 2020 at https://www.nationthailand.com/opinion/30276574

in Thailand[14]. Essentially, despite a plethora of literature on SSG/SSR in Thailand by both Western and Thai writers, there appears to be only limited in depth direct analysis of Thailand's national intelligence agencies and their specific accountability frameworks.

Having looked at the background and context of intelligence accountability, attention is then turned to the Australian NIC and the TIC, and examining the intelligence accountability systems of each. Literature pertaining to the Australian system, whilst not widespread, is easily found on various websites, particularly those of the Australian intelligence agencies themselves, and of their respective oversight bodies (such as the Parliamentary Joint Committee on Intelligence and Security (PJCIS)[15] and the Inspector General for Intelligence and Security (IGIS)[16]). The Office of National Intelligence has a particularly useful description of the history and evolution of the Australian NIC[17]. Apart from websites, Cain

[14] Prachathai, 2015, 10 Ways to Revolutionize the Thai Military: Exposing the Junta's Blind Spot, accessed via the internet on 23 December 2019 at www.prachatai.com/english/node/5611

[15] Parliamentary Joint Committee on Intelligence and Security website accessed via the internet on 19 January 2020 at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security

[16] Inspector General of Intelligence and Security website accessed via the internet on 23 December 2019 at http://www.igis.gov.au.

[17] Office of National Intelligence website accessed via the internet on 19 January 2020 at https://www.oni.gov.au/

(1994) has written extensively on the history and governance of ASIO[18], as have Horner, Blaxland and Crawley (2015)[19]. Toohey and Pinwell (1990) have done similarly for ASIS[20]. Andrew's 2001 history of the Australian Department of Defence touches on DIO, ASD and AGO[21]. The experience of the author working in Australia's intelligence community also allows for a good understanding of the topic.

Public literature on the Thai intelligence system and its accountability architecture (especially written in or translated to English) is rather more difficult to find. Most of it is peripheral to the issue at hand, and written from the perspective of SSR implementation at higher levels of government rather than an analysis of the intelligence accountability mechanisms themselves. Some information was able to be gleaned from specific Thai intelligence agency websites, but this was limited at best, misleading at worst, and did not focus on intelligence accountability at all. Definition of the Thai intelligence community was also an issue. There are a plethora of internal security-related intelligence agencies and organisations, departmental intelligence shops and intelligence

[18] Cain, F., 1994, ASIO: An Unofficial History, Spectrum Publications, Melbourne.

[19] Horner, D., Blaxland, J., and Crawley, R., 2015, The Official History of ASIO, Allen & Unwin, Sydney.

[20] Toohey, B., and Pinwell, W., 1990, Oyster, Mandarin Australia, Melbourne.

[21] Andrews, E., 2001, The Department of Defence, Oxford University Press, Melbourne.

bodies across echelons in the military. Indeed, an article in the Thai media referred to there being 27 different intelligence agencies[22]!

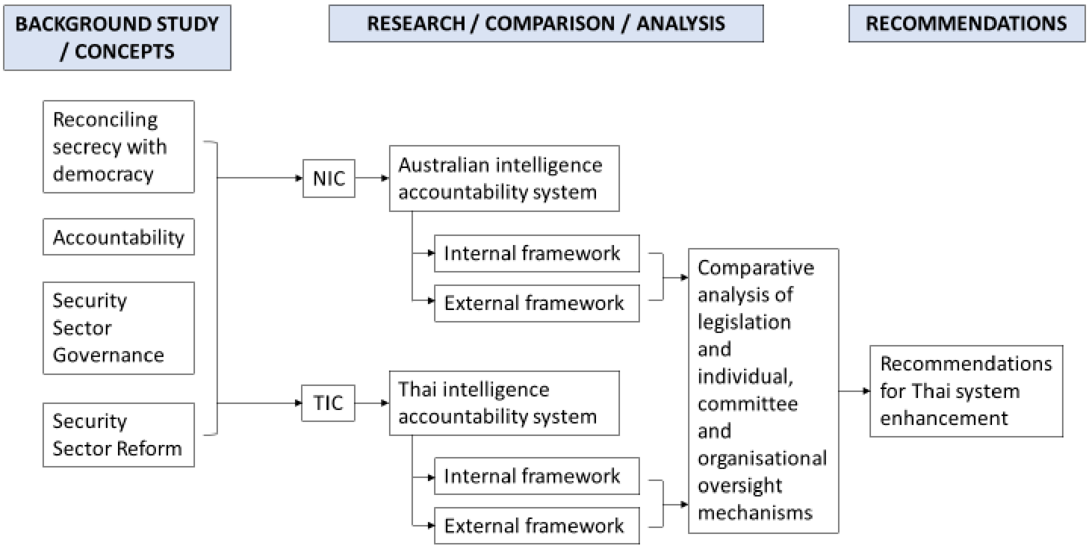
Discussions with academic staff and various people both within and external to the TIC led the author to conclude that for the purposes of the paper, only Thai intelligence agencies with approximate NIC equivalence would be considered for analysis, with security agencies and organisations beyond the scope of this paper. Likewise, operational, tactical, intra-departmental and private intelligence sources and agencies are not included. The dearth of literature, particularly in English, determined that information on the Thai intelligence accountability framework would have to be gained from first principles, by interviews with senior officials from the National Intelligence Agency (NIA); the Armed Forces Security Centre (AFSC); the Intelligence Divisions of the Royal Thai Armed Forces (RTArF), Royal Thai Army (RTA), Royal Thai Navy (RTN) and the Royal Thai Air Force (RTAF); and the Royal Thai Police Special Branch Bureau (RTPSBB).

The questions asked during each interview were developed by the author and consistently asked across interviews. They can be found at Annex E. The list of interviewees and interview dates can be found in the bibliography. The answers provided by the interviewees and their staff enabled the author to develop a thorough understanding of the TIC's

[22] Khan, A., 2017, Thailand To Consolidate Work of 27 Intelligence Agencies, accessed on 27 June 2020 at https://www.defenseworld.net/news/19867/Thailand_To_Consolidate_Work_of_27_Intelligence_Agencies#.Xvb8H-biuUk

accountability frameworks, defined or otherwise, and allowed for a comparison with the Australian NIC accountability frameworks. From there, recommendations were able to be made for potential enhancements across the Thai system. The conceptual framework for construction of this research paper is at figure one below.

Figure 2-1 Research Paper Conceptual Framework


BACKGROUND STUDY / CONCEPTS
RESEARCH / COMPARISON / ANALYSIS
RECOMMENDATIONS
Reconciling secrecy with democracy
Accountability
Security Sector Governance
Security Sector Reform
NIC
Australian intelligence accountability system
Internal framework
External framework
TIC
Thai intelligence accountability system
Internal framework
External framework
Comparative analysis of legislation and individual, committee and organisational oversight mechanisms
Recommendations for Thai system enhancement

Chapter 3
Intelligence Accountability Concepts

Background

Australia is a society characterised by strong notions of individual freedom and personal rights. Its citizens today are probably more conscious of their rights than at any time in the past. The past 30 years has seen significant reform designed to enhance governance and accountability practices of the Government, its departments and agencies at the Federal level. Initiatives have included the 'Freedom of Information Act, the Administrative Decisions (Judicial Review) Act, the Privacy Act, the establishment of the Commonwealth Ombudsman and the Human Rights and Equal Opportunity Commission and the growth of the Federal Parliament's Committee system'[1]. The framework of these administrative and accountability reforms has been underpinned by the 'rights and needs of the individual'[2].

[1] McLeod, R., 1995, *Ethics and Accountability*, presented during the Annual Conference of the Australian Institute of Professional Intelligence Officers 'Intel 95', AIPIO, Sydney

[2] ibid.

This has had significant ramifications for Australia's National Intelligence Community (NIC)[3]. As part of a more general trend in government, greater degrees of scrutiny and oversight in corporate governance and accountability have developed within the NIC, along with increased attention to citizen rights. The continuum of accountability relationships developed between the public, the Parliament, the Government and the various agencies of the NIC has resulted in a high degree of transparency in NIC activities, ensuring agencies act legally and with propriety, comply with ministerial guidelines and respect human rights[4].

[3] The National Intelligence Community (NIC) was officially formed following the Australian Government's adoption of the 2017 Independent Intelligence Review's (IIR) recommendations. The NIC comprises the six agencies that formerly made up the Australian Intelligence Community (AIC) — the Office of National Intelligence (ONI), the Australian Signals Directorate (ASD), the Australian Geospatial-Intelligence Organisation (AGO), the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO) and the Defence Intelligence Organisation (DIO) — as well as the Australian Criminal Intelligence Commission (ACIC) and the intelligence functions of the Australian Federal Police (AFP), Australian Transaction Reports and Analysis Centre (AUSTRAC) and The Department of Home Affairs.

[4] Inspector General of Intelligence and Security website accessed via the internet on 23 December 2019 at http://www.igis.gov.au.

Thailand's recent political history has been rather more unsettled than Australia's, with coups in 2006 and 2014. This has led to periods of military government and internal instability, a situation that doesn't necessarily lend itself to increased transparency and enhanced accountability. According to Chambers (2016), 'Thai support for SSR has traditionally been very weakly organized and temporary. There are no Thai civil society groups who regularly monitor security forces'[5]. One has to assume this includes the TIC intelligence agencies. Despite this rather gloomy picture for the development of transparency and accountability, it's clear that within the context of Thailand's system of democracy, there is clear oversight of, and a requirement for accountability of, the Thai national intelligence system. Sections six, eight and nine of the recently released National Intelligence Act[6], while only pertinent to the NIA and officers seconded to the NIA, makes this clear.

For the Thai intelligence agencies falling under the military banner, oversight and accountability are clear and unambiguous, following the military chain of command. Australia no longer maintains military intelligence agencies as part of a very decentralised NIC, whereas the Thai system of government with its very centralised command and control manner of operating is more suited to it, especially with the more central role of the military across government and society. The RTP are included in this, although with their focus on internal security and

[5] Chambers, P., 2016, op. cit.

[6] National Intelligence Act 2019, accessed via the internet on 23 December 2019 at http://www.ratchakitcha.soc.go.th/DATA/PDF /2562/A/050/T_0022.PDF

protection of the monarchy, their seems to be very little scrutiny of their intelligence activities.

This is not to say however, that all intelligence activity is, should or must be conducted completely in the open. The purpose of secrecy is to 'facilitate the proper functioning of government but it needs to be balanced against other competing public interests including the public's right to know'[7]. It is the role of both internal and external accountability frameworks to ensure this balance is maintained, minimising community apprehension pertaining to intelligence activities and damage to the trust relationship between the Government and its constituency. When the balance is not right, in Australia, Government responds by exercising tighter control through strengthening the accountability framework as necessary, including launching investigations and royal commissions, passing additional legislation and enhancing or creating appropriate oversight mechanisms as required.

Reconciling Secrecy with Democracy

Before examining the concept of accountability in the context of the NIC and the accountability framework within which the NIC sits, it is pertinent to discuss why an accountability framework is needed at all. Put simply, the fact that the NIC works in secrecy behind closed doors in an open and free society with information that in many instances is not publicly available is paradoxical and demands close attention. Reconciling secrecy with democracy is a difficult exercise at best. Balancing the concepts of 'need to know' and 'right to know' is central to the NIC accountability framework.

[7] McLeod, R., 1995, op. cit.

By definition, democratic societies accept the moral right of states to exist and pursue their interests. This infers a moral and ethical right for them to gather and use information to further or protect those interests. This information can be sensitive in nature and in the eyes of the user, must therefore be protected – hence the need for secrecy. In theory therefore, citizens of democracies should have few objections to the use of intelligence per se, and the need for secrecy in protecting that intelligence. The paradox, however, is that democratic nations have an expectation that decisions are taken with the knowledge and consent of citizens. This seems incompatible with the secrecy required to protect sensitive information, intelligence capabilities, sources and methods. So how then, do modern democracies in particular, attempt to reconcile secrecy with democracy? Thompson suggests that the three key methods utilised in reconciling secrecy with democracy are retrospection, generalisation and mediation[8].

Retrospection. Retrospective accountability is allowing for a decision or activity to be reviewed by citizens (or a representative body of them), but only after the decision or activity has been made or completed[9]. The Commonwealth Ombudsman, specially convened commissions and investigative teams provide retrospective accountability for NIC activities.

[8] Thompson, D., 1987, Political Ethics and Public Office, Harvard University Press, Harvard, p 24.

[9] ibid.

Generalisation. Generalisation allows for some form of prior judgement to be made by citizens or their representatives on particular activities. Whilst this may not be practicable in all cases, the general type of activity can be discussed publicly, its justifiability in various hypothetical circumstances considered, and guidelines for conducting it in those circumstances formulated[10]. Thompson uses the example of unmarked police cars to exemplify his point. It would obviously defeat the purpose he argues, ‘to decide in an open debate when and where the cars will patrol, but the policy itself, as well as constraints on it, can be publicly debated or promulgated’[11].

Mediation. Mediation is exemplified in the form of oversight[12]. If policies or activities cannot be made public, legislators acting on behalf of the public oversee the actions of the agencies that enact the policies or conduct the activities. The oversight activities of parliamentary committees and organisations such as IGIS are prime examples in the accountability framework of the NIC.

The Australian Government reconciles the secrecy surrounding NIC agency activity with the principles of a democratic society through acknowledgment of NIC agency existence, publication that their activities are kept secret and regulation of their activities by legislation and oversight bodies. In this manner, the Government fulfils the functions discussed by Thompson in terms of retrospective accountability, generalisation and mediation. Additionally, it can be argued that it is acting with the consent of the people in collecting information, maintaining and using secret

[10] ibid., p 26.

[11] ibid.

[12] ibid., p 29.

intelligence methods, and keeping sensitive information secret in its own right. In return, it can be inferred that the public knows and understands the requirement for NIC agencies, understands the requirement to keep their activities secret, and accepts that the oversight provisions contained in legislation and with the oversight bodies are sufficient. The apparent paradox of secrecy within a democratic society is therefore overcome (in the eyes of both the Government and the public) through the maintenance of an accountability framework. Accountability is therefore the essential element in reconciling secrecy with democratic principles.

Accountability

Accountability is defined by the Macquarie Dictionary as 'liable to be called to account; responsible (*to* a person, *for* an act, etc.)'[13]. The Australian National Audit Office (ANAO) defines public sector governance as 'the process by which organisations are directed, controlled and held to account. It encompasses authority, accountability, stewardship, leadership, direction and control exercised in the organisation'.[14] Democratic bureaucracies in particular couple governance procedures and structures with accountability frameworks in order to hold their many departments and agencies to account in the ever-elusive search for bureaucratic efficiency and transparency. Indeed, with respect to the NIC at large,

[13] Delbridge, A., Bernard, J.R.L., Blair, D., Butler, S., Peters, P., and Yallop, C., (eds), 1997, The Macquarie Dictionary, 3rd Edition, The Macquarie Library Pty Ltd, Sydney, p 13.

[14] Australian National Audit Office, 1999, Corporate Governance in Commonwealth Authorities and Companies, Commonwealth of Australia, Canberra, p1.

Hadyn McComas contends that 'the degree of transparency is perhaps the ultimate test of accountability for intelligence agencies'[15]. In discussing intelligence community accountability, this paper will discuss the elements of accountability and examine the internal and external accountability frameworks governing NIC activities.

Accountability Elements. Dubnick argues that accountability is underpinned by legal, organisational, professional and political elements[16]. The legal component comprises legislative measures designed to govern the actions of an organisation in a particular manner. The organisational element includes internal agency structures and systems. Professional aspects include tertiary education and professional codes of ethics. Political measures provide for oversight and review[17]. By way of example, the NIC's accountability regime comprises both an internal and external framework that encompass all four of Dubnick's principals.

The NIC's internal accountability framework takes into account Dubnick's organisational element of accountability and is affected on three levels within departments responsible for NIC agencies: individual, committee and organisational. This includes ministerial oversight and is discussed in more detail below.

[15] McComas, H., 2002, 'Quis custodies custodiet?' Who Will Guard the Guardians? Accountability in Intelligence, The Journal of the Australian Institute of Professional Intelligence Officers, Vol. 10, No. 2, 2002, AIPIO, Canberra, p 36.

[16] Dubnick, M., 1998, 'Clarifying Accountability – An Ethical Framework' in Sampford, C. and Preston, N. (eds), Public Sector Ethics, The Federation Press, Sydney, p 77.

[17] ibid., p 77.

The NIC's external accountability framework can be equated to Dubnick's three remaining facets of accountability – legislative, professional and political. With respect to NIC accountability, the legislative component comprises various pieces of legislation providing for the establishment or existence of an organisation, its roles, tasks and responsibilities, and what it can and cannot do. The professional element is largely based on societal conformity derived through similar education, training and membership of professional organisations. Each NIC agency has its own code of conduct and ethics, although the differences are minor and inconsequential. Although it plays a significant role in NIC accountability, its intangible nature leads the author to consider any further explanation beyond the remit of this paper. Finally, the political component comprises the oversight and review activities of parliamentary committees and organisations such as IGIS and the Commonwealth Ombudsman. The legislative and political components will be discussed in more detail below.

Despite different systems of government and hence differing intelligence architecture and resultant intelligence oversight and accountability mechanisms, the TIC too has both internal and external accountability frameworks that encompass all four of Dubnick's principals, though the extent and effectiveness of these frameworks differ to that of Australia's experience. Based on a series of interviews with senior Thai intelligence officials from agencies across the entire TIC, the TIC's internal accountability framework, with respect to Dubnick's organisation pillar of accountability, is implemented less formally than in Australia, and is primarily affected at the individual and organisational levels, but is effective nonetheless. This also includes ministerial oversight and is described in more detail later.

Like the NIC, the TIC's external accountability framework can be equated to Dubnick's three remaining facets of accountability – legislative, professional and political. Thailand's legislative component comprises various pieces of legislation providing for the establishment or existence of an organisation, its roles, tasks and responsibilities, and essentially what it can and cannot do. The professional element is particularly strong given the relatively rigid Thai hierarchical command and control system, and the importance of class structures in the Thai military in particular. Societal conformity appears much stronger than that in Australia and is reinforced through derived through education, training, institutions and cultural norms. Finally, the political component in Thailand comprises the oversight and review activities of various committees and organisations. In the author's opinion, despite Thailand having elements of the political facet of accountability in place, their effectiveness and coverage is relatively poor. There are no doubt political, legal and constitutional reasons for this, although discussion of these issues in depth is not the aim of this paper. The legislative and political components of Thailand's external intelligence accountability framework will be discussed in more detail below.

Chapter 4

Intelligence Accountability - The Australian Context

Background

The past 30 years has seen significant development in the governance and accountability frameworks of the Federal Government, its departments and agencies. A ramification of this has been a greater degree of scrutiny and oversight in NIC corporate governance and activity. A continuum of accountability relationships has developed between the public, Parliament, the Government and the various agencies of the NIC. This continuum has developed and grown along with the NIC itself. Although a detailed history of the NIC is beyond the scope of this paper, it is worth briefly noting the development of the NIC and its agencies to provide context for the corresponding development of the accountability frameworks which govern them.

The Australian National Intelligence Community

Immediately prior to and during the First World War, intelligence in the Australian context was primarily counter-intelligence / counter-espionage focussed and largely, though not entirely, the responsibility of the Australian military, and mostly by the Army. During the Second World War, the first parts of what was to become today's NIC were formed to support Allied forces in the Pacific theatre of war, mainly through the provision of signals intelligence (SIGINT). As a result of this experience, the Defence Signals Bureau (now known as the Australian Signals Directorate) formally came into existence in 1947[1].

Following the Second World War, the SIGINT focus shifted to focus on Soviet communications in line with Cold War priorities. At the same time, growing concerns about Australia's security led to the establishment of the Australian Security Intelligence Organisation in 1949. Its immediate purpose was to pursue Russian spies[2].

The Australian Secret Intelligence Service was formed in 1952, falling within the Department of Defence portfolio. It was modelled on its British counterpart (MI6) and focused on collecting human intelligence (HUMINT). In 1954, Ministerial authority for ASIS shifted to what we now call the Minister for Foreign Affairs, and in 1977, ASIS's existence was publicly acknowledged for the first time[3].

During the Second World War, the Department of Defence's intelligence assessment functions were shared between the three Australian Defence Force services (Army, Navy and Air Force) plus the department's intelligence assessment arm - the Joint Intelligence Bureau. In 1970, the Joint Intelligence Organisation was formed through a merger of JIB with most of the foreign assessment elements of the three armed services. Following a 1989 review of Defence intelligence, the Defence Intelligence Organisation (DIO) was established from JIO as Defence's sole strategic-level all-source intelligence assessment agency[4].

[1] https://www.oni.gov.au/where-it-all-began-aic

[2] ibid.

[3] ibid.

[4] ibid.

The second of the two intelligence assessment agencies that comprised the AIC, the Office of National Assessments, was established as an independent agency in 1978. The final organisation to join the AIC was the Australian Geospatial-Intelligence Organisation. Australia's imagery intelligence analysis capability had existed since 1964, but until 1998 it was an integrated part of DIO. In 2000, the various imagery analysis functions in the Australian Government were formally combined under a new organisation — the Defence Imagery and Geospatial Organisation, which later changed its name to AGO in order to better reflect its remit which is broader than just Defence[5].

The most recent review of the intelligence community was the 2017 Independent Intelligence Review. The review made 23 recommendations to government. The most significant of these was the recommendation to legislatively expand ONA to form a new agency, the Office of National Intelligence, with enhanced coordination and evaluation responsibilities. The review also recharacterised the intelligence community as a broader National Intelligence Community, comprising the six AIC agencies, ONI, ASD, AGO, ASIS, ASIO and DIO, as well as the Australian Criminal Intelligence Commission (ACIC) and the intelligence functions of the Australian Federal Police (AFP), Australian Transaction Reports and Analysis Centre (AUSTRAC) and The Department of Home Affairs[6]. As previously discussed, for the purposes of intelligence accountability and oversight, this paper will only consider the six traditional intelligence agencies that formally made up the now defunct Australian Intelligence Community (AIC) - ONI, ASIS, ASIO, DIO, ASD and AGO. The NIC's

[5] ibid.

[6] ibid.

accountability regime comprises both an internal and external framework that encompass all four of Dubnick's principals detailed in Chapter Three.

NIC Internal Accountability Framework

General. The internal accountability framework residing within the Australian governmental departments that NIC agencies belong to is affected on three levels: individual, committee and organisational. Specifically, intra-departmental accountability consists of Ministerial oversight, Charter Letters from departmental secretaries to agency heads, OPA between those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments. Each is discussed in detail below.

Federal Government Departmental Governance Structures. In order to understand intra-departmental accountability frameworks, departmental governance structures should also be clearly understood[7]. Federal government departmental structures reflect three different sets of roles and responsibilities that need to interact to deliver results to Government[8]. These are Output Executives, Owner Support Executives and Enabling Executives respectively. Output Executives comprise various programs that are responsible for delivering products directly for

[7] The governance structure detailed below is based upon the Department of Defence but is equally applicable to other Australian Federal Government departments responsible for NIC elements.

[8] Department of Defence Media Release, 26 June 2000, Good Governance to Underpin Defence Renewal, www.defence.gov.au/media /DeptTpl.cfm?Current, last viewed 19 April 2020.

the Government[9]. Owner Support Executives consist of programs that work in direct support of good governance and are focussed on the role of Government as the 'owner' of individual departments[10]. Programs within departmental Enabling Executives work to support the delivery of outputs from the Output Executives[11]. In the case of the NIC, ONI is considered an output program within the Department of Prime Minister and Cabinet, ASIS an output program within the Department of Foreign Affairs and Trade, ASIO an output program within the Attorney General's Department, and DIO, ASD and AGO output programs within Defence. Program Heads (including the directors general and chairs of each of the NIC agencies) answer to their respective ministers through their respective departmental secretaries.

Public Sector Internal Accountability Framework. Australian public sector intra-departmental accountability is affected on three levels: individual, committee and organisational. At the individual level, Ministerial Directives unambiguously establish individual Ministers as the "customers" for, and "owners" of the outputs delivered various programs within their portfolio. Ministerial Directives are then 'cascaded' to Program Heads in the form of Charter Letters, clearly identifying the individual accountability chain from the Minister, through Departmental Secretaries (and the Chief of the Defence Force (CDF) in the case of Defence) to Program Heads. Both Ministerial Directive and Charter Letters detail key results required and clear accountability arrangements, but not the means by which they

[9] ibid.

[10] ibid.

[11] ibid.

are to be achieved. The aim is to encourage accountable innovation within programs.

Within Departments, senior committee accountability is aligned with individual accountability arrangements. Senior committees are ostensibly advisory bodies with decision-making authority vested in respective committee chairs. Committee accountability, therefore, is unambiguously tied to accountability of their respective chairperson via Charter Letters with Departmental Secretaries.

Organisational accountability is affected through internal purchaser-provider models. Within the Australian Defence Organisation (ADO) for instance, this is known as 'customer-supplier arrangements'[12] and serves as the organisation's business model. Within all Departments, each Program Head has an Organisational Performance Agreement (OPA) with the Secretary (and CDF in the case of Defence), specifying what is expected of their program by way of sustainable performance from them[13]. Additionally, Customer Supplier Agreements (CSA) between Defence's Output and Owner Support Programs and their internal suppliers in the Enabling Program codify the arrangements for provision of goods and services needed to deliver OPA performance standards[14]. Again, note that those NIC agencies belonging to Defence are part of its Output Program. The aim is to ensure those programs responsible for specific results have control over the resources necessary to achieve those

[12] Department of Defence, 2002, *Annual Report*, op cit, p 16.

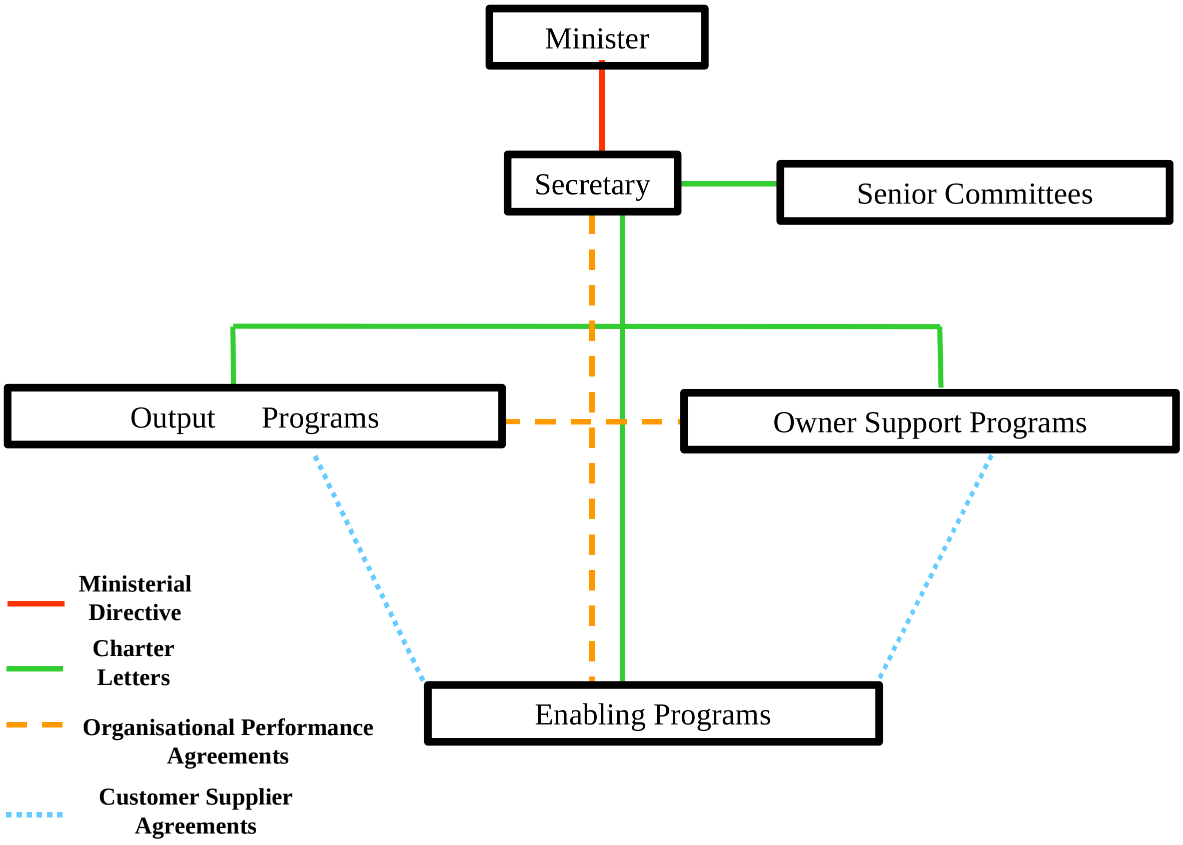
[13] ibid.

[14] ibid.

results and can therefore be held accountable for their performance. This is known as 'alignment'[15].

Public sector accountability, therefore, is multi-dimensional in that it is affected on three levels – individual, committee and organisational. The formal documentation that facilitates this accountability structure includes Ministerial Directives, Charter Letters, OPA and CSA. Figure 1 below details generic public sector intra-departmental accountability arrangements.

Figure 4-1 Generic public sector intra-departmental accountability arrangements



[15] ibid.

Whilst potentially allowing some degree of duplication, establishing multi-dimensional accountability along individual, committee and organisational lines within departments ensures no element of the public sector (and hence the NIC) is left unaccounted for. Additionally, the establishment of OPA and CSA ensures that those programs responsible for specific results have control over the resources necessary to achieve those results. In other words, responsibility is aligned with resources resulting in increased accountability.

Summary. Intra-departmental accountability for NIC elements, therefore, consists of Ministerial oversight, Charter Letters from departmental secretaries to agency heads, OPA between those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments. This ensures that each NIC element is accountable within its respective department for its management, functioning, use of resources and output.

NIC External Accountability Framework

General. Having examined the internal accountability mechanisms for those government departments that host NIC elements, it is now pertinent to examine the wider and, in the eyes of the public, more important issue of external accountability – just how the watchers are themselves watched. External accountability is affected through:

1. legislation;
2. the Parliamentary Joint Committee on Intelligence and Security (PJCIS);

3. committees of Cabinet including the National Security Committee of Cabinet (NSC) and the Secretaries' Committee on National Security (SCNS);

4. courts, tribunals and ombudsmen; and

5. an oversight body in IGIS.

A diagram portraying the external accountability framework of the NIC (less legislation) is at Annex C[16]. The diagram details reporting and accountability relationships as described below.

Legislation. The NIC agencies are subject to the operation of Australian law unless specifically exempted because of the nature of their work. Although some NIC agencies have existed in various guises for well over 85 years[17], the first legislation governing NIC activity was not enacted until 1979 as a result of the Royal Commission on Australia's Security and Intelligence Services in 1977[18]. Extant legislation underpinning the NIC accountability framework is detailed below.

The **Office of National Intelligence Act 2018** (ONI Act 2018)[19] provides the legislative basis for the existence of ONI. ONI was established

[16] This is an updated version of a diagram sourced from the Inspector General of Intelligence and Security accessed via the internet on 20 January 2020 at https://www.igis.gov.au/sites/default /files/ Accountability_Diagram%281%29.pdf

[17] Andrews, E., 2001, The Department of Defence, Oxford University Press, Melbourne, p 133.

[18] McComas, H., 2002, op. cit., p 30.

[19] Office of National Intelligence Act, 2018, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/ C2018A00155

as the Office of National Assessment (ONA) in February 1978 following recommendations from Justice Robert Hope's Royal Commission into Australia's Security and Intelligence Services in 1977[20]. Hope had recommended the need for changes in the Australian intelligence community including a new organisation to coordinate overall intelligence collection and evaluation, previously the purview of the Joint Intelligence Organisation (JIO) – the current day DIO[21]. The ONA Act 1977 was replaced by the ONI Act 2018 which prescribes ONI's functions and requires ONI to report annually to the Prime Minister. ONI's Director-General is a statutory officer with the status of a departmental secretary and is not subject to external direction on the content of assessments[22].

The **Australian Security Intelligence Organisation Act 1979** (ASIO Act 1979)[23] was also born out of the findings of the Royal Commission on Australia's Security and Intelligence Services in 1977 presided over by Justice Hope[24]. Although aimed at all NIC agencies as a result of perceived inefficiencies in operation and lack of accountability

[20] Toohey, B., and Pinwell, W., 1990, Oyster, Mandarin Australia, Melbourne, p 190.

[21] ibid.

[22] Office of National Assessments website accessed via the internet on 19 January 2020 at https://www.oni.gov.au

[23] Australian Security Intelligence Organisation Act, 1979, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00240

[24] Cain, F., 1994, ASIO: An Unofficial History, Spectrum Publications, Melbourne, p 256

for activities undertaken[25], the 1977 Hope Royal Commission recommended the 'strengthening of ASIO's legislation and the expanding of its powers'[26]. Additional recommendations included streamlining ASIO's vetting procedures and providing for the establishment of a Security Appeals Tribunal allowing individuals to appeal against their security assessment[27].

The new Fraser Government responded to the Royal Commission's recommendations by introducing the ASIO Act 1979 on 25 October of that year[28]. It prescribes ASIO's functions and provides for its responsible minister - the Attorney-General - to issue guidelines to it[29]. Interestingly, under the ASIO Act 1979, the Leader of the Opposition is also required to be briefed on national security matters by the Director-General ASIO on an as-required basis[30].

Whilst governed by the ASIO Act 1979, ASIO's main avenue of accountability is intra-departmental through the ministerial oversight provided by the Attorney General[31]. Other accountability is provided through various control mechanisms. Some, such as auditing requirements, apply to all federal government agencies; others apply specifically to ASIO[32]. ASIO also reports to a range of government and parliamentary

[25] McComas, H., 2002, op. cit., pp 30-31.

[26] Cain, F., 1994, op. cit., p 257.

[27] ibid.

[28] ibid., p 260.

[29] Australian Security Intelligence Organisation website accessed via the internet on 19 January 2020 at http://www.asio.gov.au.

[30] ibid.

[31] ibid.

[32] ibid.

committees dealing with security, legislative and financial matters. Additionally, the office of the IGIS has oversight responsibility for ASIO. It has full access to all ASIO records, the power to inquire into public complaints, conduct inquiries referred to it by Government and initiate inquiries of its own pertaining to NIC activity[33].

The Intelligence Services Act 2001 (ISA 2001)[34] came into effect on 29 October 2001 after the Government introduced the Intelligence Services Bill 2001 and associated legislation into the Parliament on 27 June 2001. ISA 2001 provides the legislative basis for the ongoing existence of ASIS and ASD prescribes the functions of ASIS and ASD and establishes a parliamentary committee to review the administration and expenditure of ASIO, ASIS and ASD. It places ASIS and ASD onto a statutory footing and outlines the levels of accountability for the agencies. It provides for oversight complementary to that conducted by IGIS, by a joint parliamentary committee to review the administration and expenditure of the agencies. Additionally, it provides limited immunities under strictly defined circumstances for the conduct of intelligence activities by ASIS.

ISA 2001 makes explicit the role of the Minister for Foreign Affairs in directing ASIS and authorising the conduct of specific activities, particularly those that may have a direct impact on Australians overseas. IGIS has access to all ASIS and ASD reporting and carries out detailed

[33] Inspector General of Intelligence and Security website accessed via the internet on 19 January 2020 at http://www.igis.gov.au.

[34] Commonwealth of Australia, 2001, Intelligence Services Act, *2001*, accessed via the internet on 19 January 2020 https://www.legislation.gov.au/Details/C2020C00029

operational audits to ensure that these agencies act in accordance with Australian law and conduct their activities with propriety.

The **Intelligence Services Legislation Amendment Act 2005** (ISLA 2005) added AGO, DIO and ONI to the original three agencies included in ISA 2001 and provided for the establishment of PJCIS in its current guise[35].

The **Inspector-General of Intelligence and Security Act 1986** (IGIS Act 1986)[36] provides for the appointment of the IGIS and regulates the exercise of the Inspector-General's powers. It establishes the IGIS as an independent statutory officer with extensive powers to scrutinise actions of the intelligence and security agencies. IGIS is covered in more detail in the case study below.

All NIC agencies are budget funded under the provisions of the **Public Service Act 1999**[37]. Other pertinent legislation includes the

[35] Australian Parliament House website accessed via the internet on 19 January 2020 at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/History_of_the_Intelligence_and_Security_Committee and at https://www.legislation.gov.au/Details/C2005C00695

[36] Inspector General of Intelligence and Security Act, 1986, accessed via the internet on 19 January 2020 at https://www. Legislation.gov.au/Details/C2019C00021

[37] Public Service Act, 1999, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00057

Financial Framework (Supplementary Powers) Act 1997[38] and the **Auditor-General Act 1996**[39], whereby all NIC agencies' financial statements are audited annually by the Auditor-General. Additionally, the Administrative Appeals Tribunal is able to review decisions to exempt records over 30 years old from release under the **Archives Act 1983**[40].

Parliamentary Joint Committee on Intelligence and Security. The purpose of Parliamentary committees is mainly to investigate specific matters of policy or government administration or performance. They provide an opportunity for organisations and individuals to participate in policy making and to have their views placed on the public record and considered as part of the decision-making process[41]. Parliamentary committees scrutinise government activity including legislation, the conduct of public administration and policy issues. Committees may oversee the expenditure of public money and they may call the Government or the public service to account for their actions and ask them to explain or

[38] Financial Framework (Supplementary Powers) Act, 1997, accessed via the internet on 19 January 2020 at https://www. legislation. gov.au/Details/C2015C00191

[39] Auditor-General Act, 1996, accessed via the internet on 19 January 2020 at http://www.legislation.act.gov.au/a/1996-23/current/pdf/1996-23.pdf.

[40] Archives Act, 1983, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00179

[41] Australian Parliament House website accessed via the internet on 19 January 2020 at https://www.aph.gov.au/Parliamentary_ Business/Committees

justify administrative decisions[42]. A Parliamentary committee consists of a group of Members or Senators (or both in the case of joint committees) appointed by one or both Houses of Parliament. Through its committees, Parliament obtains information from Government agencies and advice from experts on the matters under investigation[43]. Committees also provide a public forum for the presentation of the various views of individual citizens and interest groups resulting in Parliament being better informed on community problems and attitudes.

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is constituted under section 28 of ISA 2001 and was legislated for under ISLA 2005 that was passed during the 41st Parliament on 2 December 2005[44]. The Committee conducts inquiries into matters referred to it by the Senate, the House of Representatives or a Minister of the Commonwealth Government. It also has certain review functions under section 29 of ISA 2001[45]. It replaced the Parliamentary Joint Committee on ASIO, ASIS and DSD[46] (PJCAAD) and was established with a much broader remit than its predecessor. PJCAAD itself had replaced the former Joint Select Committee on the Intelligence Services and the Parliamentary

[42] ibid.

[43] ibid.

[44] Parliamentary Joint Committee on Intelligence and Security website accessed via the internet on 19 January 2020 at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/History_of_the_Intelligence_and_Security_Committee

[45] ibid.

[46] Defence Signals Directorate (DSD) is the former name of the current ASD.

Joint Committee on ASIO provided for under the ASIO Act 1979 and first appointed in August 1988 during the 35th Parliament[47].

Despite currently having a broader remit, the key intelligence oversight and accountability functions of PJCIS under Section 29 of ISA 2001 and ISLA 2005 include :

1. to review the administration and expenditure of ASIO, ASIS, ASD, DIO, AGO and ONI including the annual financial statements;

2. to review any matter in relation to ASIO, ASIS, ASD, DIO, AGO and ONI referred to the Committee by the responsible Minister or a resolution of either House of the Parliament; and

3. to report the Committee's comments and recommendations to each House of Parliament and to the responsible Minister[48].

In order to maintain the secrecy required for NIC operations, ISA 2001/ISLA 2005 limits the inquiry powers of PJCIS by providing that the functions of the Committee do not include :

1. reviewing the intelligence gathering priorities of ASIO, ASIS, ASD, DIO, AGO or ONI;

2. reviewing the sources of information, other operational assistance or operational methods available to ASIO, ASIS, ASD, DIO, AGO or ONI;

[47] Parliamentary Joint Committee on Intelligence and Security website accessed via the internet on 19 January 2020 at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/History_of_the_Intelligence_and_Security_Committee

[48] Intelligence Services Act, 2001, accessed via the internet on 19 January 2020 at https://www.igis.gov.au/accountability/ parliamentary-oversight

3. reviewing particular operations that have been, are being or are proposed to be undertaken by ASIO, ASIS, ASD, DIO, AGO or ONI;

4. reviewing information provided by, or by an agency of, a foreign government where that government does not consent to the disclosure of the information;

5. reviewing an aspect of the activities of ASIO, ASIS, ASD, DIO, AGO or ONI that does not affect an Australian person;

6. reviewing the rules made under Section 15 of ISA 2001 (to protect privacy of Australians); or

7. conducting inquiries into individual complaints about the activities of ASIO, ASIS, ASD, DIO, AGO or ONI [49].

PJCIS comprises eleven members, five from the Senate and six from the House of Representatives, with six members from Government parties and five from the Opposition. It is currently chaired by Mr Andrew Hastie, MP, a former officer in the Australian Army. Current Committee membership as at June 2020[50] is as follows:

[49] Parliamentary Joint Committee on Intelligence and Security website accessed via the internet on 19 January 2020 at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/History_of_the_Intelligence_and_Security_Committee

[50] ibid.

Figure 4-2 PJCIS Chair - Mr Andrew Hastie MP, Liberal Party of Australia, Canning WA

Figure 4-3 PJCIS Deputy Chair - Hon Anthony Byrne MP, Australian Labor Party, Holt VIC

Figure 4-4 PJCIS Member - Senator the Hon Eric Abetz, Liberal Party of Australia, TAS

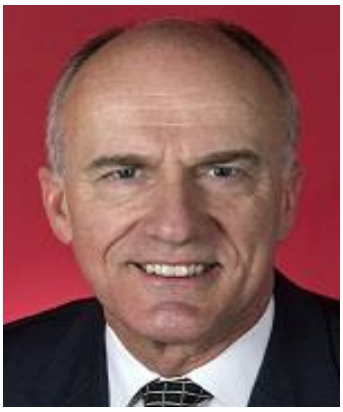


Figure 4-5 PJCIS Member - Senator the Hon David Fawcett, Liberal Party of Australia, SA

Figure 4-6 PJCIS Member - Hon Dr Mike Kelly AM MP, Australian Labor Party, Eden-Monaro NSW

Figure 4-7 PJCIS Member - Senator the Hon Kristina Keneally, Australian Labor Party, NSW

Figure 4-8 PJCIS Member - Mr Julian Leeser MP, Liberal Party of Australia, Berowra NSW

Figure 4-9 PJCIS Member - Senator Jenny McAllister, Australian Labor Party, NSW

Figure 4-10 PJCIS Member - Senator Amanda Stoker, Liberal Party of Australia, NSW

Figure 4-11 PJCIS Member - Mr Tim Wilson MP, Liberal Party of Australia, Goldstein VIC

Figure 4-12 PJCIS Member - Hon Mark Dreyfus QC MP, Australian Labor Party, Isaacs VIC

Committees of Cabinet. In addition to oversight by respective responsible ministers, PJCIS and oversight agencies, NIC activities are guided by the National Security Committee of Cabinet (NSC) supported by the Secretaries' Committee on National Security (SCNS)[51]. The NSC is a Cabinet sub-committee that is the focal point of decision making on national security. It meets on an irregular and ad-hoc basis to consider

[51] Inspector General of Intelligence and Security website accessed via the internet on 19 January 2020 at http://www.igis.gov.au, specifically https://www.igis.gov.au/accountability/ministerial-oversight

strategic development and major issues of medium to long-term relevance to Australia's national security interests[52]. The NSC is chaired by the Prime Minister and also includes the Deputy Prime Minister, Treasurer, Minister for Foreign Affairs, Minister for Defence, the Attorney-General and the Minister for Immigration, Multi-cultural and Indigenous Affairs[53]. Other Ministers may be included on an as-required basis.

The NSC is supported by SCNS, a committee of senior officials chaired by the Secretary of the Department of Prime Minister and Cabinet and comprising the heads of departments and agencies with responsibility for national security issues (including NIC agencies)[54]. Functions of SCNS include:

1. advising the NSC on national security policy,

2. coordinating implementation of policies and programs relevant to national security, and

3. providing guidance to departments and agencies involved in intelligence and security[55].

With respect to the intelligence community, the NSC (supported by SCNS) sets broad policy, priorities and budgets for NIC agencies[56]. Whilst not providing direct oversight of the NIC *per se*, the nature of the relationship with the NSC and the advisory role played by SCNS within

[52] ibid.

[53] ibid.

[54] ibid.

[55] ibid.

[56] Inspector General of Intelligence and Security website accessed via the internet on 19 January 2020 at http://www.igis.gov.au, specifically https://www.igis.gov.au/accountability/ministerial-oversight

this relationship, ensures that both committees maintain more than a passing interest in NIC activity.

Courts, Tribunals and Ombudsmen. Like all Government departments and organisations, NIC agencies subject to the rule of law. As such, their actions are open to scrutiny by courts and tribunals. This does not in itself imply oversight authority or responsibility for the courts but means that the NIC and its constituent elements are legally accountable for their actions. Essentially, the key issue for a judicial review court is the requirement that actions of a government agency must be authorised by law. This issue, and other issues such as the requirements of natural justice, depend on the nature of the actions, their impact on persons and organisations in Australia and the legislation, if any, governing the processes that an agency must follow[57].

Specific tribunals on the other hand, have jurisdiction over particular aspects of NIC activities. As mentioned earlier, decisions to exempt records over 30 years old from release under the Archives Act 1983 are able to be reviewed by the Administrative Appeals Tribunal[58]. Additionally, applicants for security clearances receiving a qualified or negative assessment from ASIO are able to appeal the assessment to the

[57] Department of the Parliamentary Library, Bills Digest No. 11 2001-02, Intelligence Services Bill 2001, accessed via the internet on 19 April 2020 at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r1350

[58] Archives Act, 1983, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00179, and Inspector General of Intelligence and Security website accessed via the internet on 19 January 2020 at http://www.igis.gov.au.

Security Division of the Administrative Appeals Tribunal[59]. Investigations into complaints about NIC activity mounted by IGIS will be considered later in this paper.

The Australian Commonwealth Ombudsman was established under the **Ombudsman Act 1976**[60]. It investigates complaints about Commonwealth Government departments' and agencies' actions to determine if they are unlawful, wrong, unjust or discriminatory[61]. The Ombudsman Act provides that the Ombudsman is to investigate the **administrative** actions of Commonwealth agencies and sets out the limits on his jurisdiction[62] (emphasis added). Note that investigation into complaints over NIC activities and operational matters is the purview of IGIS.

Inspector General of Intelligence and Security. The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office holder who reviews the activities of the NIC. The purpose of this review is to ensure that the agencies act legally and with propriety, comply with ministerial guidelines and directives and respect human rights.

[59] Inspector General of Intelligence and Security website accessed via the internet on 19 January 2020 at http://www.igis.gov.au, specifically https://www.igis.gov.au/accountability/other-accountability-mechanisms

[60] Ombudsman Act, 1976, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00076

[61] https://www.igis.gov.au/complaints/tips-and-advice-making-complaint accessed via the internet on 19 January 2020

[62] Commonwealth Ombudsman website accessed via the internet on 19 January 2020 at http://www.ombudsman.gov.au/.

The functions of the Inspector-General are prescribed under sections 8, 9 and 9A of the Inspector-General of Intelligence and Security Act 1986 (IGIS Act 1986). The Inspector-General can undertake a formal inquiry into the activities of an Australian intelligence agency in response to a complaint or a reference from a minister. The Inspector-General can also act independently to initiate inquiries and conducts regular inspections and monitoring of agency activities. In conducting an inquiry, the Inspector-General has significant powers which include requiring the attendance of witnesses, taking sworn evidence, copying and retention of documents and entry into an Australian intelligence agency's premises. The Inspector-General can also conduct preliminary inquiries into matters in order to decide whether to initiate a full inquiry[63]. According to the IGIS website, IGIS undertakes a range of investigations, considers complaints and Public Interest Disclosures, and contributes to national security reviews and inquiries as follows:

Inspections - IGIS has a regular program of inspections across intelligence agencies to check their compliance and procedures in relation to operational activities.

Inquiries - IGIS can conduct independent inquiries into matters relating to intelligence agencies. An inquiry can be initiated by the IGIS, as the result of identifying an issue of concern, or an inquiry may be referred by a Minister.

[63] Inspector General of Intelligence and Security website accessed via the internet on 19 April 2020 at http://www.igis.gov.au, specifically https://www.igis.gov.au/about

Complaints - IGIS can investigate complaints made about intelligence agencies. Complaints may be made by members of the public or by an employee or former employee of an intelligence and security agency. The IGIS may also consider a public interest disclosure about an intelligence agency.

Submissions - IGIS regularly makes submissions to parliamentary inquiries and other reviews of national security matters, providing comment on the appropriate oversight and accountability requirements relating to the powers of intelligence and security agencies.

Public Engagement - IGIS engages with community groups and national security experts in Australia and internationally through public speaking, participation in oversight forums and convening a civil society reference group[64].

The Office of the IGIS is an agency within the Attorney-General's portfolio, with separate appropriation and staffing[65]. IGIS was established under the IGIS Act 1986 on 1 February 1987 through recommendations arising from the second Hope Royal Commission[66]. Two Royal Commissions into the Australia's intelligence and security

[64] Inspector General of Intelligence and Security website accessed via the internet on 3 June 2020 at http://www.igis.gov.au, specifically https://www.igis.gov.au/what-we-do

[65] IGIS Annual Report 2018-19 accessed via the internet on 19 April 2020 at https://igis.govcms.gov.au/Annual-Report-2018-2019/site/index.html

[66] Blick, B., 1998, Opening Address (Unpublished Paper), Annual Conference of the Australian Institute of Professional Intelligence Officers 'Intel 98', AIPIO, Melbourne.

agencies within a decade convinced Hope of the need for ongoing external review and oversight of NIC activities. The first IGIS, R.N. McLeod, stated that ‘Hope saw my statutory role as Inspector-General as one which would assist the responsible Ministers and would also act as an "independent watchdog" which would bring the agencies to book if they were misbehaving and reassure the public if concerns that they were misbehaving were misplaced’[67]. Today, IGIS is a key element of the NIC’s external accountability framework, assisting the ministers responsible for NIC elements to oversee and review their activities, providing independent assurance to the Australian government, the Parliament and the people that the agencies act legally and with propriety, comply with ministerial guidelines and directives and respect human rights[68].

The current IGIS is Hon Margaret Stone AO FAAL (see figure 14 below). To guarantee independence of the office, the IGIS is appointed for a fixed term of up to five years, cannot be dismissed by the government and is able to be reappointed only once[69]. IGIS has a small staff of about 35 people and is located within the Attorney General’s Department[70] in Barton, ACT. IGIS is a budget-funded agency under the provisions of the Public Service Act 1999 and is subject to scrutiny by Senate legislation committees on its budget allocations and issues relevant to its functions.

[67] McLeod, R., 1995, *Ethics and Accountability*, presented during the Annual Conference of the Australian Institute of Professional Intelligence Officers ‘Intel 95’, AIPIO, Sydney, p 5.

[68] Inspector General of Intelligence and Security website accessed via the internet on 19 January 2020 at http://www.igis.gov.au.

[69] ibid.

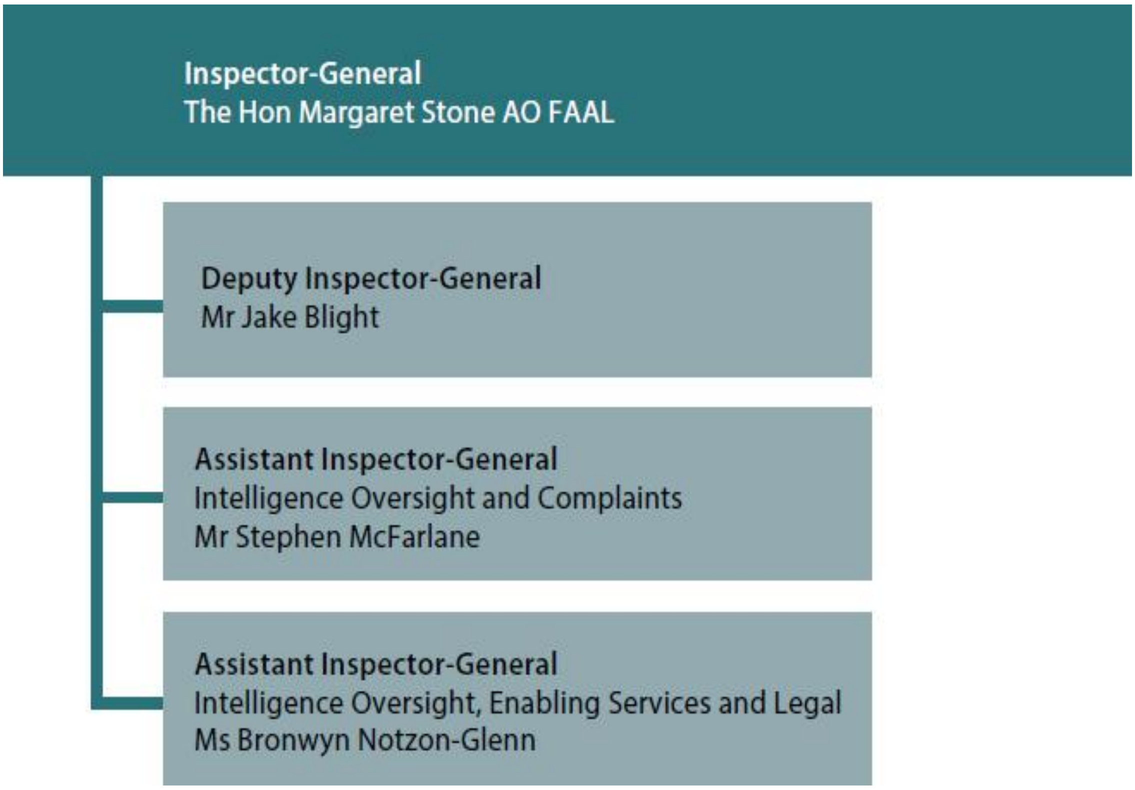
[70] ibid.

Figure 4-13 Inspector General of Intelligence and Security the Honourable Margaret Stone, AO FAAL

IGIS is structured along functional lines with the Inspector-General supported by a Deputy Inspector-General and two Assistant Inspectors-General. The Deputy Inspector-General has responsibility for legal and parliamentary matters, as well as finance and office management. The Assistant Inspector-General Intelligence Oversight and Complaints Branch manages the teams responsible for inspection programs of six agencies within IGIS's current jurisdiction, as well as complaints handling. The Assistant Inspector-General Intelligence Oversight, Enabling Services and Legal Branch manages the teams responsible for engagement with the four additional agencies in IGIS's proposed jurisdiction (the Australian Criminal Intelligence Commission (ACIC) and the intelligence functions of the Australian Federal Police (AFP), Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Department of Home Affairs), as well as corporate, legal and policy services for the office[71]. IGIS's functional structure is detailed in figure 15 below.

[71] IGIS Annual Report 2018-19 accessed via the internet on 19 April 2020 at https://www.igis.govcms.gov.au/Annual-Report-2018-2019/site/index.html

Figure 4-14 IGIS organisational structure at 30 June 2019


Inspector-General
The Hon Margaret Stone AO FAAL
Deputy Inspector-General
Mr Jake Blight
Assistant Inspector-General
Intelligence Oversight and Complaints
Mr Stephen McFarlane
Assistant Inspector-General
Intelligence Oversight, Enabling Services and Legal
Ms Bronwyn Notzon-Glenn

Roles and tasks of IGIS include:

1. regular monitoring of NIC activity;

2. the conduct of inquiries, either self-initiated or at the request of government;

3. investigation of complaints about NIC agencies;

4. delivering recommendations on NIC activities and procedures to Government; and

5. providing annual reports on the NIC to Parliament[72].

[72] Inspector General of Intelligence and Security website accessed via the internet on 19 January 2020 at http://www.igis.gov.au

In conducting these roles and tasks, IGIS is able to exercise its extensive legislative powers to obtain information. It is able to:

1. require any person to answer questions and produce relevant documents,

2. take sworn evidence, and

3. enter NIC agency premises.

Complaints to IGIS pertaining to NIC agency activity whilst not necessarily numerous, are regular. The agency most frequently complained about in 2018-19 was ASIO with 772 complaints[73], of which 750 were related to visa and citizenship applications where ASIO conducts the security background checks of each individual. The largest number of complaints made to IGIS in 2018-19 related to delays in student visa applications, accounting for approximately 52% of all visa and citizenship-related complaints and primarily due to the length of time needed for ASIO to perform its background checks. Of the 750 visa and citizenship applications complaints, 93% were resolved within 14 days of receipt[74].

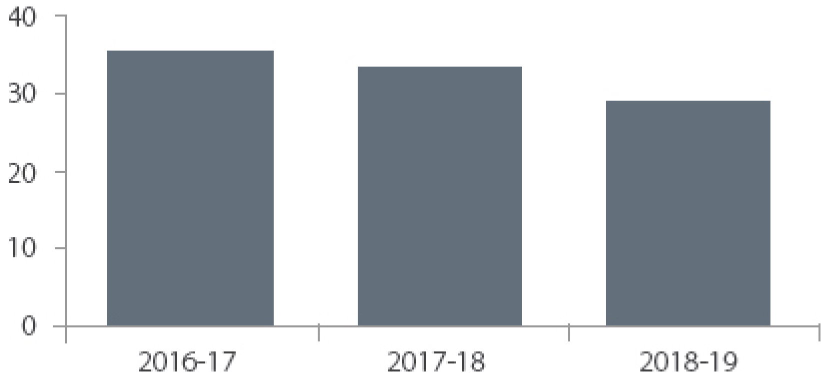
The visa and citizenship complaints skew the number and type of complaints received by ISIS. For the purposes of this paper, it is far more useful to quarantine these complaints and concentrate on the non-visa and citizenship application complaints. In 2018-19, IGIS received 29 non-visa/citizenship-related complaints in the reporting period, continuing a downward trend since the 2016-17 reporting period (see

[73] IGIS Annual Report 2018-19 accessed via the internet on 19 April 2020 at https://igis.govcms.gov.au/Annual-Report-2018-2019/site/index.html

[74] ibid.

figure 16 below)[75]. Ten complaints received in 2017-18 were carried into the 2018-19 reporting period, while at the end of 2018-19 one complaint remained open.

Figure 4-15 Non-Visa/Citizenship Complaint Statistics 2016-17 to 2018-19



Of these 29 complaints, the majority (22) were about ASIO, while five were about ASD and two concerned ASIS. No complaints were received concerning AGO, DIO or ONI[76]. The above figures are neither too unusual nor unexpected. ASIO is the most visible of the four collection agencies (ASIO, ASIS, ASD and AGO) and as such, can be expected to receive the majority of complaints. ASD and AGO collect via technical means that are not physically intrusive or normally detectable by the subject. Low numbers of complaints against them should expected. ASIS conducts the majority of its business overseas and as such, there is limited interaction with the Australian public. DIO and ONI are primarily analytical agencies rather than physical collectors of intelligence, so their normal activities are unlikely to impinge upon public

[75] ibid.

[76] ibid.

privacy. The number of complaints pertaining to these agencies is therefore usually low.

The complaints received in 2018-19 covered a wide range of matters, including allegations about security assessments for employment, recruitment irregularities, obstruction in obtaining software certification and harassment[77]. Figure 16 below details the nature of the allegations against the agency they were made against. There appear to be remarkably few about nefarious NIC activity, and most seem to be related to procedural fairness and governance issues rather than operations aspects of the NIC. According to the IGIS website, complaints to IGIS in the past about NIC activity have included 'allegation of unlawful "bugging" of telephones, inappropriate surveillance, delays in security assessments of asylum seekers, inappropriate involvement in court matters, poor recruitment practices, etc'[78]. Previous IGIS Annual Reports also cite warrant operations and procedures, use of foreign translators, dealings with law enforcement agencies, separation grievance, termination of relationship with human source as complaints received[79]. Inspection of IGIS annual reports since 1986-7 suggests that these complaints are indicative and representative of those made since IGIS was established[80].

[77] ibid.

[78] Inspector General of Intelligence and Security website accessed via the internet on 19 April 2020 at http://www.igis.gov.au.

[79] IGIS Annual Report 2001-2 accessed via the internet at http://www.igis.gov.au/fs_annual.html.

[80] IGIS Annual Reports from 1986-7 to 2018-19 accessed via the internet at http://www.igis.gov.au/fs_annual.html.

Table 4-1 Non-Visa/Citizenship Complaints by NIC Agency 2018-19

Allegations	**ASIO**	**ASIS**	**ASD**
Communication issues	2	0	0
Delay – security assessment	11	0	0
Detriment to member of public arising from agency action	2	0	1
Employment – internal security	1	1	2
Employment – management action	1	0	1
Legality	2	1	1
Harassment	3	0	0

When a complaint is received, it is initially assessed to determine if it is a matter able to be investigated by IGIS. Factors taken into account include:

1. whether the complaint actually relates to an NIC organization,
2. how long ago the events which led to the complaint occurred,
3. whether the agency concerned has conducted, or is already conducting a review of its own,
4. whether the matter should be referred elsewhere, and
5. whether the matter is serious enough to warrant an investigation[81].

[81] Inspector General of Intelligence and Security website accessed via the internet on 19 April 2020 at http://www.igis.gov.au.

If a complaint is found to have no basis, IGIS informs the complainant via a written explanation. Justifiable complaints, however, are directed to the relevant agency head and the responsible Minister. If unable to be resolved by IGIS immediately, a complaint is investigated. The initial inquiry into a complaint is called a preliminary inquiry. If comparatively uncomplicated, it is normally able to be resolved within a few weeks[82]. Should the matter be relatively complex or if information is uncovered that suggests a serious breach under the appropriate legislation, then a full inquiry is initiated. Additionally, the Inspector-General may initiate a preliminary inquiry in order to determine if a specific case warrants a full inquiry. Full inquiries are detailed investigations that may involve the examination of intelligence-related material, inspections, searches and interviews. They can take several months and, in some cases, up to a year[83]. In conducting an inquiry, IGIS has significant powers including requiring the attendance of witnesses, taking sworn evidence, the copying and retention of documents and entry into an agency's premises[84].

As a result of a preliminary or full inquiry, IGIS can recommend that an NIC organisation 'reconsider or change a decision, change its rules or procedures, or pay compensation for any loss that been suffered as a result of its decisions or actions'[85]. In theory, Ministers responsible for NIC organisations and/or the agencies themselves are not compelled to accept IGIS findings and recommendations from their inquiries.

[82] ibid.

[83] ibid.

[84] ibid.

[85] ibid.

In reality however, IGIS and the NIC maintain an excellent working relationship. Justifiable complaints normally arise from NIC agencies' genuine mistakes in procedure rather than any devious intent. Consequently, IGIS findings and recommendations are usually accepted and taken in the manner they were intended. As per the IGIS Act 1986, if a full inquiry is critical of an NIC element, IGIS must consult with the relevant agency head and the responsible Minister[86]. In addition to complaints from the public, IGIS can investigate the activities of an agency in response to a complaint or reference from a Minister[87]. The Inspector-General can also act independently to initiate inquiries[88].

Summary. Extra-departmental accountability for Australia's NIC elements, therefore, consists of legislation; the Parliamentary Joint Committee on Intelligence and Security; committees of Cabinet including the NSC and SCNS; courts, tribunals and ombudsmen; and an oversight body in IGIS. This ensures that the NIC as a whole, and its individual constituent agencies, are forced to remain as transparent and accountable to the public as possible, within the operational constraints of their secret work, for its management, functioning, use of resources and output.

[86] Inspector General of Intelligence and Security Act, 1986, accessed via the internet on 19 January 2020 at https://www. legislation. gov.au/Details/C2019C00021..

[87] Inspector General of Intelligence and Security website accessed via the internet on 19 April 2020 at http://www.igis.gov.au.

[88] Inspector General of Intelligence and Security Act, 1986, accessed via the internet on 19 January 2020 at https://www. legislation. gov.au/Details/C2019C00021.

Summary

The past 30 years has seen significant development in the governance and accountability frameworks of the Federal Government, its departments and agencies. A ramification of this has been a greater degree of scrutiny and oversight in NIC corporate governance and activity. A continuum of accountability relationships has developed between the public, Parliament, the Government and the various agencies of the NIC. This Accountability framework has both internal and external components and has resulted in a high degree of transparency in NIC activities, ensuring their actions are legal, ethical and respect the right of individual citizens.

Perhaps the most difficult aspect of this accountability framework is reconciling democratic practices with maintaining organisations that necessarily work in secrecy. Balancing the concepts of 'need to know' and 'right to know' is central to the NIC accountability framework. Democratic principles stress an expectation that decisions are taken with the knowledge and consent of citizens. This seems incompatible with the secrecy required to protect sensitive information, intelligence capabilities, sources and methods. The Australian Government reconciles the secrecy surrounding NIC activity with democratic principles through acknowledgment of NIC agency existence, publication that their activities are kept secret and regulation of their activities by legislation and oversight bodies. In this manner, the Government fulfils the functions laid out by Thompson in terms of retrospective accountability, generalisation and mediation. Accountability then, is the cornerstone to reconciling secrecy with democratic principles.

Dubnick has theorised that an accountability framework must have legal, organisational, professional and political facets to it[89]. The legal component comprises legislative measures designed to govern the actions of an organisation in a particular manner. The organisational element includes internal agency structures and systems. Professional aspects include tertiary education and professional codes of ethics. Political measures provide for oversight and review[90]. The NIC's accountability regime comprises both an internal and external framework that encompass all four of Dubnick's principals.

The internal accountability framework residing within the Australian governmental departments that NIC agencies belong to is affected on three levels: individual, committee and organisational. Specifically, intra-departmental accountability consists of Ministerial oversight, Charter Letters from departmental secretaries to agency heads, OPA between those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments.

External accountability is affected through legislation; the Parliamentary Joint Committee on Intelligence and Security; committees of Cabinet including the NSC and SCNS; courts, tribunals and ombudsmen; and an oversight body in IGIS. The principal elements of the NIC's external accountability framework are summarised below:

1. Key legislation governing NIC agency activity includes the ONI Act 2018, ASIO Act 1979, ISA 2001, ISLA 2005 and IGIS Act 1986.

2. Parliamentary committees generally scrutinise government activity including legislation, the conduct of public administration and

[89] Dubnick, M., 1998, op. cit., p 77.

[90] ibid.

policy issues. The PJCIS is constituted under section 28 of ISA 2001 and is legislated for under ISLA 2005. Its primary function is to review the activities, administration and expenditure of the NIC agencies.

3. The NSC (supported by SCNS) sets broad policy, priorities and budgets for the NIC.

4. NIC agencies are subject to the rule of law and thus their actions are open to scrutiny by courts and tribunals. This does not imply oversight authority or responsibility for the courts but means that the NIC and its constituent elements are legally accountable for their actions.

5. The Commonwealth Ombudsman is able to investigate complaints of an administrative nature pertaining to NIC agencies.

6. IGIS assists the ministers responsible for NIC elements in overseeing and reviewing their activities and provides independent assurance to the Australian government, Parliament and people that the agencies are acting legally and with propriety, comply with ministerial guidelines and directives and respect human rights.

IGIS in particular provides the main oversight body in the NIC's accountability framework. As per its charter under the IGIS Act 1986, the organisation conducts regular monitoring of NIC activity; launches inquiries (self-initiated or at the request of Government); investigates complaints about NIC agencies; delivers recommendations on NIC activities and procedures to Government; and provides annual reports on the NIC to Parliament. IGIS is able to exercise its extensive legislative powers to obtain information to complete these tasks. Complaints are assessed to determine if they require investigation by IGIS. If they cannot be resolved immediately, it is investigated through a preliminary inquiry and if warranted, a full inquiry is initiated. Results and findings are presented to the responsible Minister, the agency involved and Parliament, are normally accepted and recommendations implemented.

It is in this manner therefore, that NIC agencies are held to account by the public they serve. The internal and external accountability frameworks described above are underpinned by the rights and needs of the individual and ensure organisations that necessarily work in secret are nonetheless transparent, open, honest and held responsible for their actions. The apparent paradox of secrecy within a democratic society is overcome (in the eyes of both the Government and the public) through the maintenance of this accountability framework.

Chapter 5
Intelligence Accountability - The Thai Context

Background

The respective national intelligence communities of Thailand and Australia are significantly different from each other. This stems from myriad reasons, including vastly different national histories and geopolitical circumstances; systems of government; roles, functions and purposes of the various intelligence agencies; weighting differences between internal and external national security focus; threat environments; extant alliance structures; technical and technological capabilities; and cultural factors[1]. This list is not exhaustive, but suffice to say that drawing direct comparisons between the national intelligence systems of Australia and Thailand is difficult.

Despite this, organisational architectural similarities in form and function are able to be distilled in a macro sense. For instance, both national intelligence systems have complimentary internal and external accountability arrangements, clearly defined or otherwise, although they bear little resemblance to each other. As detailed in the previous chapter, Australia's internal intelligence accountability framework delivering intra-departmental accountability comprises Ministerial oversight, Charter Letters from departmental secretaries to agency heads, OPA between

[1] Lieutenant General Wichai Chucherd, Director General, Armed Forces Security Centre, Royal Thai Armed Forces. Interview. 11 June 2020.

those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments. Australia's external intelligence accountability framework delivering extra-departmental accountability comprises various legislative instruments, the Parliamentary Joint Committee on Intelligence and Security; committees of Cabinet including the NSC and SCNS; courts, tribunals and ombudsmen; and an oversight body in IGIS.

The Thai apparatus is similar, if appearing somewhat less prescriptive and well defined. Thailand's intelligence agencies are the oldest and amongst the largest in Southeast Asia, and as in other regional countries, several Government departments and the military control their operations[2]. (This is a major difference between the systems of Australia and Thailand – in Australia, the military intelligence directorates were dissolved over 20 years ago with the advent of military jointry in the Australian Defence Force). In general, Thai intelligence agencies can be categorised into three broad strata: Governmental level (NIA), Ministerial level (for instance, Ministry of Defence) and Military level (including the intelligence functions of RTArF, the RTA, RTN and RTAF, as well as those of the Royal Thai Police)[3]. All of the NIC-equivalent agencies in the TIC, military or civilian, have clear and unambiguous command and

[2] Kisak, P., 2004, Encyclopedia of Intelligence and Counterintelligence, Carlisle, R. (ed), Routledge, London.

[3] Vice Admiral Wuttichai Saisatien, Director General, Naval Intelligence Department, Royal Thai Navy. Interview. 28 May 2020.

control structures, and ‘are clearly defined in terms of responsibilities and operations by legal contexts’[4].

These structures notwithstanding, depending on the nature, importance, time imperative and significance of the intelligence being reported, the reporting chain does not necessarily always mirror the command and control framework. Discussions with the Directors of Intelligence in the TIC agencies indicates this focus on effective outcomes in intelligence reporting is broadly replicated in terms of intelligence accountability. Operational effectiveness and the protection of national security is prioritised over being held accountable to the public. That said, there are clear accountability frameworks in place that are similar in nature to the Australian intelligence accountability system, both internal and external. Before looking at the accountability architecture, a brief overview of the TIC agencies considered for this paper is warranted.

The Thai Intelligence Community

For the purposes of this paper, the Thai Intelligence Community is considered to comprise those agencies with comparable roles and tasks to the agencies of the Australian NIC. It is acknowledged that it is not a neat fit, there are no directly comparable agencies and the roles and tasks of Thai intelligence agencies differs significantly to those of Australian intelligence agencies. There are however, broad overlaps in remit between some Australian and Thai agencies despite there being no true equivalence. Bearing this in mind, this paper will therefore only consider national intelligence agencies in the traditional sense, with security agencies and

[4] Lieutenant General Natee Wongissares, Director of Joint Intelligence, Royal Thai Armed Forces. Interview. 27 May 2020.

organisations being beyond its scope. Operational, tactical, intra-departmental and private intelligence sources and agencies are likewise not considered. To that end, for the purposes of this paper, the following organisations and agencies will be considered from an accountability framework perspective:

National Intelligence Agency. The National Intelligence Agency (NIA) is Thailand's counter-intelligence and security agency. It is subordinate to the Office of the Prime Minister, and is broadly equivalent in remit to elements of ONI, ASD, ASIS and ASIO. It is responsible for both domestic and foreign intelligence, the conduct of intelligence operations, counterintelligence and signals intelligence. NIA also is also responsible for synchronising the efforts of all Thai intelligence agencies through the National Intelligence Coordinating Center (NICC). It also maintains an intelligence training and professional development role. The first nationally centralised intelligence agency in Thailand was established in 1954 as the Department of Administrative Intelligence under the Cabinet of Thailand. It was renamed the Department of Central Intelligence in 1959 before settling with its current name during the government of Prime Minister Prem Tinsulanonda. It was initially formed with the help of the US Central Intelligence Agency to counter communist insurgents operating in Thailand, who at the time, were mainly affiliated with North Vietnam. As the war in Vietnam developed, so too the Thai intelligence network grew with US guidance and support. In 1985, the National Intelligence Act, B.E. 2528 (1985) made the NIA the lead Thai intelligence agency, which was subsequently confirmed by the National Intelligence Act, B.E. 2562 (2019).

Military Intelligence Agencies. The Intelligence Divisions of the Royal Thai Armed Forces (RTArF), Royal Thai Army (RTA), Royal Thai Navy (RTN) and the Royal Thai Air Force (RTAF) provide the intelligence functions for each of the respective services of the Thai military. They are broadly equivalent in remit to elements of DIO and AGO in the main, as well as providing some additional, but less prominent, capabilities. The Armed Forces Security Centre (AFSC) essentially provides a great deal of Thailand's operational intelligence capability and a recently developed intelligence fusion centre to make sense of the data collected. It is broadly equivalent in remit to elements of ASD, DIO, ASIO and AGO. Australia's military intelligence directorates were dissolved and the majority of their capabilities transferred to NIC agencies and the ADF's Joint Operations Command in the 1990s.

The Royal Thai Armed Forces Headquarters has its foundations in the Supreme Command Headquarters of RTArF, established as a Special Task Headquarters during the Franco-Thai War in 1940 and again during the Greater East Asia War (as Thailand's involvement in the Second World War is also known as locally) in 1941. However, the Supreme Command Headquarters was dissolved following the end of each of the wars. The position of the Supreme Commander was revived in 1957 during with the Defence Staff Department of the Ministry of Defence serving as staff for the Supreme Commander. In 1960, the Government permanently established the Supreme Command Headquarters in order to prepare Thailand's combat forces and safeguard the country. In 2008, the Ministry of Defence was restructured and the Supreme Command Headquarters renamed the Royal Thai Armed Forces Headquarters headed by the Chief of Defence Forces. It is tasked with preparing

Thailand’s military forces, safeguarding the Kingdom, and using military force pursuant to the authority vested in the Ministry of Defence. It currently comprises four groups – Command Group, Joint Staff Group, Operations Group and Special Services Group.

Currently, the Directorate of Joint Intelligence sits within the Joint Staff Group. It has responsibility for policy, coordination, supervision and operations pertaining to security and military diplomacy of the Supreme Command, in addition to intelligence coordination for Thailand’s armed forces. It plans and conducts intelligence operations with other agencies, both internal and external to the Ministry of Defense. It is also responsible for the production of strategic intelligence estimates and international engagement with foreign militaries and defence-related intelligence agencies.

The AFSC currently resides within HQ RTArF’s Operations Group, and is responsible for aspects of Thai operational intelligence and counter-intelligence. It also conducts military security intelligence and communications and signals intelligence work alongside intelligence education and training. Apart from that, the AFSC also assists in providing security, together with other relevant departments, for the Royal Family and other VIPs in the Thai hierarchy.

The Intelligence Directorates of the Royal Thai Army, Royal Thai Navy and Royal Thai Air Force developed independently along with their parent services over many years. Although intelligence work was being done in the RTA from at least 1895, the precursor organisation of the RTA Directorate of Intelligence was first established in 1910, making it one of the oldest continuous intelligence organisations world-wide. It has a duty to plan, coordinate and conduct intelligence and security operations, diplomatic tasks including international engagement activities with foreign Defence and Army Attachés in Thailand and running Thailand's overseas network of Army Attachés. It also has staff, analytical, ceremonial, training and cartographical responsibilities within the RTA.

Directly subordinate to the RTA Directorate of Intelligence is an organisation called the Military Intelligence Agency (MIA) headed by a Major General that is essentially the operational intelligence provider for RTA, RTN and RTAF. This is an area where oversight and accountability are critical, much more so than the intelligence staff functions provided by the respective intelligence directorates.

The RTN Naval Intelligence Department has been in existence in one guise or another, with some gaps in service, since 1899. The current organisation was established in 1955 and has a duty to plan, coordinate and conduct maritime intelligence, security and naval counterintelligence operations and analysis, diplomatic tasks including international engagement activities with foreign Defence and Naval Attachés in Thailand and running Thailand's overseas network of Naval Attachés. It also has staff, analytical, ceremonial and training responsibilities within the RTN.

The RTAF Intelligence Department and its precursor agencies have been involved in Air Force-related intelligence work since the Royal Thai Air Force was founded in 1913. Today's RTAF Intelligence Department was established in 1952 and is responsible for Air Force intelligence policies, planning, coordination and technical development. Governance oversight, staff and analytical functions, ceremonial aspects and intelligence training are also part of their remit, along with Air Force counterintelligence and security functions. As with the other military services, the RTAF Directorate of Intelligence is responsible for international engagement activities with foreign Defence and Air Attachés in Thailand and running Thailand’s overseas network of Air Attachés.

Royal Thai Police Special Branch Bureau. The Royal Thai Police Special Branch Bureau (SBB) is a law enforcement agency under the Royal Thai Police Headquarters that was established in 1932. SBB’s major functions are to provide security for the Royal Family and collect, produce and act on intelligence relating to people or groups presenting a threat to national security through subversive activities. Whilst there is no direct equivalent agency in Australia, some elements of SBB’s remit are commensurate with parts of ASIO’s roles and responsibilities (as well as those of the Australian Federal Police who are not included in this analysis).

TIC Internal Accountability Framework

General. In general, Thai intelligence accountability frameworks are less well defined, regulated and legislated than in Australia. This is primarily due to differences in governmental systems and governance, a more centralised command and control regime, historical and cultural factors, different foci of intelligence agencies and a different threat environment within and against which they operate. For the same reasons, Thailand’s internal intelligence accountability framework is much more robust than its external framework, although it should be noted that Thailand does not generally share the same definition of, or need for intelligence oversight and accountability as does Australia. Indeed, there is no comprehensive definition or understanding of an intelligence accountability framework or architecture, so the author has developed the Thai context from first principles.

Ministerial Oversight and Chains of Command. Like Australia, the internal accountability framework residing within the Thai governmental departments that TIC agencies belong to is affected on three levels: individual, committee and organisational. In the Thai context however, due to strong centralisation of command and decision making, the chain of command provides the strongest accountability mechanism for the majority of TIC agencies. This fact was reinforced by most of the interviewees[5]. NIA, being a wholly civilian (and the most senior) agency that is covered by recent and comprehensive legislation, is a point of difference that will be discussed further later. From an accountability perspective, the Thai chain of command can be thought of as broadly equivalent to Australian intra-departmental accountability mechanisms.

[5] Lieutenant General Terdsak Dumkhum, Director General of Intelligence, Directorate of Intelligence, Royal Thai Army. Interview. 26 May 2020. Lieutenant General Natee Wongissares, Director of Joint Intelligence, Royal Thai Armed Forces. Interview. 27 May 2020. Vice Admiral Wuttichai Saisatien, Director General, Naval Intelligence Department, Royal Thai Navy. Interview. 28 May 2020. Lieutenant General Wichai Chucherd, Director General, Armed Forces Security Centre, Royal Thai Armed Forces. Interview. 11 June 2020. Police Major General Saksira Pheuak-um, Deputy Commissioner Royal Thai Police Special Branch Bureau. Interview. 29 June 2020. Major General Pongtep Gaewchaiyo, Deputy Director General Border Affairs, Royal Thai Armed Forces. Interview. 8 July 2020.

There is clear and unambiguous ministerial oversight that is definitely more centralised and probably more stringent than in Australia. Australia's ministerial oversight of the NIC is affected through four ministers (including the Prime Minister). In Thailand, this is reduced to effectively one, as the Prime Minister also acts as the Defence Minister and the Police Minister, and NIA reports directly to the Prime Minister as well[6].

However, depending on the nature, importance, time imperative and significance of the intelligence being reported, the reporting chain does not necessarily always mirror the command and control framework. The Prime Minister is currently assisted in his centralised intelligence role by the Deputy Prime Minister who acts as an intelligence Czar, of sorts, providing an additional layer of accountability and a filter between the intelligence agencies and the Prime Minister when necessary and/or appropriate. This arrangement has the potential to undermine intelligence accountability due to the systemic 'short circuit' it provides around the chain of command, and is reflective of the internal bias towards operational effectiveness of the TIC versus its transparency and public accountability. It should be noted that this current structure is not necessarily permanent, and may change with future changes of government or changes of ministers. Although more likely due to a vested interest in the effectiveness of the TIC agencies and their reporting, this close

[6] Lieutenant General Natee Wongissares, Director of Joint Intelligence, Royal Thai Armed Forces. Interview. 27 May 2020, Mr Krissada Aksornsong, Director Counter-Terrorism and Trans-National Crime, National Intelligence Agency. Interview. 23 June 2020, and Police Major General Saksira Pheuak-um, Deputy Commissioner Royal Thai Police Special Branch Bureau. Interview. 29 June 2020.

ministerial oversight by the Prime Minister and Deputy Prime Minister provides a layer of accountability much like Australia's, and is similarly effective.

The Ministry of Defence also exercises oversight of its respective TIC agencies through the Intelligence Board. Its roles include the coordination of military TIC agency activities, ensuring compliance with the National Intelligence Policy and development of various policies and procedures[7].

Inspectors General. Within the military and police chains of command, there also resides respective Departments of Inspectors General[8]. Again, NIA does not have this element in their chain of command[9]. Theoretically, the Inspectors General (IG) act as the internal eyes and ears for their respective commander in chief across the entire organisation, including (to a degree) the intelligence agencies. The RTArF IG for instance, has the authority to 'scrutinise the conduct and performance of military units, including Joint Intelligence'[10]. Should a relatively major issue or serious anomaly be identified within an intelligence agency, the

[7] Lieutenant General Terdsak Dumkhum, Director General of Intelligence, Directorate of Intelligence, Royal Thai Army. Interview. 26 May 2020.

[8] From organisational charts on TIC agency websites and through discussions with TIC agency heads or their representatives.

[9] Mr Krissada Aksornsong, Director Counter-Terrorism and Trans-National Crime, National Intelligence Agency. Interview. 23 June 2020.

[10] Lieutenant General Natee Wongissares, Director of Joint Intelligence, Royal Thai Armed Forces. Interview. 27 May 2020.

respective IG would inform the respective commander in chief who would then establish a commission to investigate the matter. For major issues and prominent matters, the commander in chief would usually chair the commission and the IG would act as the commission secretary. Should the matter be relatively minor in nature, the commander in chief would direct the relevant agency director to deal with the matter appropriately. In practice, it rarely gets to this as whilst the IGs have oversight responsibility for behavioural issues in general, cultural norms mean they are not very powerful in reality and would not usually conduct oversight activities of their respective TIC agencies unless specifically directed to by their relevant commander in chief, or sparked by an external vector such as an unfavourable media report.

For the RTPSBB, internal oversight mechanisms include the Internal Audit Office and Office of the Inspector General. The Internal Audit Office is concerned with overseeing management systems, finance and budgets. The Office of the Inspector General reviews operations and intelligence activities to ensure everything is done legally[11].

In the author's opinion, stronger IG departments with broader powers of oversight would significantly enhance internal accountability and provide commanders in chief greater control of their respective intelligence agencies. This in turn would likely result in more focussed, efficient and effective intelligence operations and outcomes.

[11] Police Major General Saksira Pheuak-um, Deputy Commissioner Royal Thai Police Special Branch Bureau. Interview. 29 June 2020.

Formal Intra-departmental Accountability Documentation. The formal documentation that facilitates the NIC's internal accountability structure includes Ministerial Directives, Charter Letters from departmental secretaries to agency heads, OPA between those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments. While there is no defined equivalent in the Thai system, there are unambiguous command and control structures that 'are clearly defined in terms of responsibilities and operations by legal contexts'[12]. Thai legislation therefore, crosses the internal / external intelligence accountability threshold, reducing complexity and reinforcing the chain of command as the primary internal accountability mechanism. Relevant Thai legislation is discussed in further detail below.

A key issue with this system as it currently stands is the possibility that legislation may not be specific enough to ensure accountability is affected in the level of detail required. For instance, relying on legislation and good will of other organisations whilst lacking OPA and CSA means that TIC agencies responsible for specific results potentially have no control over the resources necessary to achieve those results. Having specific and directive OPA and CSA would ensure responsibility is aligned with resources resulting in increased accountability for TIC agencies, both in terms of effectiveness and oversight. In the author's opinion, Thailand would benefit from a more clearly defined TIC internal accountability structure detailing key results required and clear accountability arrangements, but not the means by which results are to be achieved. This would encourage accountable innovation within TIC agencies, whilst improving effectiveness.

[12] ibid.

Summary. Intra-departmental accountability for TIC elements, therefore, consists of Ministerial oversight, respective chains of command and departments of Inspectors General in each of the TIC agencies less NIA. To a degree, legislation also partially covers some of the accountability requirements encapsulated in the Australian system by Ministerial Directives, Charter Letters from departmental secretaries to agency heads, OPA between those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments. Collectively, this results in a very robust internal accountability framework and ensures that each TIC agency is accountable within its respective department for its management, functioning, use of resources and output.

TIC External Accountability Framework

General. Having examined TIC internal accountability mechanisms, it is now pertinent to examine the wider and, in the eyes of academia and the public throughout the democratic world, more important issue of external accountability – just how the watchers are themselves watched. TIC extra-departmental (external) accountability is affected through legislation; senate appointed committees; the National Security Council; courts, tribunals and ombudsmen. The media also has a major role to play, although clearly not part of the formal accountability framework. Each of these is discussed below. A diagram portraying the accountability framework of the TIC (less legislation) is at Annex D[13]. The diagram details reporting and accountability relationships as described below.

[13] This diagram was created by the author based on substantial readings and interviews conducted for the production of this paper.

Legislation. Legislation is the key pillar in Thailand's external intelligence accountability framework. All of the military TIC agencies operate under the same legislation, the RTP has its own police-specific legislation under which RTPSBB falls, whilst agency-specific legislation encompasses NIA and those seconded officers from other agencies working under NIA auspices. This paper does not consider the legislation in detail, just its purpose and the fact it exists or otherwise.

All Thai MoD intelligence agencies and units are governed under the Organization of Ministry of Defence Act B.E. 2551 (2008)[14]. This is the primary legislation for all military TIC agencies. Additional supporting and/or overarching legislation governing TIC military agency operations and functions is provided by the **Official Information Act, B.E. 2540 (1997); Regulations on Maintenance of Official Secrets, B.E. 2544 (2001)**; Regulations of the Office of the Prime Minister on National Security, B.E. 2552 (2009); with overarching though non-specific legislation provided by the **Constitution of the Kingdom of Thailand, B.E. 2560 (2017)**[15]. From a transparency perspective, the Official Information Act provides scope for the public to request information from Government, subject to provisions in other legislation pertaining to official secrets and information that may jeopardise the monarchy or national security[16].

[14] Lieutenant General Natee Wongissares, Director of Joint Intelligence, Royal Thai Armed Forces. Interview. 27 May 2020.

[15] Reinforced by all military interviewees, but specifically Lieutenant General Terdsak Dumkhum, Director General of Intelligence, Directorate of Intelligence, Royal Thai Army. Interview. 26 May 2020.

[16] Government of Thailand, Official Information Act, B.E. 2540 (1997), Chapter 2, Sections 14-12.

The RTP’s Special Branch operates under the Royal Thai Police Act B.E. 2547 (2004), and the Royal Decree on Roles within the RTP B.E.2558 (2015). As per the military organisations, it is also governed by the Official Information Act, B.E. 2540 (1997); Regulations on Maintenance of Official Secrets, B.E. 2544 (2001); and Regulations of the Office of the Prime Minister on National Security, B.E. 2552 (2009); which collectively determine confidentiality measures pertaining to state secrets and protection against leaks, espionage, terrorism and other threats[17].

NIA has particularly strong legislation underpinning its functions, but also providing clear parameters and limits for its operations and the public disclosure of information resulting from court orders by tribunals[18]. The National Intelligence Act, B.E. 2562 (2019) outlines the roles and tasks of the organisation and its director in much the same way as Ministerial Directives and Charter Letters do in the Australian intelligence accountability context. It also establishes a National Intelligence Coordination Center with power and authority to monitor, assess, and analyse situations both in and outside of Thailand, and to take remedial measures in cases of emergency. This in itself provides a degree of extra-departmental oversight of other TIC agency activities.

It should be noted that despite provisions for public disclosure in much of the legislation governing the TIC agencies described above, sections 26, 28, 32, 33 and 36 of the Constitution of the Kingdom of

[17] Police Major General Saksira Pheuak-um, Deputy Commissioner Royal Thai Police Special Branch Bureau. Interview. 29 June 2020.

[18] Government of Thailand, National Intelligence Act, B.E. 2562 (2019), Section 8.

Thailand, B.E. 2560 (2017) allow for the restriction of rights and liberties with regards to national security. In practice, this includes the limiting of transparency and accountability to some degree. Transparency is also made more difficult (hence raising suspicions and damaging public trust) when the legislation and regulations that govern some TIC agencies are difficult to find. In the author's opinion, the legislation and regulations governing TIC activities and operations should be easily accessible on each of the agency's respective public websites.

Governmental Committees. From an intelligence accountability and oversight perspective, there are four main committees of interest, all appointed by the Thai Senate, that function in this space. The Military Commission is tasked with monitoring and providing recommendations to the military as deemed fit. It also has the authority to conduct inquiries on any military matter, including military intelligence, that they may be interested in or may be of public interest[19]. Whilst their purview includes the TIC military agencies, they are but a small part of the Military Commission's remit and so any oversight would be minimal at best. The Military Commission is chaired by the Prime Minister.

The RTP also has a senate-appointed oversight committee, the Police Commission, also chaired by the Prime Minister. They have a similar role to the Military Commission, but for the RTP. They also look at police ethics and regulations to govern and improve police behaviour[20].

[19] Lieutenant General Natee Wongissares, Director of Joint Intelligence, Royal Thai Armed Forces. Interview. 27 May 2020.

[20] Police Major General Saksira Pheuak-um, Deputy Commissioner Royal Thai Police Special Branch Bureau. Interview. 29 June 2020.

Additionally, there are Standing Committees of the National Legislative Assembly to review thematic areas of national governance. The two potentially pertinent to intelligence accountability are the Senate Standing Committee on the Armed Forces and State Security and the Senate Standing Committee on Laws, Justice Procedure and Police Affairs. The Senate Standing Committee on the Armed Forces and State Security has duties and powers to consider organic law bills, bills, carry out activities, consider undertaking fact-finding or study any matter concerning the administration of the State security, the development of bureaucratic systems including the systematization of the central and provincial administration, the performance of duties of state officials as well as protecting and maintaining the security of state and military affairs. The Committee on Laws, Justice Procedure and Police Affairs has duties and powers to consider organic law bills, bills, carry out activities, consider undertaking fact-finding or study any matter concerning the legal system, justice procedure, as well as human rights, consumers' protection and police affairs[21]. The Opposition is not represented in these committees, undermining their independence and effectiveness as oversight and accountability mechanisms in general. They are also not intelligence-specific, so their role in Thailand's intelligence accountability framework, whilst having potential, is relatively weak.

The National Security Council. Whilst the purpose of this paper is not to explore the detailed workings of the Thai National Security Council, it clearly plays an important role in directing, guiding, coordinating and overseeing TIC activities. The Thai NSC is the functional equivalent of

[21] https://www.senate.go.th/assets/portals/1/files/form_load/ Dutiesand Power_ommittees.pdf

FICC, SCNS and NSC in Australia. Similar to the NSC in Australia, the Thai NSC is the focal point of decision making on national security. It is chaired by the Prime Minister with the Deputy Prime Minister acting as deputy chair and the remainder of the quorum being various ministers. In terms of oversight, the NSC's remit is more about effectiveness of intelligence reporting and TIC agencies' operations rather than intelligence accountability. Similar to Australia, whilst not providing direct oversight of the TIC *per se*, the nature of the relationship and makeup of the NSC ensures that the TIC operates within parameters set by the NSC.

Courts, Tribunals and Ombudsmen. Like all Government departments and organisations in both Thailand and Australia, TIC agencies subject to the rule of law. As such, their actions are open to scrutiny by courts and tribunals. This does not in itself imply oversight authority or responsibility for the courts but means that TIC agencies are legally accountable for their actions.

The Office of the Ombudsmen Thailand is a relatively recent innovation, having been established late last century under the Ombudsman Act of B.E. 2542 (1999). It is not a typically or traditionally Thai style of institution, and in practice, operates at a relatively high level within the bureaucracy. Apart from considering and investigating circumstances and providing justice to people who have been treated unfairly by all types of civil servants or State employees, additional roles of the Ombudsman are to oversee the ethical practice of politicians, government officials or state officials as well as to establish a Code of Ethics to be followed by all agencies. It is also tasked to follow up and provide recommendations in compliance with the Constitution as well as matters for consideration in support of Constitutional amendment[22]. In practice, it is extremely rare for the Ombudsman to become involved or investigate matters pertaining to intelligence in Thailand.

Role of the Media. As in Australia, the media plays a significant role in scrutinising Government in Thailand (and by extension, the arms of government such as the NIC and the TIC). With regards to intelligence agency accountability, the role of the media in Thailand takes on greater significance however, due to the lack of truly independent statutory intelligence oversight bodies. Strict media censorship makes the job even more difficult, and arguably therefore even more important. Due to cultural and systemic practices, it would not be usual for oversight bodies (Inspectors General for instance) to initiate a review or investigation of intelligence activities unless sparked by an external vector such as an unfavourable media report. From an intelligence accountability perspective, this is not a great way to conduct business. The media should be complementary to, not a substitute for, a self-starting, truly independent statutory oversight body. In the NIC context, this is IGIS.

Summary. Extra-departmental accountability for Thailand's intelligence community, therefore, consists of legislation; Governmental committees; the Thai National Security Council; and courts, tribunals and ombudsmen. The media also plays a significant non-official role in identifying issues requiring investigation or further scrutiny. The TIC's external accountability framework does not appear as robust or as comprehensive as Australia's. Indeed, having the Prime Minister chair many of these oversight bodies allows claims of 'conflict of interest' to arise from external observers, and that the Thai system allows 'the fox

[22] https://www.ombudsman.go.th/10/eng/2_1.asp

into the henhouse' colloquially speaking. Strengthening this element of the Thai intelligence accountability framework would ensure the TIC and its individual constituent agencies, remain as transparent and accountable to the public as possible, within the operational constraints of their secret work, for its management, functioning, use of resources and output. This builds trust and support amongst the community and the media, strengthening internal security and promoting national harmony.

Summary

Despite Thailand and Australia having different forms of Government, different external threat and internal security contexts (and therefore intelligence agencies with different roles and functions), organisational architectural similarities in form and function are able to be distilled in a macro sense. For instance, both national intelligence systems have complimentary internal and external accountability arrangements, clearly defined or otherwise, although they bear little resemblance to each other. However, Thai intelligence accountability frameworks are generally less well defined, regulated and legislated than in Australia. This would seem particularly so with the external intelligence accountability framework.

Intra-departmental intelligence accountability for TIC elements comprise Ministerial oversight, respective chains of command and departments of Inspectors General in each of the TIC agencies less NIA. Authority vested in chains of command is the key pillar of the internal intelligence accountability framework in Thailand. To a degree, legislation also partially covers some of the accountability requirements encapsulated in the Australian system by Ministerial Directives, Charter Letters from departmental secretaries to agency heads, OPA between those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments. Collectively, this results in a very robust internal accountability framework and ensures that each TIC agency is accountable within its respective department for its management, functioning, use of resources and output. Some improvements are possible with regards to definition of the accountability framework, and greater empowerment of Inspectors General within each of the military agencies to provide assurance to the chain of command.

Extra-departmental intelligence accountability for Thailand's intelligence community comprises legislation; Governmental committees; the Thai National Security Council; and courts, tribunals and ombudsmen. Legislation is the key element of the external intelligence accountability framework in Thailand. The media also plays a significant non-official role in identifying issues requiring investigation or further scrutiny. The TIC's external accountability framework does not appear as robust or as comprehensive as Australia's. Indeed, having the Prime Minister chair many of these oversight bodies allows claims of 'conflict of interest' to arise from external observers, and that the Thai system allows 'the fox into the henhouse' colloquially speaking. Additionally, the lack of a truly independent statutory intelligence oversight body means that transparency and accountability, to an outside observer, are not necessarily comprehensive and invite greater scrutiny rather than alleviating concerns.

Chapter 6
Conclusion and Recommendations

Comparing the Australian and Thai Systems

In Australia over the last 30 years, greater scrutiny and oversight in corporate governance and accountability have developed within Government, including the NIC, along with increased attention to citizen rights. The continuum of accountability relationships developed between the public, the Parliament, the Government and the various agencies of the NIC has resulted in a high degree of transparency in NIC activities, ensuring agencies act legally and with propriety, comply with ministerial guidelines and respect human rights. This increased transparency of intelligence agencies for the public (within practical, operational and security limitations) has increased the level of trust in government and public support for the national intelligence institutions. This in turn has increased the effectiveness of Australia's internal security intelligence agency (ASIO) along with that of the various non-NIC homeland security intelligence agencies including the various police jurisdictions and the ACIC.

Australia has developed an intelligence accountability framework that attempts to reconcile democratic practices with maintaining organisations that necessarily work in secrecy. Balancing the concepts of 'need to know' and 'right to know' is central to this accountability framework. Clearly, much intelligence work needs to be done behind closed doors. The purpose of secrecy is to facilitate the proper functioning of government, but it needs to be balanced against other competing public interests including the public's right to know. It is the role of accountability frameworks to ensure this balance is maintained, minimising community apprehension pertaining to intelligence activities and damage to the trust relationship between the Government and its constituency. Australia's intelligence accountability framework comprises both intra-departmental (internal) and extra-departmental (external) facets that work together in achieving the necessary balance required.

The internal accountability framework residing within the Australian governmental departments that NIC agencies belong to is affected on three levels : individual, committee and organisational. Specifically, intra-departmental accountability consists of Ministerial oversight, Charter Letters from departmental secretaries to agency heads, OPA between those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments. External accountability is affected through legislation; the Parliamentary Joint Committee on Intelligence and Security; committees of Cabinet including the NSC and SCNS; courts, tribunals and ombudsmen; and an independent statutory oversight body in IGIS.

In Thailand, the context is somewhat different. Vastly different national histories and geopolitical circumstances; systems of government; roles, functions and purposes of the various intelligence agencies; weighting differences between internal and external national security focus; threat environments; extant alliance structures; technical and technological capabilities; and cultural factors have resulted in systems and norms not akin to Australia's or, indeed, those of the Western world. Thailand does not generally share the same definition of, or need for intelligence oversight and accountability as does Australia. Indeed, there is no comprehensive definition or understanding of an intelligence accountability framework or architecture. That said, despite the fundamental differences, Thailand does have an intelligence accountability framework, and organisational architectural similarities in form and function are able to be distilled in a macro sense. For instance, both national intelligence systems have complimentary internal and external accountability arrangements, clearly defined or otherwise, although they bear little resemblance to each other.

In general, the Thai government is more concerned with the effectiveness of intelligence reporting and TIC agencies' operations in support of national security rather than intelligence accountability. Thai intelligence accountability frameworks are more complicated, less well defined, regulated and legislated than in Australia due to those same issues outlined above. Similarly, and again for the same reasons, Thailand's internal intelligence accountability framework is much stronger than its external intelligence accountability framework.

Intra-departmental (internal) intelligence accountability for TIC elements comprise Ministerial oversight, respective chains of command and departments of Inspectors General in each of the TIC agencies less NIA. Authority vested in chains of command is the key pillar of the internal intelligence accountability framework in Thailand. To a degree, legislation also partially covers some of the accountability requirements encapsulated in the Australian system by Ministerial Directives, Charter Letters from departmental secretaries to agency heads, OPA between those same individuals and CSA between NIC agencies and their Enabling Programs within respective departments. Collectively, this results in a relatively robust internal accountability framework and ensures that each TIC agency is accountable within its respective department for its management, functioning, use of resources and output.

By way of improvement, in the author's opinion, the internal intelligence accountability system would benefit from being more clearly defined, recognised and understood within the TIC itself. Written directives, publicly available, from the responsible Minister to each of the TIC agency heads would also aid understanding and enhance transparency, building trust in the community without undermining Government and TIC goals. Additionally, stronger IG departments with broader powers of oversight would significantly enhance internal accountability and provide commanders in chief greater control and oversight of their respective intelligence agencies. This in turn would likely result in more focussed, efficient and effective intelligence operations and outcomes.

Extra-departmental (external) intelligence accountability for Thailand's intelligence community comprises legislation; Governmental committees; the Thai National Security Council; and courts, tribunals and ombudsmen. Legislation is the key element of the external intelligence accountability framework in Thailand. The media also plays a significant non-official role in identifying issues requiring investigation or further scrutiny. Unfortunately, despite having generally strong legislation governing TIC agency activities, there are several weaknesses in the external framework. This includes senate oversight committees that are neither bipartisan nor intelligence-specific, and are chaired by the Prime Minister. They can therefore hardly be independent nor impartial oversight bodies. But perhaps the largest hole in Thailand's intelligence accountability architecture is that of an independent statutory oversight body, unencumbered by politics, to review the activities and operations of the TIC to ensure compliance with the relevant legislation and regulatory instruments.

A tabular comparison of the internal and external elements of the two national intelligence accountability frameworks is below. The elements of both nations' intelligence accountability frameworks are traffic light colour coded according to effectiveness and where more work needs to be done, in the author's opinion. Green denotes effective / no further action required. Amber denotes partially effective / some amendments needed. Red denotes ineffective / significant further action required.

Table 6-1 Tabular Comparison of Australian and Thai National Intelligence Internal Accountability Framework Mechanisms

Accountability Framework	**Mechanism**	**Australia**	**Thailand**	**Remarks**
Internal	Ministerial Oversight	Yes	Yes (including where delegated, for instance MoD Intel Board and RTP Board)	More centrally controlled in Thailand (e.g. NIA and RTP report to PM, PM is Defence and Police Minister, Deputy PM acts as an ‘Intel Czar’ of sorts).
	Directives to Agency Heads	Yes	Some	Thailand’s not well defined and mostly verbal. Mitigated by strong chains of command, though should still be defined.
	Agency Performance Agreements	Yes	Some	Informal in Thailand. Some captured in legislation (NIA). Better definition needed.

	Agency Inspectors General	No (Not needed due to IGIS role and function, but could be included in respective ministries)	Most	None in NIA. Thai IG are well structured, but not empowered for oversight & accountability.
	Agency Supply Agreements	Yes	No	Minor issue in Thai context due to strong chains of command.

Table 6-2 Tabular Comparison of Australian and Thai National Intelligence External Accountability Framework Mechanisms

Accountability Framework	**Mechanism**	**Australia**	**Thailand**	**Remarks**
External	Legislation	Yes (various, all agencies covered)	Yes (various, all agencies covered)	Neither country has complete over-arching intelligence legislation, but both systems are strong enough.
	Governmental Oversight Committees	Yes (PJCIS)	Yes (Senate Standing Committee for Armed Forces / Military Commission; Senate Standing Committee for Police / Police Commission)	Opposition not included in Thai system. Senate committees not independent nor intel-specific and hence relatively weak. PM as chair undermines independence of the committees.

	Directing and Coordinating Bodies	Yes (NSC, SCNS, FICC, ONI)	Yes (NSC, NIA-NICC)	Australian system overly complicated.
	Courts, Tribunals and Ombudsmen	Yes	Yes	More accessible to the public in Australia, and probably more effective in terms of providing transparency and accountability. Relatively minor aspects.
	Independent Statutory Oversight Body	Yes (IGIS)	No	Key issue. No independence of oversight (and therefore accountability) in Thailand.

Recommendations

Stemming from the research, the recommendations provided below are the author's opinion only, and are those the author believes are achievable and would provide benefit to Thailand's national security apparatus. The recommendations can be broken down into four main areas : define and implement, strengthen, publicise and develop, and are as follows :

1. DEFINE AND IMPLEMENT. Firstly, and most importantly, Thailand's intelligence accountability framework, both internal and external, needs to be clearly defined. This paper goes some way in achieving that. The architecture already exists, as described in the paper above, it just requires formal definition and some modification to become an effective tool of Government. The defined intelligence accountability framework should be included in the National Strategy for Intelligence and made public to the best and greatest degree possible. Adoption and implementation of this newly defined intelligence accountability framework should be enforced upon the TIC from the highest level of Government to ensure it is mandatory, not optional, for all agencies.

2. STRENGTHEN. Strengthening the accountability framework would provide greater assurance to the Prime Minister and Government's senior leadership regarding the direction, actions and activities of the TIC; develop greater public trust in Thailand's intelligence system; diminish the ability of media to undermine systems and processes under the guise of transparency; while at the same time enhancing the capability of Thailand's national security apparatus. Reconciling secretive intelligence work with democratic ideals, although sometimes difficult, will become easier and less ambiguous over time with the implementation, maintenance and development of a robust accountability framework governing the work of Thailand's intelligence agencies. Enhance public trust in the national security apparatus provides a solid mandate to undertake the necessary intelligence work, sometimes distasteful, with the backing of the population. This can only enhance the effectiveness and efficiency of TIC agencies. Specifically, recommendations for strengthening the Thai national intelligence accountability framework include:

2.1 In the author's opinion, Thailand would benefit from more formal arrangements associated with the TIC's internal accountability structure that detail key results required and clear accountability arrangements, but not the means by which results are to be achieved. This would encourage accountable innovation within TIC agencies, whilst improving effectiveness. In Australia, this is done through Charter Letters and Agency Performance Agreements. This formalises and crystallises relationships, allowing for greater accountability and transparency. These are simple measures that cost little and provide benefit from an external scrutiny perspective.

2.2 In the author's opinion, the legislation and regulations governing TIC activities and operations should be easily accessible on each of the agency's respective public websites. These websites are the first portals visited from an accountability perspective. Currently, they are not very well organised and not very useful. They should be used as an effective information operations tool to educate the public and assuage public concerns about the activities of the TIC. The first step in this process is to ensure the public that there are no rogue organisations here – each and every one is covered by robust legislation and a strict regime of oversight and accountability, and where possible, transparency to the greatest permissible degree. TIC agency websites should be simple, clear, consistent and helpful.

2.3 In the author's opinion, stronger Inspectors General departments with broader powers of oversight would significantly enhance internal accountability and provide commanders in chief greater control of their respective intelligence agencies. This in turn would likely result in more focussed, efficient and effective intelligence operations and outcomes. The organisations are already in place, they just need to be empowered for the oversight and accountability functions.

2.4 Of Dubnick's four pillars of accountability (legal, organisational, professional and political), the political component in Thailand comprises the extra-departmental oversight and review activities of various committees and commissions. In the author's opinion, despite Thailand having elements of the political facet of accountability in place, their effectiveness and coverage is relatively poor. There are no doubt political, legal and constitutional reasons for this, although discussion of these issues in depth is not the aim of this paper. It is recommended that the roles and tasks of the Senate Standing Committee for Armed Forces and State Security / Military Commission, the Senate Standing Committee for Law, Justice Procedure and Police Affairs / Police Commission, the RTP Board and the MoD's Intelligence Board be reviewed and amended to include greater provision for intelligence accountability and oversight from a holistic perspective, not just in a review and investigative capacity. Similar roles and responsibilities to Australia's PJCIS are recommended.

2.5 In the author's opinion, the most significant element missing from Thailand's national intelligence accountability framework is an independent statutory organisation to provide oversight and accountability for all TIC agencies, that can report without fear or favour, and remains answerable to Government, though independent of Government influence. It could also be the public conduit for transparency of the TIC, to the greatest extent possible, given the requirement of TIC agencies to operate in secret. It is in this manner that TIC agencies can be seen to be accountable to both Government and the public, that the rights and needs of the public are satisfied to the greatest degree possible, and that organisations and agencies necessarily working in secret are nonetheless transparent, open, honest and held responsible for their actions.

Strengthening the system through implementation of the recommendations above would go a long way towards overcoming the apparent paradox of secrecy within a democratic society in the eyes of both the Government and the public.

3. PUBLICISE. Once Thailand’s intelligence accountability architecture is defined, implemented and strengthened, it is recommended that it should be publicised as widely as possible. Media and academia should be invited to a briefing on the system and how it provides benefit the public, Government and national security alike. Indeed, requesting recommendations for improvement from the public, including the media and academics, would only help strengthen the system and elicit buy-in from those who will benefit from enhanced national security – all Thais.

4. DEVELOP. Although this paper goes some way to describing the Thailand’s national intelligence accountability framework, more research and work is required to refine the definition of the system and include all of Thailand’s national security agencies in a broader architecture. Sending a Thai delegation to Australia to study the NIC’s accountability framework and take away elements beneficial to Thailand would be beneficial. In the author's opinion, Thailand's intelligence landscape is far too complex for the mission sets required of various agencies. Many agency missions, roles, responsibilities and tasks overlap. Clarification holistically across the entire spectrum of Thailand's intelligence and security apparatus would be beneficial to avoid confusion, duplication of effort, inter-agency fratricide and rank inefficiency that in the author's opinion, are apparent in today's system. Further research and review in this area would be of great benefit to the system as a whole, and therefore ultimately to Thailand's national security.

Bibliography

Books, Journals, Newspapers and Websites

Andrews, E., 2001, The Department of Defence, Oxford University Press, Melbourne. Archives Act, 1983, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00179

Asian Political and International Studies Association website accessed via the internet on 28 April 2020 at https://www.apisa.org/programs/security_sector.html

Auditor-General Act, 1996, accessed via the internet on 19 January 2020 at http://www.legislation.act.gov.au/a/1996-23/current/pdf/1996-23.pdf.

Australian Bureau of Criminal Intelligence (ABCI), 1997, Guiding Principles for Law Enforcement Intelligence, developed during Critical Issues Seminar : Standing Committee on Organised Crime and Criminal Intelligence, Australian Institute of Police, Manly, NSW.

Australian Security Intelligence Organisation website accessed via the internet on 28 April 2020 at http://www.asio.gov.au.

Australian Security Intelligence Organisation Act, 1979, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00240

Australian Secret Intelligence Service website accessed via the internet on 28 April 2020 at http://www.asis.gov.au.

Australian Signals Directorate website accessed via the internet on 28 April 2020 at https://www.asd.gov.au/

Barrett, P., Government Sector Accountability – The Impact of Service Charters in the Australian Public Service, Commonwealth of Australia, Canberra. 2003,

Barrett, P., Balancing Accountability and Efficiency in a More Competitive Public Sector Environment, extract from a speech delivered at the Government-in-Excellence Summit 2000, 'Reinventing Government – a Manifesto for Achieving Excellence and Managing for Results in the New Millennium',24-26 May 2000, Singapore. 2000,

Blick, B., Opening Address (Unpublished Paper), Annual Conference of the Australian Institute of Professional Intelligence Officers 'Intel 98', AIPIO, Melbourne. 1998,

Born, H. and Leigh, B., Democratic Accountability of Intelligence Services, Policy Paper No. 19, Geneva Centre for the Democratic Control of Armed Forces, Geneva. 2007,

Cain, F., 1994, ASIO: An Unofficial History, Spectrum Publications, Melbourne.

Chambers, P., 2014, A Dearth of Demilitarization, Centre for Security Governance, accessed via the internet on 19 January 2020 at https://www.secgovcentre.org/2014/07/32847/

Chambers, P., Civil-Military Relations in Thailand since the 2014 Coup : The Tragedy of Security Sector "Deform", Peace Research Institute, Frankfurt, accessed via the internet on 19 January 2020 at https://www.jstor.org/stable/resrep14467.7, 2016.

Chambers, P., Obstacles to Civilian Control of the Security Sector in Thailand, Middle East Institute, accessed via the internet o n 20January 2020 at https://www.mei.edu/publications/obstacles-civilian-control-security-sector-thailand, 2014.

Chongkittavorn, K., Thai Intelligence Agencies Need a Revamp, accessed via the internet on 20 January 2020 at https://www.nationthailand.com/opinion/30276574 2016,

Cimbala, S., 1987, Intelligence and Intelligence Policy in a Democratic Society, Transnational Publishers Inc., New York.

Commission of Inquiry into the Australian Secret Intelligence Service, 1995, Report on the Australian Secret Intelligence Service: Public Edition, Australian Government Publishing Service, Canberra.

Commonwealth of Australia, 1977, Intelligence and Security Royal Commission, First Report, Commonwealth Government Printer, Canberra.

Commonwealth of Australia, 1977, Intelligence and Security Royal Commission, Second Report, Commonwealth Government Printer, Canberra.

Commonwealth of Australia, 1977, Intelligence and Security Royal Commission, Third Report (Abridged Findings and Recommendations), Commonwealth Government Printer, Canberra.

Commonwealth of Australia, 1977, Intelligence and Security Royal Commission, Fourth Report Vol. I Parliamentary Paper 249/1977, Commonwealth Government Printer, Canberra.

Commonwealth of Australia, 1977, Intelligence and Security Royal Commission, Fourth Report Vol. II Parliamentary Paper 249/1977, Commonwealth Government Printer, Canberra.

Commonwealth Ombudsman website accessed via the internet on 28 April 2020 at http://www.ombudsman.gov.au/.

Defence Imagery and Geospatial Organisation website accessed via the internet on 28 April 2020 at https://defence.gov.au/ago/

Defence Intelligence Organisation website accessed via the internet on 28 April 2020 at https://www.defence.gov.au/dio/index.shtml

Delbridge, A., Bernard, J.R.L., Blair, D., Butler, S., Peters, P., and Yallop, C., (eds), 1997, The Macquarie Dictionary, 3rd Edition, The Macquarie Library Pty Ltd, Sydney.

Department of Defence Media Release, 26 June 2000, Good Governance to Underpin Defence Renewal, www.defence.gov.au/media /DeptTpl.cfm?Current, last viewed 19 April 2020.

Department of the Parliamentary Library, Bills Digest No. 11 2001-02, Intelligence Services Bill 2001.

Douglas, R., 1998, 'Administrative Law and Good Government' in Sampford, C. and Preston, N. (eds), Public Sector Ethics, The Federation Press, Sydney.

Draper, J., 2016, Special Circumstances, accessed via the internet on 10 April 2020 at https://prachatai.com/english/node/6183

Dubnick, M., 1998, 'Clarifying Accountability – An Ethical Framework' in Sampford, C. and Preston, N. (eds), Public Sector Ethics, The Federation Press, Sydney.

Financial Framework (Supplementary Powers) Act, 1997, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2015C00191

Flanagan, S., Managing the Intelligence Community, International Security, vol. 10, no. 1, 1985.

Forell, C., How we are Governed, Longman Cheshire Pty Ltd, Melbourne Geneva Centre for Security Sector Governance website accessed via the internet on 19 January 2020 at https://www.issat.dcaf.ch/Learn/SSR-Overview, 1986.

Gill, P., Policing Politics: Security Intelligence and the Liberal Democratic State, Frank Cass and Co. Ltd., London., 1994.

Holt, P., "The Media" in Secret Intelligence and Public Policy, pp 171-188, Congressional Quarterly, USA., 1995.

Horner, D., Blaxland, J., and Crawley, R., The Official History of ASIO, Allen & Unwin, Sydney, 2015.

Inspector General of Intelligence and Security Annual Report 2018-19 accessed via the internet on 19 April 2020 athttps://www.igis.govcms.gov.au/Annual-Report-2018-2019/site/index.html

Inspector General of Intelligence and Security website accessed via the internet on 23 December 2019 at http://www.igis.gov.au.

Inspector General of Intelligence and Security Act, 1986, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00021

Intelligence Services Act, 2001, accessed via the internet on 19 January 2020 https://www.legislation.gov.au/Details/C2020C00029

Intelligence Services (Consequential Provisions) Act, 2001, accessed via the internet on 28 April 2020 at https://www.legislation.gov.au /Details/C2004A00929.

Janthayanot, D., National Road Traffic Management Strategy, The National Defence College of Thailand Journal, Vol. 61, No. 3 September-December 2019, pp 8-30.

Joint Select Committee on the Intelligence Services. Report of Intelligence Services Committee – Findings and Recommendations, dated 27 August 2001.

Karkoszka, A., The Concept of Security Sector Reform, Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva, accessed via the internet on 19 January 2020 at https://www.un.org/ruleoflaw/files/Karkoszka.pdf, 2003.

Khan, A., Thailand To Consolidate Work of 27 Intelligence Agencies, accessed via the internet on 27 June 2020 at https://www.defenseworld.net/news/19867/Thailand_To_Consolidate_Work_of_27_Intelligence_Agencies#.Xvb8H-biuUk, 2017.

Kisak, P. Encyclopedia of Intelligence and Counterintelligence, Carlisle, R. (ed), Routledge, London, 2004.

Kitiyadisai, K., Information Systems for National Security in Thailand: Ethical Issues and Policy Implications, Journal of Information, Communication and Ethics in Society, Vol. 6 No. 2, pp. 141-160. 2008,

Knightley, P. The Second Oldest Profession, Pan, London., 1987.

Kocak D., and Kode J. ‘Impediments to Security Sector Reform’ in Thailand in Heiduk F. (ed), Security Sector Reform in Southeast Asia, Critical Studies of the Asia PacificSeries, Palgrave Macmillan, London. , 2014,

McComas, H. ‘Quis custodies custodiet?’ Who Will Guard the Guardians? Accountability in Intelligence, The Journal of the Australian Institute of Professional Intelligence Officers, Vol. 10, No. 2, 2002, AIPIO, Canberra., 2002.

McLeod, R. Ethics and Accountability, presented during the Annual Conference of the Australian Institute of Professional Intelligence Officers ‘Intel 95’, AIPIO, Sydney, 1995.

Mendel, T. The Public’s Right to Know : Principles on Freedom of Information Legislation, accessed via the internet on 19 January 2020 at https://www.article19.org/data/files/pdfs/standards/righttoknow.pdf. 1999,

National Intelligence Act 2019, accessed via the internet on 23 December 2019 at http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/050/T_0022.PDF

National Intelligence Agency website accessed via the internet on 23 December 2019 at https://www.nia.go.th/niaweb59/default_EN.asp

National Security website accessed via the internet on 19 January 2020 at https://www.nationalsecurity.gov.au/WhatAustraliaisdoing/Pages/National SecurityAgencies.aspx.

Office of National Intelligence website accessed via the internet on 19 January 2020 at https://www.oni.gov.au/.

Office of National Intelligence Act, 2018, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2018A00155

Ombudsman Act, 1976, accessed via the internet on 28 April 2020 at http://www.austlii.edu.au/au/legis/cth/consol_act/oa1976114/.

Parliamentary Joint Committee on Intelligence and Security website accessed via the internet on 19 January 2020 https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security

Parliamentary Joint Committee on the Australian Security Intelligence Organisation, 2000, A Watching Brief: The Nature, Scope and Appropriateness of ASIO's Public Reporting Activities, The Parliament of the Commonwealth of Australia, Canberra.

Prachathai, 2015, 10 Ways to Revolutionize the Thai Military: Exposing the Junta's Blind Spot, accessed via the internet on 23 December 2019 at www.prachatai.com/english/node/5611

Prachathai, New National Intelligence Act Sanctions Use of Electronic Tools to Access Private Information, accessed via the internet on 23 December 2019 at https://www.prachatai.com/english/node/80262019,

Public Service Act, 1999, accessed via the internet on 19 January 2020 at https://www.legislation.gov.au/Details/C2019C00057

Royal Thai Air Force website accessed via the internet on 23 December 2019 at http://www.rtaf.mi.th/th/Pages/default.aspx

Royal Thai Armed Forces Armed Forces Security Centre website accessed via the internet on 23 December 2019 at http://www.conf.17ram.org/

Royal Thai Armed Forces website accessed via the internet on 23 December 2019 at https://www.rtarf.mi.th/index.php/en/2016-06-23-07-14-58/2016-06-24-03-50-12

Royal Thai Army website accessed via the internet on 23 December 2019 at https://www.rta.mi.th/rta_website_v2/

Royal Thai Navy website accessed via the internet on 23 December 2019 at https://www.navy.mi.th/index.php/main/index?language=en

Royal Thai Police Special Branch Bureau website accessed via the internet on 23 December 2019 at https://www.sbpolice.go.th/

Sampford, C. and Preston, N. (eds), 1998, Public Sector Ethics, The Federation Press, Sydney.

Sombatpoonsiri, J., 2018, Securing Peace? Regime Types and Security Sector Reform in the Patani (Thailand) and Bangsamoro (the Philippines) Peace Processes, 2011–2016, Strategic

Analysis, accessed via the internet on 23 December 2019 at https://www.tandfonline.com/doi/abs/10.1080/09700161.2018.1482628

Sookmark, K., Security Sector Reform in the National and Regional Contexts, Seminar Summary and Conclusions, accessed via the internet on 23 December 2019 at http://www.archive.ipu.org/splz-e/Phuket06/report.pdf, 2006.

Privacy International State of Privacy Thailand, website accessed via the internet on 23 December 2019 at https://privacyinternational.org/state-privacy/1011/state-privacy-thailand, 2017,

Thai Netizen Network website accessed via the internet on 23 December 2019 at https://www.apc.org/en/member/thai-netizen-network

Thailand to Consolidate Work of 27 Intelligence Agencies, 13 July 2017, accessed via the internet on 23 December 2019 at https://www.defenseworld.net/news/19867/Thailand_To_Consolidate_Work_of_27_Intelligence_Agencies#.XqftBfZuJaQ

Thompson, D., Political Ethics and Public Office, Harvard University Press, Harvard, 1987.

Toohey, B., and Pinwell, W., Oyster, Mandarin Australia, Melbourne, 1990.

Treverton, G. Reshaping National Intelligence in an Age of Information, Cambridge University Press, Cambridge, 2001.

United Nations, Unanimously Adopting Resolution 2151 (2014), Security Council Underscores Need for National Ownership of Security-Sector Reform, accessed via the internet on 23 December 2019 at https://www.un.org/press/en/2014/sc11369. doc.htm, 2014.

United Nations, UNDP sees Security Sector Reform as Foundation for Peace and Development, accessed via the internet on 23 December 2019 at https://www.undp.org/content/undp/en/home/presscenter/articles/2015/02/13/undp-sees-security-sector-reform-as-foundation-for-peace-and-development-.html2015,

United Nations, Security Sector Reform, United Nations and the Rule of Law website accessed via the internet on 23 December 2019 at https://www.un.org/ruleoflaw/thematic-areas/access-to-justice-and-rule-of-law-institutions/ssr/, 2020.

United Nations, Securing States and Societies : Strengthening the United Nations Comprehensive Support to Security Sector Reform, accessed via the internet on 23 December 2019 at https://www.un.org/en/ga/search/view_doc.asp?symbol=S/2013/480, 2013.

Wanandi, J. Theory and Practices of Security Sector Reform : The Case of Indonesia, Centre for Strategic and International Studies, Jakarta, accessed via the internet on 23 December 2019 at https://www.un.org/ruleoflaw/files/Wanandi.pdf, 2003,

Wigan, B., Intelligence and Security: A Realistic Conception Promoting Justice, the Protection of Rights and a Quality of Life, presented at the QUT Justice Studies Conference, Queensland University of Technology, Brisbane, 1993.

Interviews

Air Marshal Punpakdee Pattanakul, Director of Intelligence, Royal Thai Air Force. Interview. 21 May 2020.

Lieutenant General Terdsak Dumkhum, Director General of Intelligence, Directorate of Intelligence, Royal Thai Army. Interview. 26 May 2020.

Lieutenant General Natee Wongissares, Director of Joint Intelligence, Royal Thai Armed Forces. Interview. 27 May 2020.

Vice Admiral Wuttichai Saisatien, Director General, Naval Intelligence Department, Royal Thai Navy. Interview. 28 May 2020.

Lieutenant General Wichai Chucherd, Director General, Armed Forces Security Centre, Royal Thai Armed Forces. Interview. 11 June 2020.

Mr Krissada Aksornsong, Director Counter-Terrorism and Trans-National Crime, National Intelligence Agency. Interview. 23 June 2020.

Police Major General Saksira Pheuak-um, Deputy Commissioner Royal Thai Police Special Branch Bureau. Interview. 29 June 2020.

Major General Pongtep Gaewchaiyo, Deputy Director General Border Affairs, Royal Thai Armed Forces. Interview. 8 July 2020.

Appendix (if any)

ANNEX A
THE AUSTRALIAN NATIONAL INTELLIGENCE COMMUNITY (NIC)

The Australian National Intelligence Community, or NIC, is an informal term used to describe the six traditional Australian intelligence agencies. It comprises the following agencies:

The Office of National Intelligence (ONI) produces all-source assessments on international political, strategic and economic developments to the Prime Minister, senior ministers in the National Security Committee of Cabinet, and senior officials of government departments. ONI also has responsibility for coordinating and evaluating Australia's foreign intelligence activities.

The Australian Security Intelligence Organisation (ASIO) is Australia's national security service with a primarily domestic focus. ASIO's main role is to gather information and produce intelligence that will enable it to warn Government about activities or situations that might endanger Australia's national security.

The Australian Secret Intelligence Service (ASIS) is Australia's overseas human intelligence collection agency. Its mission is to protect and promote Australia's vital interests through the provision of unique foreign intelligence services as directed by Government.

The Australian Signals Directorate (ASD) is responsible for collection, analysis and distribution of foreign signals intelligence and is the national authority on communications and computer security.

The Defence Intelligence Organisation (DIO) is an intelligence assessment agency that provides services and advice at the national level. Its mandate is to support Defence and Government decision-making and assist with the planning and conduct of Australian Defence Force operations.

The Australian Geospatial-Intelligence Organisation (AGO) was established by amalgamating the Australian Imagery Organisation and Directorate of Strategic Military Geographic Information, and the Defence Topographic Agency to provide geospatial intelligence, from imagery and other sources, in support of Australia's defence and national interests.

ANNEX B
THE THAI INTELLIGENCE COMMUNITY - NIC EQUIVALENT AGENCIES

For the purposes of this paper, the Thai Intelligence Community is considered to comprise those agencies with comparable roles and tasks to the agencies of the Australian NIC. It is acknowledged that it is not a neat fit, there are no directly comparable agencies and the roles and tasks of Thai intelligence agencies differs significantly to those of Australian intelligence agencies. There are however, broad overlaps in remit between some Australian and Thai agencies despite being no true equivalence. Bearing this in mind, this paper will therefore only consider pure national intelligence agencies in the traditional sense, with security agencies and organisations being beyond its scope. Operational, tactical, intra-departmental and private intelligence sources and agencies are likewise not considered. To that end, for the purposes of this paper, the following organisations and agencies will be considered from an accountability framework perspective:

The National Intelligence Agency (NIA) is Thailand's counter-intelligence and security agency. It serves as part of the Office of the Prime Minister. It is broadly equivalent in remit to elements of ONI, ASD, ASIS and ASIO.

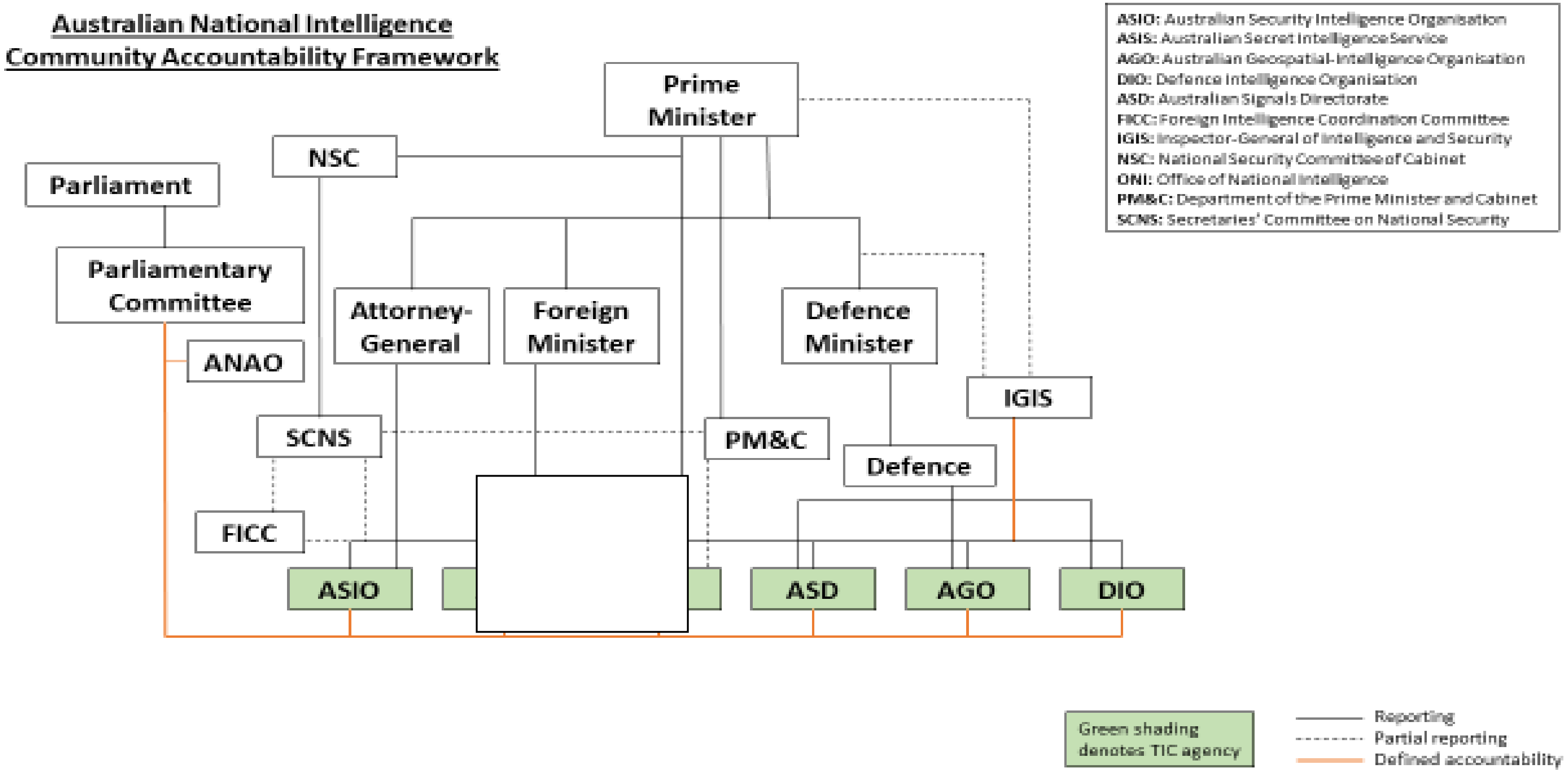
The Armed Forces Security Centre (AFSC) has a mission regarding intelligence and resistance to military intelligence. Also assists in providing security, together with other relevant departments, for the Royal Family and other VIPs. It also conducts military security intelligence and communications and signals intelligence work alongside intelligence education and training. It is broadly equivalent in remit to elements of ASD, DIO, ASIO and AGO.

The Intelligence Divisions of the Royal Thai Armed Forces (RTArF), Royal Thai Army (RTA), Royal Thai Navy (RTN) and the Royal Thai Air Force (RTAF) provide the intelligence functions for each of the respective services of the Thai military. They are broadly equivalent in remit to elements of DIO and AGO.

The Royal Thai Police Special Branch Bureau (SBB) is a law enforcement agency under the Royal Thai Police Headquarters. SBB's major functions are to provide security for the Royal Family and collect, produce and act on intelligence relating to people or groups presenting a threat to national security through subversive activities. Whilst there is no direct equivalent agency in Australia, some elements of SBB's remit are commensurate with parts of ASIO's roles and responsibilities.

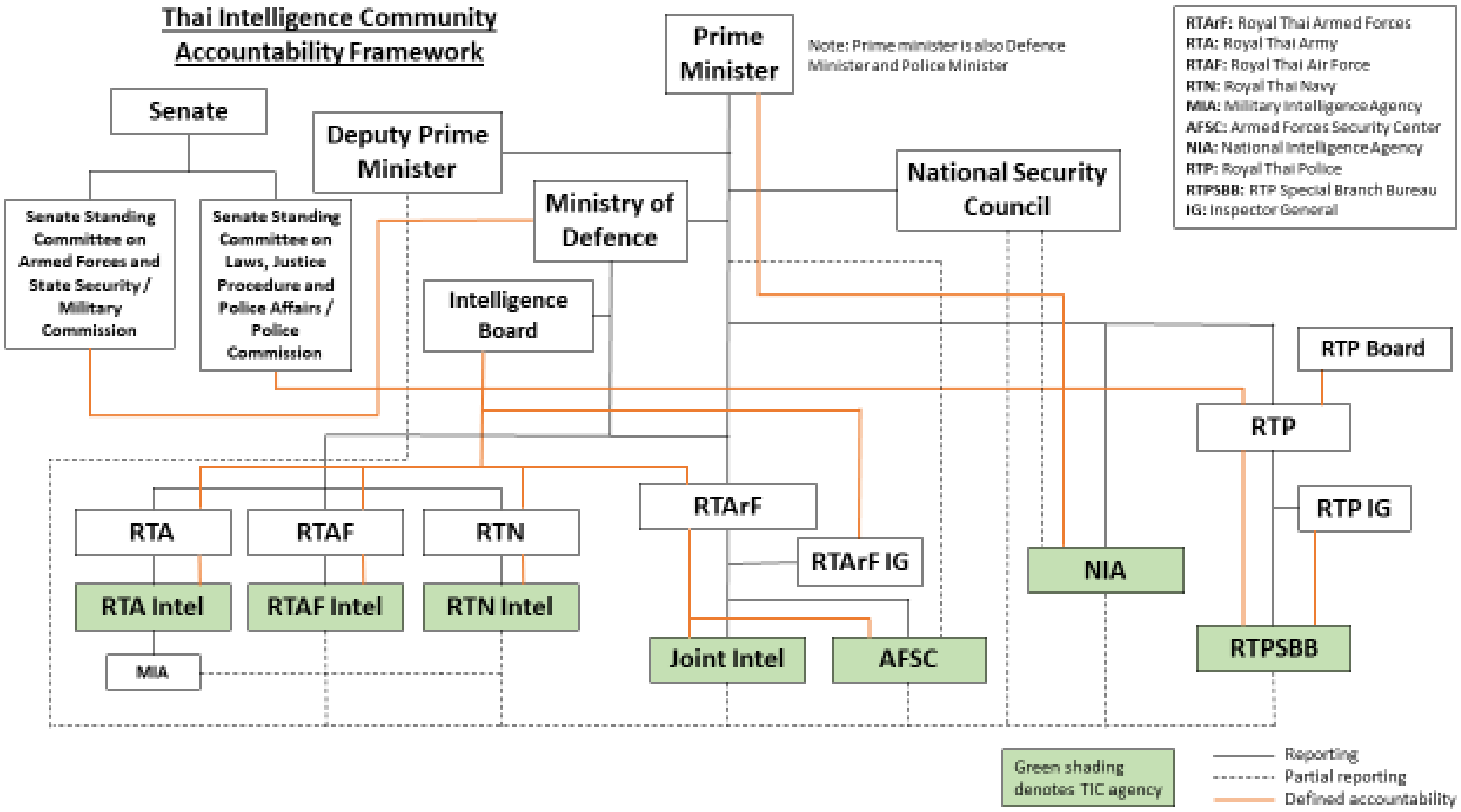
ANNEX C

AUSTRALIAN NATIONAL INTELLIGENCE COMMUNITY ACCOUNTABILITY FRAMEWORK


Australian National Intelligence Community Accountability Framework
Prime Minister
NSC
Parliament
Parliamentary Committee
ANAO
Attorney-General
Foreign Minister
Defence Minister
IGIS
SCNS
PM&C
Defence
FICC
ASIO
ASD
AGO
DIO
ASIO: Australian Security Intelligence Organisation
ASIS: Australian Secret Intelligence Service
AGO: Australian Geospatial-Intelligence Organisation
DIO: Defence Intelligence Organisation
ASD: Australian Signals Directorate
FICC: Foreign Intelligence Coordination Committee
IGIS: Inspector-General of Intelligence and Security
NSC: National Security Committee of Cabinet
ONI: Office of National Intelligence
PM&C: Department of the Prime Minister and Cabinet
SCNS: Secretaries' Committee on National Security
Green shading denotes TIC agency
Reporting
Partial reporting
Defined accountability

ANNEX D

THAI INTELLIGENCE COMMUNITY ACCOUNTABILITY FRAMEWORK


Thai Intelligence Community Accountability Framework
Prime Minister
Note: Prime minister is also Defence Minister and Police Minister
RTArF: Royal Thai Armed Forces
RTA: Royal Thai Army
RTAF: Royal Thai Air Force
RTN: Royal Thai Navy
MIA: Military Intelligence Agency
AFSC: Armed Forces Security Center
NIA: National Intelligence Agency
RTP: Royal Thai Police
RTPSBB: RTP Special Branch Bureau
IG: Inspector General
Senate
Deputy Prime Minister
National Security Council
Ministry of Defence
Senate Standing Committee on Armed Forces and State Security / Military Commission
Senate Standing Committee on Laws, Justice Procedure and Police Affairs / Police Commission
Intelligence Board
RTP Board
RTP
RTArF
RTA
RTAF
RTN
RTP IG
RTArF IG
NIA
RTA Intel
RTAF Intel
RTN Intel
Joint Intel
AFSC
RTPSBB
MIA
Green shading denotes TIC agency
Reporting
Partial reporting
Defined accountability

ANNEX E
QUESTIONS FOR INTERVIEWEES

1. In the Thai context, how important is it for intelligence agencies to be held accountable to Government and to the public for their activities, methods and funding? How does Thailand reconcile the intelligence agencies' need for secrecy while at the same time trying to uphold transparency and operating within the law?

2. Australia's intelligence agencies operate under an accountability framework that has internal (intra-departmental) accountability aspects and external (extra-departmental aspect) as follows:

2.1 Internal:

2.1.1 Ministerial oversight of agency activities;

2.1.2 A written directive from the departmental secretary to each intelligence agency head; and

2.1.3 Written performance agreements between the intelligence agencies and the Commander in Chief of their service or program.

2.2 External:

2.2.1 Legislation;

2.2.2 A Parliamentary intelligence oversight committee (both government and opposition representation);

2.2.3 Cabinet oversight committees (senior Civil Service representation);

2.2.4 Courts / tribunals / ombudsmen (allowing for the hearing of complaints); and

2.2.5 Inspector General of Intelligence and Security (detailed oversight and investigation into specific activities or allegations).

Does Thailand have a similar framework, and if so, what does it look like?

1. Is your organisation’s intelligence reporting chain of command the same as your accountability chain of command? What do they look like?

2. What laws and regulations does your organisation operate under?

3. What changes would you make to the current system of intelligence accountability in Thailand to make it more effective?

Biography

Full Name : Stephen Francis Fomiatti

Date of Birth : 2 March 1968

Education Background :

: Master of Justice Graduate Diploma of Management

: Graduate Diploma of Intelligence and Security Analysis

: Graduate Diploma of Information Management and Analysis

: Bachelor of Science

Military Courses :

: National Defence College of Thailand (Class 62)

: Senior intelligence management

: Joint and advanced operations planning courses

: Strategic, operational and tactical level intelligence courses

: Australian Command and Staff College (Class of 2003)

: Technical intelligence and analysis courses

Military Experience **:** Defence Attaché, Australian Embassy, Bangkok, Thailand

: Senior Personnel Executive, Forces Command, Australia

: Assistant Defence Adviser, Australian High Commission, Kuala Lumpur, Malaysia

: Global Intelligence Manager, Joint Operations Command, Australia

: Senior Intelligence Analyst, ISAF Joint Command, Afghanistan

: Commanding Officer, UNSW Regiment, Australia

: Director, Criminal Intelligence Priorities, Australian Crime Commission, Australia

: Senior Intelligence Manager, UNTAET/UNMISET, East Timor

: Exchange Officer, US Army Intelligence Center, USA

Current Position **:** Australian Defence Attaché to the Kingdom of Thailand

SUMMARY

Field : Strategy

Title : A Comparison of Australian and Thai National Intelligence Accountability Frameworks

Name : Colonel Stephen Fomiatti, Australian Army

Course : NDC **Class :** 62

Position : Australian Defence Attaché to the Kingdom of Thailand

Background and Significance of Problem

As part of a more general trend in government, greater degrees of scrutiny and oversight in corporate governance and accountability have developed within the Australian National Intelligence Community (NIC)[1], along with increased attention to citizen rights. The continuum of accountability relationships developed between the public, the Parliament, the Government and the various agencies of the NIC has resulted in a high degree of transparency in NIC activities, ensuring agencies act legally and with propriety, comply with ministerial guidelines and respect human rights.

[1] For the purposes of this paper, the NIC comprises the Office of National Intelligence (ONI), the Australian Signals Directorate (ASD), the Australian Geospatial-Intelligence Organisation (AGO), the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO) and the Defence Intelligence Organisation (DIO).

Thailand's recent political history has been rather more unsettled than Australia's, with coups in 2006 and 2014. This has led to periods of military government and internal instability, a situation that doesn't necessarily lend itself to increased transparency and enhanced accountability. Thai support for security sector reform has traditionally been temporary and poorly organised, and there are no Thai civil society groups who regularly monitor the agencies of the Thai Intelligence Community (TIC)[2].

This is not to say however, that all NIC and TIC activity is, should or must be conducted completely in the open. The purpose of secrecy is to facilitate the proper functioning of government, but it needs to be balanced against other competing public interests including the public's right to know. It is the role of both internal and external accountability frameworks to ensure this balance is maintained, minimising community apprehension pertaining to national intelligence activities and damage to the trust relationship between the Government and its constituency.

Given this context, it is appropriate to examine the apparent paradox of secrecy within a democratic society and explore how in Australia, a multi-faceted accountability framework has been designed to overcome this to the satisfaction of both the Government and the public. Furthermore,

[2] For the purposes of this paper, the TIC comprises the National Intelligence Agency (NIA), the Armed Forces Security Center (AFSC), the Intelligence Divisions of the Royal Thai Armed Forces (RTArF), Royal Thai Army (RTA), Royal Thai Navy (RTN) and the Royal Thai Air Force (RTAF), and the Royal Thai Police Special Branch Bureau (RTPSBB).

and despite significant institutional and architectural differences between Australia's and Thailand's national intelligence frameworks, it is interesting to examine which parts, if any, of the Australian intelligence accountability framework may contain useful insights for Thailand's various intelligence agencies and the Government departments / institutions / entities to whom they necessarily answer.

Objectives of the Research

Specific objectives of this research paper are to :

1. **study** concepts pertinent to intelligence accountability to provide a degree of context for the research;

2. **describe** the Australian system of intelligence accountability, both internal and external, through the use of intra-departmental governance and accountability practices, relevant legislation, Parliamentary committees, committees of Cabinet, courts, tribunals, ombudsmen and oversight agencies;

3. **describe** the current Thai system of intelligence accountability for NIC-equivalent agencies as per that done for the Australian system; and

4. **compare** the two frameworks and **recommend** potential enhancements for Thailand's national intelligence accountability framework.

Scope of the Research

The scope of research comprises an examination of existing literature with findings and recommendations based on analysis of this material and the Australian National Intelligence Community experience of the author. This is supported by interviews with a range of experienced Thai intelligence practitioners and the heads of various Thai intelligence agencies regarding their experiences with intelligence accountability and potential scope for further development of this issue in the Thai framework. Data for this paper was sourced over the period December 2019 to July 2020 (secondary data), with interviews conducted in May, June and July 2020 (primary data).

Methodology

This research is a qualitative research, conducted by gathering relevant data, researching literature pertinent to intelligence accountability concepts and the actual accountability frameworks themselves, the experience and knowledge of the author from working in the Australian National Intelligence Community, and the information obtained from interviews with representatives from Thai intelligence community. The primary methodology utilised in addressing the research objectives is necessarily descriptive and analytical in nature – first setting the scene through examining the apparent paradox of secrecy within a democratic society; followed by describing the current Australian National Intelligence Community accountability framework and where it came from; detailing observations from analysis of current pertinent literature and legislation; and discussing case studies of intelligence accountability within the Australian context. From this examination of the Australian setting, expert points of view from Thai Intelligence Community helped shape understanding of the Thai context. This data was then analysed and the two systems compared in order to obtain recommendations for development for the TIC’s intelligence accountability framework.

Results

In general, Thai intelligence accountability frameworks are less well defined, regulated and legislated than in Australia. This is primarily due to differences in governmental systems and governance, a more centralised command and control regime, historical and cultural factors, different foci of intelligence agencies and a different threat environment within and against which they operate. For the same reasons, Thailand's internal intelligence accountability framework is much more robust than its external framework, although it should be noted that Thailand does not generally share the same definition of, or need for intelligence oversight and accountability as does Australia. Indeed, there is no comprehensive definition or understanding of an intelligence accountability framework, so the author has developed the Thai context from first principles.

A tabular comparison of the internal and external elements of the two national intelligence accountability frameworks is below.

Accountability Framework	Mechanism	Australia	Thailand	Remarks
Internal	Ministerial Oversight	🟩 Yes	🟩 Yes (including where delegated, for instance MoD Intel Board and RTP Board)	More centrally controlled in Thailand (e.g. NIA and RTP report to PM, PM is Defence and Police Minister, Deputy PM acts as an 'Intel Czar' of sorts).
	Directives to Agency Heads	🟩 Yes	🟧 Some	Thailand's not well defined and mostly verbal. Mitigated by strong chains of command, though should still be defined.
	Agency Performance Agreements	🟩 Yes	🟧 Some	Informal in Thailand. Some captured in legislation (NIA). Better definition needed.
	Agency Inspectors General	🟧 No (Not needed due to IGIS role and function, but could be included in respective ministries)	🟥 Most	None in NIA. Thai IG are well structured, but not empowered for oversight & accountability.
	Agency Supply Agreements	🟩 Yes	🟩 No	Minor issue in Thai context due to strong chains of command.

Note : Green denotes effective / no further action required. Amber denotes partially effective / some amendments needed. Red denotes ineffective / significant further action required.

Accountability Framework	Mechanism	Australia	Thailand	Remarks
External	Legislation	Yes (various, all agencies covered)	Yes (various, all agencies covered)	Neither country has complete over-arching intelligence legislation, but both systems are strong enough.
	Governmental Oversight Committees	Yes (PJCIS)	Yes (Senate Standing Committee for Armed Forces / Military Commission; Senate Standing Committee for Police / Police Commission)	Opposition not included in Thai system. Senate committees not independent nor intel-specific and hence relatively weak. PM as chair undermines independence of the committees.
	Directing and Coordinating Bodies	Yes (NSC, SCNS, FICC, ONI)	Yes (NSC, NIA-NICC)	Australian system overly complicated.
	Courts, Tribunals and Ombudsmen	Yes	Yes	More accessible to the public in Australia, and probably more effective in terms of providing transparency and accountability. Relatively minor aspects.
	Independent Statutory Oversight Body	Yes (IGIS)	No	Key issue. No independence of oversight (and therefore accountability) in Thailand.

Note : Green denotes effective / no further action required. Amber denotes partially effective / some amendments needed. Red denotes ineffective / significant further action required.

Recommendations

The recommendations can be broken down into four main areas: define and implement, strengthen, publicise and develop, and are summarised as follows:

1. DEFINE AND IMPLEMENT:

1.1 Clearly define Thailand’s intelligence accountability framework, both internal and external;

1.2 Include the defined intelligence accountability framework in the national strategy for Intelligence and made public to the best and greatest degree possible; and

1.3 Make adoption and implementation of this newly defined intelligence accountability framework mandatory, not optional.

3. STRENGTHEN:

3.1 Introduce formal instruments in the chain of command from Ministers down to agency heads detailing key results required and clear accountability arrangements, but not the means by which results are to be achieved.

3.2 Redesign and implement TIC agency websites that are simple, clear, consistent and helpful. The legislation and regulations governing TIC activities and operations should be easily accessible on each of the agency’s respective public websites.

3.3 Empower Inspectors General departments with broader authority, provision for oversight and an accountability function.

3.4 Review the roles and tasks of the appropriate Senate Standing Committees / Military Commission / Police Commission, the RTP Board and the MoD's Intelligence Board and amend their responsibilities to include greater provision for intelligence accountability and oversight from a holistic perspective, not just in a review and investigative capacity.

3.5 Create and resource an independent statutory organisation to provide oversight and accountability for all TIC agencies, that can report without fear or favour, and remains answerable to Government, though independent of Government influence.

4. PUBLICISE:

Once Thailand's intelligence accountability architecture is defined, implemented and strengthened, it is recommended that it should be publicised as widely as possible.

5. DEVELOP:

5.1 Further research to refine the definition of the system and include all of Thailand's national security agencies in a broader architecture.

5.2 Send a Thai delegation to Australia to study the NIC's accountability framework and take away elements beneficial to Thailand.

5.3 Clarify roles and tasks across the entire spectrum of Thailand's intelligence and security apparatus. Further research and review in this area would be of great benefit to the system as a whole, and therefore ultimately to Thailand's national security.