New Zealand
Security Intelligence
Service
Te Pā Whakamarumaru

Review of Compliance

Review completed 30 June 2015
Unclassified summary released October 2015

Contents

Introduction

Soon after taking up her appointment in May 2014, the Director of Security initiated a review of the compliance systems and functions in the New Zealand Security Intelligence Service (NZSIS). A reviewer, seconded from another government department, was brought in to conduct a thorough examination of NZSIS's systems and processes, measuring those against what is considered a best practice approach to compliance.

The resulting report from that review is classified SECRET//NZEO (New Zealand Eyes Only). It recommends ways to strengthen systems and processes. The detailed information in the classified report, if made public, would expose vulnerabilities within the NZSIS to adversaries. The classified report has been provided to the Inspector-General of Intelligence and Security (IGIS), who is required to make an annual assessment of the intelligence agencies' compliance systems. Recognising that NZSIS is committed to being transparent about its work where it can, the reviewer has prepared an unclassified version for public release. This unclassified report is set out below.

Summary of Review

All state sector organisations must comply with the law and demonstrate compliance to the public. It is well understood at NZSIS that the organisation as a whole and its individual staff members must act at all times in both a lawful and proper manner. The necessarily covert nature of many of the activities and capabilities used by NZSIS when exercising its statutory powers, however, means that its activities cannot generally be subjected to public scrutiny. In order to maintain the public trust and confidence that is critical to NZSIS, specific oversight arrangements are in place to provide public assurance[1].

The best practice compliance framework used for the review is attached as Annex A.

The reviewer was given complete access to NZSIS material. Staff contributions were sought through individual interviews, group discussions and written feedback and this process was well supported. The reviewer reported open and frank discussion from all levels within the organisation. A comprehensive picture was obtained by aggregating feedback to get a sense of the overall position. Understanding of compliance varied at different levels within and across teams in the organisation.

The reviewer did not find any evidence of (nor was given any reason to believe there was) significant non-compliance within NZSIS. There is a collective awareness of the need to act lawfully and to some extent there is a preoccupation with doing so. While there may be inadvertent instances of non-compliance, the need to identify and manage these situations is well understood. Several areas of strength were identified where the exercising of statutory powers (e.g. intelligence warrants, other forms of operational activity) are scrutinised and subject to robust approvals processes.

[1] Ministerial, Intelligence and Security Committee of Parliament, the Inspector-General of Intelligence and Security (IGIS), the Commissioner of Security Warrants, Office of the Ombudsman, Office of the Privacy Commissioner and the Auditor-General

The review found that NZSIS's systems and processes need strengthening to provide a systematic and standardised approach to compliance, highlighting a number of specific examples that would benefit from strengthening and standardisation.

The review found that NZSIS staff are diligent in their duties and mindful of their obligations. They do their best to conduct themselves in a manner which is both lawful and proper. The review found that there is no intention on behalf of NZSIS staff to act in ways that are other than fully within its statutory powers.

> *"All staff have been frank and constructive in their discussions with me and when providing feedback. My impressions are that NZSIS staff are very committed to the role they play in protecting New Zealand and enhancing its interests. They want to contribute to improving and developing NZSIS for the future and are highly motivated to carry out their functions competently and in a compliant manner.*"

The organisation's ability to maintain full awareness of its obligations and monitor compliance, however, is described as fragile. Despite the best intentions of staff, the systems used to promote and monitor compliance are weak and mainly reactive. The organisation therefore carries some risk of non-compliance.

The weaknesses identified were found to be symptomatic of an organisation experiencing pressure stemming from a rapidly changing environment resulting in competing priorities. There is an inconsistent understanding and application of compliance obligations across the organisation. Guidance is often sought from others (managers, colleagues, or the legal team) reactively because access to clearly articulated, comprehensive, centralised policy and guidance is limited.

The reviewer recommended a holistic approach that establishes compliance as a core business function. This approach is consistent with the emphasis we already place on accountability, ownership and personal responsibility.

Where systems or processes are strong, NZSIS needs to monitor adherence to maintain these high standards. Conversely, where systems are weak it needs to have a centrally controlled programme to continuously identify and address areas for improvement.

Recommendations of the Review:

The reviewer made a number of recommendations aligned with a best-practice compliance framework, summarised as follows:

The Director and the Senior Leadership Team to make a commitment to compliance through:

- Establishing a compliance function, located in the Office of the Director, reporting to the Associate Director, and separate from the Legal Team.

- Developing a compliance framework, and a corresponding compliance programme, to incorporate compliance activities into the internal operational environment, then setting compliance objectives and measurable targets to meet these objectives.

Continuously assessing and monitoring compliance obligations by:

- Reviewing work previously undertaken to determine NZSIS's compliance obligations, keeping the record of compliance obligations in one easily accessible location, whether a register, database, or other form of collection, and establishing a system for regularly maintaining these compliance obligations.

- Establishing a legislative policy function.

Supporting compliant behaviour and preventing non-compliance through:

Operational policies

- Strengthening the operational policy framework with a corresponding operational policy function, to ensure there is centralised responsibility for identifying operational policy requirements organisation-wide, policy development, endorsement, and maintenance, and oversight for all other guidance documents stemming from operational policies.

- Addressing immediately the operational policy gaps identified prior to, and during the course of, this review.

- Requiring the operational policy function to maintain an accessible, searchable, and centralised database of all operational policies, Standard Operating Procedures, other operational guidance documents, Memorandums of Understanding, and other agreements affecting operational activity. Documents should be cross-referenced where applicable and stored centrally – not in team or individual's workspaces.

Training

- Enhancing initial and ongoing training for all operational staff, and linking this training to fitness to continue carrying out a role, as well as career progression and remuneration.

- Supporting the implementation of a formalised training programme by providing training staff with appropriate training to enable them to carry out their roles effectively. The Legal team, and the operational policy and compliance areas, should also work closely with training staff to feed into training programmes.

Internal quality assurance

- Making clear what level of detail and responsibility is expected of each existing quality assurance, advice, and oversight role, and incorporating compliance responsibilities into the expectations for these roles. If the expectations on these roles exceed capacity, the numbers in these roles need to be increased, roles redefined, or alternatives created, to cover the gap and residual risks.

Monitoring compliance and detecting non-compliance by:

- Developing an internal audit programme and annual audit schedule, covering both basic processes and quality of decision making. Results to be communicated to managers, the Senior Leadership Team, and the IGIS, and fed back into ongoing improvement of the compliance programme and framework.

- Strengthening mandatory reviews within all operational policies, including more clarity around the purpose and responsibilities for all those involved.

- Encouraging and supporting business improvement workflows, and enforcing the use of those in existence, to ensure better records and auditability.

Responding to non-compliant activity by:

- Directing the compliance function to be the central escalation point for reporting potential and actual compliance issues, maintaining a register, investigating issues, reporting findings to the Senior Leadership Team, and feeding findings back into the compliance programme. The compliance function to develop policies on this for all operational staff.

Strengthening external reporting by:

- Clearly articulating responsibility for reporting instances of actual or potential non-compliance and overall performance of the compliance programme to the IGIS, mandatory reporting expectations, and expected content, in internal policy and performance agreements. These requirements to be communicated to, and agreed on, with the IGIS.

Measuring improvement by:

- Measuring performance of the compliance programme against the compliance objectives and targets. Requiring the compliance function to be responsible for monitoring this information through internal escalation and audits and reporting this to the Senior Leadership Team.

Continuously improving by:

- Requiring the compliance function to feed information gathered through the monitoring, responding, and measuring processes back into the compliance programme to ensure continuous improvement, prioritised by risk, and delivered in line with a programme of improvement so that progress on this can be measured.

Director’s Response

This report provides an unclassified summary of a report that is comprehensive and constructive. I am heartened to see the review confirm the dedication and hard work of the staff at NZSIS and the mindfulness of their obligations to statutory compliance but I can also see that there is much work ahead of us in order to implement a best-practice compliance framework. I am grateful for all the work that went into the review, including specifically the work of the Reviewer.

I have accepted all of the recommendations of the Report. The NZSIS is now recruiting a new compliance team to support delivery of the full recommendation programme.

Annex One: Compliance Review Methodology

Assessing and identifying compliance obligations:

The first step to ensuring compliance must be establishing the compliance obligations created by the particular operating and legal environment. This should include mechanisms for regularly reviewing and updating obligations to take account of new and amended legislation, developments in case law, and other developments that have the ability to affect the way an organisation operates.

Supporting compliant behaviour and preventing non-compliance:

Once compliance obligations have been established, staff must be provided with the support and tools necessary to comply with these obligations. Support for staff should include:

- readily available information on compliance obligations that is up-to-date and can be applied easily, with clear processes, consistent across the organisation, and
- encourage accountability, appropriate training, and effective quality assurance mechanisms.

Monitoring compliance and detecting non-compliance:

Despite this fundamental support, non-compliant activity can never be completely prevented and organisations need systems and processes for detecting non-compliance through appropriate audit and review processes and external oversight. Identifying non-compliance should also lead into reviewing the effectiveness and appropriateness of existing controls.

Responding to non-compliant activity:

Where non-compliant activity or issues affecting compliance are identified there must be clear procedures for escalating and addressing these proportionately. These procedures must encourage accountability and self-reporting.

External reporting:

Where non-compliance has been identified and addressed this should be reported to an appropriate external authority and statistics made public. There should be clear internal guidelines and responsibility for this reporting.

Measuring:

Information on compliance should be available in a way that allows an organisation to understand its strengths and weaknesses, monitor trends, and identify areas for improvement.

Improving:

Lessons learned throughout the compliance cycle should be continuously fed back into the organisation to improve policies, processes, training, systems and other controls and supporting tools.

New Zealand
Security Intelligence
Service
Te Pā Whakamarumaru

www.nzsis.govt.nz

New Zealand Government