



The Federation of
Islamic Associations
of New Zealand (Inc.)

اتحاد الجمعيات الإسلامية النيوزيلندية

SINCE 1979

NATIONAL SECURITY, SURVEILLANCE AND SECRECY A FIANZ CONVERSATION ON PRINCIPLES

WITH THE REVIEW
THE INTELLIGENCE AND SECURITY ACT 2017

WWW.FIANZ.COM

July, 2022

For More Information Contact:

Abdur Razzaq

Chairperson of FIANZ Royal Commission and Follow-Up

info@FIANZ.com; FIANZ.Advocacy@gmail.com



CONTENTS

1.00	Intent of the Act	02
2.00	Determining the Value Proposition	05
3.00	Democratic Oversight	09

PREAMBLE

The Federation of Islamic Associations of New Zealand (FIANZ), established 1979, is the national Muslim umbrella organization.

The following is supplementary to our prior conversation on 28 June, 2022 with the Review of the Intelligence and Security Act 2017.

Our submission is predicated on three baseline rationale:

- i) **Ensure Checks and Balance:** In a democratic society there are a plethora of legislation , such as the Human Right Act , NZ Bill of Rights and others , aimed at safeguarding the interests of all citizens. However, it is also essential that there are significant checks and balances with the invasive mission creep of the powers of the intelligence agencies .
- ii) **Application of Core Principles:** The Muslim community suffered from the terrorism of 15 March with 51 shuhada and 40 bullet wounded . The Royal Commission of Inquiry (RCOI) noted with respect to the NZSIS, that the “concentration of counter-terrorism resources on the threat of Islamist extremist ...was inappropriate”. We believe there are core principles which need to be revisited and ensure lessons learned beyond what was related in the RCOI given their limited Terms of Reference.
- iii) **Mitigate Trust Deficit:** There has been a history of engagement misalignment and trust deficit between the intelligence agencies and vulnerable communities in Aotearoa New Zealand . They include the tangata whenua and faith-based communities, like ours. This needs to be recognised, addressed and mitigated with a future-proofing legislative anchor.

Abdur Razzaq
Chairperson, FIANZ RCOI
27 July , 2022

1.00 INTENT OF THE ACT

“The purpose of this Act is to protect New Zealand as a free, open, and democratic society by—
 (a) establishing intelligence and security agencies that will effectively contribute to—
 (i) the protection of New Zealand’s national security; and
 (ii) the international relations and well-being of New Zealand; and
 (iii) the economic well-being of New Zealand;”¹

1.1 Aotearoa New Zealand (A/NZ) does not have a national security strategy.

The result has been that different government agencies have defined their own security environment resulting in a silo approach. Whilst the RCOI stressed the importance of an aligned approach, the variations remain some two years after their Report.

EXAMPLE OF DIFFERENT AGENCIES WITH WITH THEIR OWN TAKE ON "SECURITY ENVIRONMENT".			} 'ALL OF GOVERNMENT' EFFICACY REQUIRES A COMMON AND ALIGNED APPROACH NOT PIECEMEAL SEPARATE APPROACHES BY AGENCIES
AGENCY	FOCUS	SOURCE	
NZ Defence	Security Environment	https://www.defence.govt.nz/what-we-do/assessing-our-future-strategic-environment/	
NZSIS	Security Environment	https://www.nzsis.govt.nz/news/navigating-domestic-security-threats-in-a-world-of-uncertainty/	
NZ Police	Security Environment	https://www.police.govt.nz/about-us/programmes-and-initiatives/national-security-insights-consultation	
MFAT	Security Environment	https://www.mfat.govt.nz/en/peace-rights-and-security/international-security/regional-security/?m=725762#search:U2VjdXJpdHkgRW52aXJvbm11bnQ=	
DPMC	Security Environment	https://dPMC.govt.nz/our-programmes/national-security-and-intelligence/new-zealands-national-security-system/national	

DPMC, in the absence of the yet to be established National Intelligence and Security Agency (NISA), is leading the program to develop a national security strategy. However, the systems and structures for silo shall remain unless there are purpose-specific legislation to address these. Developing a strategy without concomitant structural and process changes may be counterproductive.

¹ <https://www.legislation.govt.nz/act/public/2017/0010/37.0/DLM6920829.html>

Example of Legislative Scope

With respect to national intelligence investigation and assessment what are the demarcation boundaries between roles of NZSIS and NZ Police Intelligence? Working arrangements and culverts of responsibilities need legislative mandates.

Example of Legislative Scope

The most recent IGIS Report (2021) noted “One area of review that has raised interesting issues in different contexts is the intersection between law enforcement and the role of the intelligence agencies. The agencies have no enforcement function, but can report intelligence to the Police and in limited circumstances disclose information about crime that they discover incidentally while collecting intelligence.”

Example of Legislative Scope

Without definitional specificity of national security , the underlying legislations (e.g. Terrorism Suppression Act, Search and Surveillance Act etc) has the potential to negatively impact vulnerable communities.

We also need to ensure that the definitional baseline is determined in consultation with the tangata whenua , since te tiriti is our foundation document, otherwise the optics of national security will have no ‘buy-in’.

1.2 International relations for the intelligence community in the national security context have been mainly the nexus with the Five Eye countries. There are cooperation with other countries however the Five Eyes have dominated our national security relations. NZ is a net recipient of intelligence from the Five Eyes. As such, from our perspective , the potential exists for sovereignty subservience with this relationship. This needs further analysis and legislative clarification

The NZSIS’s relationships with the Five Eyes network of partners are vital to our ongoing ability to deliver positive security and intelligence outcomes for New Zealand.



Potential for Disintegration Scope

NZSIS is obliged to withhold information gained from Five Eyes on New Zealanders living in NZ. This has the potential to impact on the judicial decision-making process as well the outcome.

Potential for Disintegration Scope

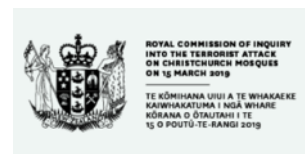
NZSIS may be inadvertently party to and provide tacit approval to illegal activities conducted by the Five Eyes partners since the current scope for legislative remedy is limited. (Information gained from torture of Afghan detainees)

Potential for Disintegration Scope

We have to be cognizant to the importance of ‘public interest’ and this cannot be left to the vagaries of intelligence community policy makers. In this context it is pivotal to recognise that “secrecy should not be based solely on harm to international relations but also require that such harms be balanced against the public interest in disclosure.”²

1.3 The importance of economic wellbeing is obvious, however as the Royal Commission noted, “fundamental to New Zealand’s future wellbeing and security is social cohesion”³ This social dimension is currently absent from the Act and its inclusion would enhance and embrace the community voices in the national security setting matrix. For us, social cohesion will define the integrity baseline of ‘wellbeing’.

Fundamental to New Zealand’s future wellbeing and security is social cohesion. While social cohesion in New Zealand is much higher than many other countries, there are fault lines. Maintaining and enhancing social cohesion is a vital task for government.



Example of Integrity-Matrix Scope

There is a dire need to have an equity lens to national security and this needs to be reflected in legislative changes. The lack of equity lens has marginalized the tangata whenua and vulnerable minorities.

Example of Integrity-Matrix Scope

The demographic transition evident with the multi-ethnic and multi-faith diversity trajectory post-2023, needs to be recognized. The social construct of Aotearoa New Zealand is as important as the focus on the economy. Failure to address this will continue the prevailing notion of ‘otherness’.

¹ Norwegian Parliamentary Oversight Committee on Intelligence and Security Services https://d1wqtxts1xzle7.cloudfront.net/52315630/MIICA_book-FI-NAL_3-libre.pdf?1490560096=&response-content-disposition=attachment%3B+filename%3DMaking_International_Intelligence_Cooper.pdf&Expires=1657780776&Signature=eeKTalMfcMI-cAqOSqise3V8RzZk3RloYtW0lecre9luhANwPX9a~mTW~eH0uzOXJ~ZpPgAm1O1LEhibm8S3Td176tyBBIMti~LRJ9mxYLouy3Cii5MVxCg7phly6Sj6gAy447SSRjdhHs9-HkSJ2JTObcuaqnVehw4s782Jcs4nuGzRt725mcrZcd6bUU3bJ2bvO8~k89HFrclyOyL6ZqaqCQEMpkaQIFJ28iWlw1gx7Z013~yq9u~XaQt3~LBRJHJ5Sq5EIMgtnNVxl-hKin0NAEbbWoXNKFMz3y49oqRy0qmDMngkPjFAPV-0Zr92ipf6pbwBZIRNFidiQSiXA__&Key-Pair-Id=APKAJLOHF5GGSLR5V4Z4

² <https://christchurchattack.royalcommission.nz/the-report/findings-and-recommendations/end-note/>

2.00 DETERMINING THE VALUE PROPOSITION

The key value proposition of the Intelligence and Security Act 2017 is its ability to enable the intelligence community to function effectively to keep us safe. Whilst the 2016 Cullen-Reddy Review advocated for a single, integrated and comprehensive Act, they also raised an important caveat, that “there should always be debate about how best to ensure this purpose is achieved”.⁴ Critical to this debate is an evidence-based efficacy assessment at two levels.

- i) Efficacy of the legislative-based activities generating intelligence and whether they meet/respond to the intelligence needs.
- ii) Efficacy of the current assessment programme(s) of the intelligence activities and whether they meet/responds to the community needs.

In our view, this granular focus and dual pathway needs to be considered by the current Review for a number of reasons. It cannot always be assumed that the intelligence needs determined by the intelligence agencies are aligned to the needs of the community it purports to keep safe. At a very raw level, the Operation 8 Tuhoe raids notes this misalignment.

At another level, the lack of intelligence prioritisation can also be counter to the community needs. The March 15 terror-tragedy highlighted that the priority focus on Right Wing Extremism (RWE) was missing and was too late. Moreover as the Royal Commission findings stated the “concentration of counter-terrorism resources on the threat of Islamist extremist ... was (also) inappropriate”. As such, the misalignment is again evident, albeit it was not a deliberate. The legislation needs to reflect the conclusion that the RCOI arrived at (there are 3 Recs in this respect).

These misalignment are however the symptom of a more fundamental issue. This relates to assessing the intelligence community’s analytical performance and its prerequisite of determining the effectiveness metrics of our national intelligence. Some have used organisational theory to assess “how intelligence organisations have adapted their mission and mandates”⁵. It is noteworthy that the Arotake Report takes this approach, which NZSIS commissioned to determine its own efficacy prior to March 15. The Report is an indication of the necessity of formalized evaluation on structured and on-going basis. We consider this essential given the mission creep which we have noted recently with rushed legislation like the recent omnibus Counter Terrorism Legislation Bill (Terrorism Suppression Act 2002 and the Search and Surveillance Act 2012; amend the Terrorism Suppression (Control Orders) Act 2019).

⁴ <https://igis.govt.nz/assets/Uploads/Review-report-Part-1.pdf>

⁵ https://www.jstor.org/stable/10.7249/mg804dhs.13?seq=3#metadata_info_tab_contents

A growing body of research is also adapting 'business analytics' to determine the efficacy of intelligence value. This analytics refers to the skills, technologies, and practices for systematically applying qualitative, quantitative, and statistical computational tools and methods to analyze data, gain insights, and inform and support decision-making.⁶ At the end however it boils down to the basic capabilities "to capture the primary requirements for successful CT intelligence"⁷.

- collection capabilities for gathering information
- analysis capacity to identify and assess the data
- storage to retain relevant information for future use
- information-sharing and transfer mechanisms to move either raw collected data or analytical products to the individuals and organizations that need them
- capability, authority, and willingness to act on the information.

The Chang 'Getting it Right' approach, as published in the American Intelligence Journal⁸ highlights that efficacy should also include determining the 'predictive accuracy'. This effectively means determining whether the predictive assessment is consistent with the outcomes. It is this level of sophistication that needs to be part of the systemic evaluation.

Cullen-Reddy(2016) raised another fundamental rationale. They stated that the purpose of the legislation is to protect New Zealand as a free, open and democratic society and these should also be the principles to judge the activities of the intelligence agencies. Here again the misalignment is profoundly problematic. When international intelligence cooperation agreement dictates the accessibility or otherwise of intelligence information, even to democratically elected parliamentarians, there are core democracy and sovereignty principles which have to be carefully assessed. This debate has yet to take place in A/NZ compared to the EU. A number of countries have begun addressing this issue⁹. For instance, Canada, Norway and Portugal, have revisited their respective legal frameworks. "Information classification is certainly an area which needs regular revision, considering the emerging and hybrid threats to national security and the new risks related to the unauthorized obtaining and disclosure of information due to advancements in technology and new forms of information sharing."¹⁰


⁶ <https://www.americanprogress.org/article/intelligence-community-doesnt-know-hurting-united-states/>

⁷ https://www.jstor.org/stable/10.7249/mg804dhs.13?seq=4#metadata_info_tab_contents

⁸ https://www.researchgate.net/publication/237145269_Getting_it_Right_Assessing_the_Intelligence_Community%27s_Analytic_Performance

⁹ https://www.dcaf.ch/sites/default/files/publications/documents/MIIICA_book-FINAL.pdf

¹⁰ https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-06/DCAF%20NATO%20PA_%20Survey_Report_Revised%20NYS2611_FINAL%20%28002%29.pdf



The underlying principles, known as the Tshwane Principles set a host of categories of information that may be classified. Having such , provides a public optics to balancing secrecy and transparency,

The Tshwane Principles

- “Information about on-going defense plans, operations, and capabilities for the length of time that the information is of operational utility.
- Information about the production, capabilities, or use of weapons systems and other military systems, including communications systems.
- Information about specific measures to safeguard the territory of the state, critical infrastructure, or critical national institutions against threats or use of force or sabotage, the effectiveness of which depend upon secrecy;
- Information pertaining to, or derived from, the operations, sources, and methods of intelligence services, insofar as they concern national security matters; and
- Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality.”

NZ has yet to develop our principles aligned to te tiriti and the conversation has to begin and the outcome included in an overarching legislation .

The all-important dimensions of secrecy and classification has to be addressed clearly . As the Royal Commission noted , “pervasive secrecy requirements are in themselves a serious limit on what can be said publicly. All of this has meant that there is at best limited public understanding of the threat of terrorism and the work that the counter-terrorism agencies carry out”¹¹. As a result of the RCOI , the intelligence sector have redefined their categories without any external and community oversight on this . It is setting a dangerous precedence where by the recipient and the user of intelligence also determines the secrecy levels.

¹¹ <https://christchurchattack.royalcommission.nz/the-report/part-8-assessing-the-counter-terrorism-effort/evaluation-of-the-counter-terrorism-effort/>

A recent major study have noted that there are prescriptive legislation relating to such classification.¹² The study noted that in a majority of countries ‘ there is one consolidated law dedicated exclusively to regulating information classification and the handling of classified information’¹³

Table 1: Legal Frameworks on Information Classification

Questions	Q1– Does your country have a law on classification and the handling of classified information?			Q6 – Does the law clearly and conclusively define the categories of information that may be classified?		
	State/responses	There is a stand-alone law on classified information.	Classified information is regulated by several pieces of legislation.	Classified information is addressed under a broader law on security.	Categories of information are listed in the law/decrees.	No conclusive list of categories, any information that may cause harm to national security interests can be classified.
ALBANIA		<input type="radio"/>			<input type="radio"/>	
BELGIUM		<input type="radio"/>				<input type="radio"/>
BULGARIA		<input type="radio"/>			<input type="radio"/>	
CANADA			<input type="radio"/>		n/a ¹⁵	
CROATIA		<input type="radio"/>			<input type="radio"/>	
CZECH REPUBLIC		<input type="radio"/>				<input type="radio"/>
DENMARK			<input type="radio"/>			<input type="radio"/>
ESTONIA		<input type="radio"/>			<input type="radio"/>	
GERMANY			<input type="radio"/>			<input type="radio"/>
GREECE		<input type="radio"/>			<input type="radio"/>	
HUNGARY		<input type="radio"/>				<input type="radio"/>
ICELAND			<input type="radio"/>			<input type="radio"/>
ITALY				<input type="radio"/>		<input type="radio"/>
LATVIA		<input type="radio"/>			<input type="radio"/>	
LITHUANIA		<input type="radio"/>			<input type="radio"/>	

In NZ , the recommendations of the 2018 Review of the NZ Security Classification System by IGIS has yet to be implemented. We believe this should be subject to further public conversation , given the March 19 tragedy. As part of the Review, we believe it is necessary to consider the basis of classification through public discussion and only then proceed to appropriate legislation. Leaving such matters for intelligence agencies to self-determine is not a democratic option.

¹² https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-06/DCAF%20NATO%20PA_%20Survey_Report_Revised%20NYS2611_FINAL%20%28002%29.pdf
¹³ https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-06/DCAF%20NATO%20PA_%20Survey_Report_Revised%20NYS2611_FINAL%20%28002%29.pdf

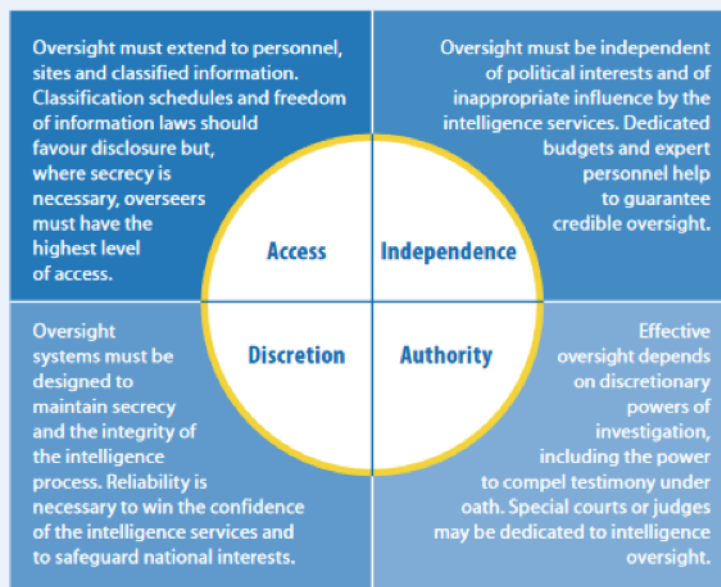
3.00 DEMOCRATIC OVERSIGHT

FIANZ is advocating systemic oversight which covers not only the current mandate but also the operation processes. It needs to be continuous and contingent. Continuous to ensure operational modalities are in keeping with best practices and lesson learned and contingent to ensure fulfillment of all the relevant legal and Human Right instruments. In such a context, the issue of resourcing and priorities set by the intelligence agencies may also be included in the oversight mandate. This is a radical departure from the current approach, but one which is necessary given the enormous powers and mission creep of the intelligence community with the recent changes to the Terrorism Suppression Act 2002 and the Search and Surveillance Act 2012 and the Terrorism Suppression (Control Orders) Act 2019. The other side of the coin is the arguable dubious legacy of the

- ‘unlawful’ access of data on ‘large proportion of New Zealanders ‘ by the NZSIS (Report of IGIS- 2017) [Mainly trawling through Customs’ data for 17 years of over 11 million passengers)
- “lack of precision and forthrightness” (Report by IGIS- 2017)
- “concentration of counter-terrorism resources on the threat of Islamist extremist ...was inappropriate”. (Royal Commission , 2020)
- “a number of official reports recording widespread mistreatment of detainees by certain Afghan authorities with whom the New Zealand intelligence agencies directly, or indirectly, shared information.” (IGIS Annual Report, 2020)

What we are not raising is the issue of whether are enough oversight agencies . As the current Director General, Rebecca Kitteridge highlighted in her speech on ‘Increasing Transparency’ on 2017, there are already of plethora of agencies like the IGIS, Intelligence and Security Committee; the OIA and Privacy Act with the Office of the Ombudsman and also the privacy Commissioner and as a state agency the oversight under the State Services Commissioner. Our focus is that with the enormous power of the intelligence agencies there is a need for ongoing oversight at the internal agency control level. This should be by IGIS. It must include more resources and legal mandate than presently available. The current executive (Ministerial) control, parliamentary oversight (IGIS) should also be supplemented with an independent oversight , which we believe should be under the proposed National Intelligence and Security agency- NISA . The rationale is that without such intensive and extensive oversight , the important democratic principles of transparency and checks and balance becomes reactive-issue focused rather than an integral and operational part of the intelligence surveillance and analytics.

Figure 3 Effective democratic oversight of intelligence requires that overseers have both the mandate and the power to credibly assess the performance of intelligence services



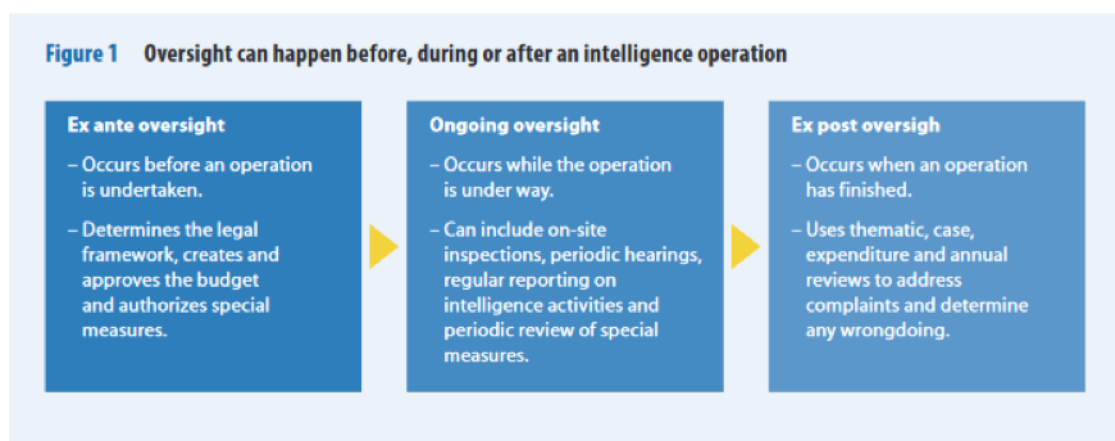
Source – Centre for Security, Development and the Rule of Law

For us this oversight is also more than external review and compliance to legislation, but it also includes who produces the intelligence and their controls, who is using it and for what purposes. With the high-stake and high-volume of intelligence information through the net (in all its articulation from open source to deep and dark web), this oversight becomes even more necessary. The scope covers human intelligence (NUMINT), signals intelligence (SIGINT) or geospatial intelligence (GEOINT) .

In the above context it is also important to qualify the notions of ‘control’ and ‘oversight’. Control implies the power to direct the intelligence agency’s policies and activities, for example by making rules, codes or policies that determine how an organization functions. Oversight means verifying whether rules and laws are obeyed and codes and policies are applied.¹⁴ For us , oversight organization like IGIS should also have legal mandate to possess certain control responsibilities. The example being when intel gained from torture is passed on from external intelligence organization and has the potential to influence the decision making of a NZ intelligence organization.

¹⁴ https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_11_Intelligence%20Oversight.pdf

The Centre for Security, Development and the Rule of Law, have given perhaps the most lucid definition of democratic oversight – “Oversight of intelligence services assesses their performance, integrity and compliance with the law as well as the quality of both executive and internal control”¹⁵. The democratic oversight also extends to before, during or after an intelligence operation. In the NZSIS context, such operations be focused on individuals, organisations or ideology or interest specific communities.



There are a number of key challenges to the democratic oversight which include secrecy management, discretionary authority, political will and exaggerated threat perceptions. These have to be addressed as part of the oversight process. Below we have outlined some examples from our perspective.

a) Secrecy Management : In NZ we have had issues in gaining intel derived from the Five Eyes, yet the intel had a significant impact on local community. Secrecy worked against the community interest and the right to know.

b) Discretionary Authority : The professionals and NZSIS have discretionary authority to make decisions, however challenging the decision produces a layered response ranging from full information to total secrecy. As such, the authority needs to be clearly specified in law and subject to democratic oversight.

c) Political Will: The clear example is the false categories by a former Minister of the issue of jihadi brides from NZ going to Syria. There was a political will to force a narrative which despite being inaccurate had to be followed by the NZSIS.

d) Exaggerated threat Perceptions: The Muslim community faced almost 8 years of such Islamophobic perception, yet the first major terrorism in recent times targeted the Muslim community.

¹⁵ https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_11_Intelligence%20Oversight.pdf



The Federation of
Islamic Associations
of New Zealand (Inc.)

اتحاد الجمعيات الإسلامية النيوزيلندية

SINCE 1979