
The 2019 Terrorist Attacks in Christchurch:

A review into NZSIS processes and decision making in the lead up to the 15 March attacks

June 2019

Property of the New Zealand Security Intelligence Service.
Reclassification or dissemination requires prior consent.

Contents

Executive summary	7
Introduction	15
Background.....	15
Terms of Reference	16
Review Approach	17
NZSIS's Operating Context	20
Part 1. What holdings <i>did</i> NZSIS have in respect of the individual	22
Question: How was the search of NZSIS records planned and conducted?	22
Question: Were there any limitations or restrictions in respect of the searches?	26
Question: What information did those searches produce and how was it assessed?	29
Question: What material in NZSIS records relates, or potentially relates, to the individual	30
Part 2. What <i>should</i> NZSIS have known about the individual ?	35
Part 2.1. NZSIS Priorities and Priority Setting	36
Business Renewal	36
Question: How are NZSIS's strategic intelligence priorities decided?	37
Renewal of Intelligence Processes	37
External Processes	38
Internal Processes.....	39
Question: Do NZSIS's prioritisation processes work effectively and have they produced appropriate focus?	44
National Security and Intelligence Priorities	44
Interpreting National Security and Intelligence Priorities.....	44
Question: What issues exist within the current intelligence prioritisation process?	50
Question: Did these issues substantively impede the discovery of the individual ?	52
Part 2.2. NZSIS Resource Allocation	53
Question: How are decisions made on resourcing NZSIS's Intelligence Directorate?.....	53
Investigative Resources	56

Analytical Resources.....	57
Intelligence Collection Resourcing	57
Regional Office Resources	58
Question: Were these resourcing decisions effective?	59
Question: Are there resourcing matters which would benefit from reconsideration?.....	61
Question: Did resourcing decisions substantively impact on NZSIS’s ability to identify the individual?	65
Part 2.3. NZSIS Legal and Compliance Frameworks.....	66
Question: How does NZSIS regulate its activities?.....	66
Significant Developments in Legal and Compliance Frameworks.....	66
Independent Review.....	66
The Intelligence and Security Act 2017	67
Warrants	68
Ministerial Policy Statements (MPS)	69
Policies.....	70
Direct Access Agreements	70
Restricted Information	70
Access to business records of telecommunications networks and financial service providers.....	71
Compliance with New Zealand law and human rights obligations	71
Inspector-General of Intelligence and Security.....	72
Question: How effective is NZSIS’s regulatory framework?	73
Question: Are there issues within the current regulatory framework?	74
Warrant thresholds	74
Investigative thresholds.....	77
MPSs/JPSs	77
Direct Access, Restricted Information and Access to business records of telecommunications networks and financial service providers.....	78
Question: Did these issues substantively impact NZSIS’s ability to identify the individual?	80
Part 2.4. NZSIS Partnership Arrangements	81

Question: How does NZSIS engage with its partners? 81

- International Liaison 81
- Domestic Partnerships..... 82

Question: Does NZSIS effectively use its partnerships?..... 83

Question: What issues arise in NZSIS’s partnerships? 83

Question: Did partnership issues substantively impede NZSIS’s discovery of **the individual**? 86

Part 2.5. NZSIS Investigative and Operational Frameworks 87

Question: What Frameworks does NZSIS Use?..... 87

- Process Reform..... 87
- Investigative Model 87
- Discovery and Baselining Projects 89

Question: Are these systems effective in pursuing national security investigations? 92

Question: What was NZSIS doing regarding Right-wing extremism? 94

Question: Are there issues within current systems? 101

Question: Did these issues substantively impact NZSIS’s ability to identify **the individual**? 103

Part 2.6. Mock Investigation Exercise 104

- Notional Lead Information 104
- Conduct of the Exercise 106
- Session 1: Consideration of Individual Leads 106
- Session 2: Considering the Leads in Totality 107
- Session 3: Changing NZSIS’s Investigative and Operational Settings 108

Part 3. What *could* NZSIS have known about **the individual**? 110

Consideration 1: Building National Security Understanding across Government, Business and the Community..... 110

- What is Proposed?..... 111
- Why is it Important?..... 113
- What Would Need to Occur? 113
- Who are the Key Stakeholders? 113
- Are there Likely to be Significant Resourcing Implications? 113

Consideration 2: Enhanced Lead Generation by NZSIS..... 114

What is Proposed?.....	114
Why is it Important?.....	115
What Would Need to Occur?	115
Who are the Key Stakeholders?	116
Are there Likely to be Significant Resourcing Implications?	116
Consideration 3: Wider Direct Access to Government Data.....	116
Why is it Important?.....	117
What Would Need to Occur?	118
Who are the Key Stakeholders?	118
Are there Likely to be Significant Resourcing Implications?	118
Consideration 4: Criminalising a Wider Range of Preparatory Acts in Respect of Terrorism	118
What is Proposed?.....	119
Why is it Important?.....	120
What Would Need to Occur?	120
Who would be the Key Stakeholder?	120
Are there Likely to be Significant Resourcing Implications?	120
Recommendations	121
NZSIS Priorities and Priority Setting.....	121
Intelligence Prioritisation	121
NZSIS Investigative and Operational Frameworks.....	122
Leads Generation.....	122
Investigational and Operational Policy Frameworks.....	124
Access to Information and Data	125
NZSIS Resource Allocation.....	126
Systems, Processes and Using Resources More Effectively	126
Specific Resourcing Pressures	127
NZSIS Legislative and Compliance Frameworks.....	128
Removing Ambiguity.....	128
Ministerial Policy Statements and Joint Policy Statements	128

Released by the Director-General of Security

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

NZSIS Partnership Arrangements..... 129
 Increased engagement with government, business and the wider public 129
Appendix 131

~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

Executive summary

On 15 of March 2019, terrorist attacks at the Al-Noor Mosque, and shortly afterwards, at the Linwood Islamic Centre in Christchurch resulted in the deaths of 51 worshippers and caused serious injuries to more than 30 others. Allegedly, the attack was carried out by ^{the individual} [REDACTED], an Australian citizen living in New Zealand. Shortly after the attacks, following advice from New Zealand's policing and intelligence community, the Government announced ^{the individual} [REDACTED] was not on any intelligence watch-lists.

On 25 March 2019, Prime Minister Jacinda Ardern announced the establishment of a Royal Commission of Inquiry into the attacks to report to Government by 10 December 2019. On 8 April, the New Zealand Security Intelligence Service (NZSIS) Director-General of Security Rebecca Kitteridge commissioned an internal review (the "Review") to consider whether NZSIS's actions had been reasonable and appropriate and what might NZSIS do to improve its ability to identify and disrupt such attacks into the future. This is the report from that Review.

The terms of reference directed the Review to:

- Consider the NZSIS prioritisation of threats or potential threats and allocation of resources;
- Identify if there were any impediments to the gathering or sharing of information to/by/with NZSIS that would have presented a reasonable opportunity for NZSIS to identify the offender(s)' attack planning or the threat he/they posed, such as legislative or intelligence sharing challenges amongst relevant state sector agencies; and
- Make recommendations as to what changes, if any, should be implemented to improve NZSIS systems or operational practices designed to identify such a threat and prevent such an attack.

To answer those questions the Review focused on three broad areas of inquiry:

- What information **did NZSIS hold** about ^{the individual} [REDACTED] at the time of the terrorist attacks on 15 March 2019 (if anything)?

- What **should NZSIS have known** about [the individual] at this time (if anything)? This included considering priority setting frameworks; resource allocation; legislative and compliance frameworks; partnerships; and investigational systems and practices (and the investigations related to those); and
- What **could NZSIS have known** about [the individual] at this time (if anything)? This involved considering whether changes in the settings or practices in place in the period leading-up to the attack could have substantively increased the likelihood of identifying [the individual] prior to the attack.

To determine **what NZSIS *did* hold about** [the individual], the Review conducted what was probably the most forensic search of NZSIS records ever undertaken. This search was informed by post-attack national and international investigations and included more than 270 search terms ranging from telephone numbers and IP addresses to key lines/phrases in the 'manifesto' [the individual] published immediately prior to the attack. Using search terms identified following the attack, and 'fuzzy logic' searching tools, the Review sought to determine whether NZSIS held any information, no matter how minor, that could have been investigated and led to the identification of [the individual]'s planning.

In all, these searches generated more than 32,000 responses, with many being the result of search methodologies which captured near or partial hits. The Review considered these hits and documented its findings. The Review found that the only information NZSIS held in respect of [the individual] before the attack related to his movements in and out of New Zealand – information that in itself was unremarkable and held in respect of every individual crossing the New Zealand border. Moreover, this information could only be used for data-matching purposes and was not accessible to NZSIS investigators.

Separately, through a range of mechanisms, the Review asked NZSIS staff whether any had recollections of information, events or issues that might relate to the 15 March 2019 attacks. Helpfully, a very small number of staff did come forward and in each case the information was considered. None of the matters raised, however, can be linked directly to [the individual] or attack planning.

As a result of these detailed searches, and input from NZSIS's staff, the Review has concluded [the individual] was not under investigation, nor the subject of any substantive lead information, at anytime before 15 March 2019.

The Review's second question related to **what *should* NZSIS have known** about [the individual] prior to the attacks. The Review considered this question in the context of NZSIS's existing

breadth and depth of legislative and organisational responsibilities. This included NZSIS's substantial business renewal programme mandated by the Government and facilitated by substantial investment since 2016.

The Review considered the prioritisation and resourcing decisions for this business renewal to be beyond its purview. Nonetheless, it noted the sequencing of this renewal entailed a deliberate initial focus on improving enabling functions, in order to support the subsequent expansion of NZSIS's intelligence capabilities. At the time of the attacks, NZSIS was in the third year of a four year programme, in which NZSIS had begun to redirect its focus toward the 'front line.'

In this context, the Review considered the various systems shaping NZSIS's investigative and operational focus: prioritisation processes; resource decision-making; legal and compliance frameworks; partnerships; and its investigative and operational frameworks.

The prioritisation of New Zealand's high-level security and intelligence requirements has been evolving in recent years, both in its structure and detail, to ensure the work of New Zealand's intelligence community is appropriately focused. Within these priorities, the Government has identified six thematic areas of focus for NZSIS's covert intelligence collection capabilities, which include foreign interference (including espionage) and terrorism. Since 2016, NZSIS has proactively developed two mechanisms for interpreting these high-level priorities: its strategic analysis capability to identify trends and emerging threats, and its ten-year operational strategy (Project STERLING). Both were well-considered and effective tools for directing NZSIS's investigative and operational efforts. NZSIS implemented broadly effective systems and processes for prioritising its national threat investigations, and processing lead information, as well as its allocation of scarce collection resources.

NZSIS's resource decision-making has been re-designed as part of the organisation's business renewal. Workforce sequencing decisions, combined with the difficulties of growing 'front line' capabilities, meant substantive growth in the NZSIS Intelligence Directorate (responsible for investigations and intelligence collection) did not occur until 2018. The number of investigators doubled in 2018, with investigative staff spread evenly between state intelligence and counter-terrorism investigations. The decision to invest a higher concentration of investigative experience in the state intelligence unit was a reasonable one; reflecting NZSIS's STERLING prioritisations and the increasing threat from state actors to New Zealand's democratic processes. Despite its rapid growth and focused capability building, the Intelligence Directorate's overall staffing will likely fall short (but not dramatically so) of NZSIS's ambitious workforce plan for 2018/19.

In the last five years, NZSIS has been through a significant period of review in regard to its legal and compliance frameworks; including being subject to a thorough Independent Review of Intelligence and Security in New Zealand, the implementation of new governing legislation and the development of a significant amount of new policy to incorporate the new legislation into practice. The new legislation and the accompanying policies have brought about a significant change to NZSIS's business processes. The implementation of a new compliance regime, of which the Inspector-General of Security and Intelligence (with increased oversight powers) is a significant part, has been complicated by interpretative issues, which continue to impact efficiencies and strain resources, particularly the capacity of NZSIS's in-house legal team. Although the new legislative regime has acted as an enabling tool in many respects, the Review makes some recommendations as to areas for potential improvement.

In addition to its own collection and assessments, NZSIS's international partnerships provide the Government with unique intelligence and insights, which require protection. These sensitivities have historically caused NZSIS to isolate itself from its domestic government partners, including law enforcement agencies. Global events and changes in the domestic threat environment have required NZSIS to become more transparent and collaborative with its domestic partners. National counter-terrorism efforts since 11 September 2001, and especially since the rise of Islamic State in 2013, has seen NZSIS develop increasingly productive and effective relationships with law enforcement but, for a variety of practical and technological reasons, it has yet to establish a truly joint partnership with New Zealand Police (NZ Police).

NZSIS has long used a 'classical model' for its investigations, which is well suited to assessing known threats using established intelligence collection techniques. The model served NZSIS well through a multitude of Islamic State-related threats, which largely (but not exclusively) dominated the New Zealand terrorism threat environment until early 2018. This focus on the most urgent threats, although likely at the expense of building a detailed picture of emerging issues, was reasonable. However, the 'classical model' has limitations with respect to identifying emerging threats in the modern security environment, in which those meaning to harm New Zealand interests can more effectively conceal their identities and actions, particularly online. NZSIS benefits greatly from lead information provided by its domestic and international partners, but needs to ensure it can effectively share its requirements and generate its own leads using modern technologies.

The Review found NZSIS's existing systems and processes to be reasonable and broadly effective in ensuring it had the focus, resources and frameworks necessary to fulfil its

national security responsibilities. However, the Review has also identified some areas which would benefit from further consideration:

- Refining processes for the prioritisation of NZSIS's intelligence function, including further embedding the role of strategic intelligence analysis;
- Increasing staffing in its Christchurch office and online operations areas, whilst also empowering the ability of investigators to access open-source information and appropriate database holdings;
- Reducing ambiguity in NZSIS's legal and compliance frameworks by testing investigative and warrant thresholds and refining processes within the current policy framework;
- Continuing efforts to grow transparency but to also seek to empower others in government, business and the community to support NZSIS's functions; and
- Increasing priority and resourcing for the generation and management of lead information, and baselining, to support the identification of emerging threats.

As **the individual** was a lone actor, who took deliberate and effective steps to conceal his plans, and such weak signals would have been difficult for any security service to detect. The Review considered the most likely (possibly only) way NZSIS might have discovered **the individual**'s plans was if NZSIS had gained an intelligence warrant and mounted a covert technical attack on **the individual**'s computer and emails to acquire a copy of his manifesto. Through a mock investigation, the Review concluded that, even if NZSIS had acquired the lead information obtained through subsequent investigations, NZSIS would not have met the threshold for a warrant.

Therefore, despite its recommendations, the Review does not consider these recommended changes could have substantively increased the likelihood of NZSIS identifying **the individual**'s intention to mount his attacks. However, if enacted, the recommendations should allow NZSIS to offer the Government greater assurance that lone actor threats are more likely to be detected in the future.

The third question the Review considered, specifically **what could NZSIS have known** about **the individual**, looks to identify potential changes to current high-level settings and processes which might enable NZSIS (and the wider national security community) to identify

threats, the likes of the individual, into the future. At this stage, and given the timeframes available, the issues identified in this part of the report have not been worked through to the same level of detail provided in the report's previous parts. Indeed, several of the Review's observations relate to initiatives which are of a nature or scale that is beyond the ability of NZSIS acting alone to change (including legislative amendment).

The first area the Review considered under this question related to building national security understanding across New Zealand's government, business and community. Throughout most of their history, Western security and intelligence services have operated as largely self-sufficient entities with limited connections to wider government. National security matters were not part of mainstream government business, but rather were regarded as anomalous and managed quietly through special arrangements and channels. This is no longer the case. In many Western nations, national security is now a government-wide priority, and security and intelligence services cannot be effective unless they are closely connected with government, business and the wider public. While security and intelligence services (and their Governments) have had to adapt to this new reality, the rate of adaptation across the world has not been uniform – and in some countries, where national security issues have been less evident or compelling, change has been slower.

Following the attacks in Christchurch, alongside continuing concerns regarding Islamist extremism, foreign interference, espionage and cyber-attacks, it may now be time for NZSIS (and the Government) to consider whether national security issues should be more transparent and part of the public debate in New Zealand. For NZSIS to continue to be effective it will need to increasingly expand understanding and support for its role. A failure to do so will likely leave it isolated. Further, as an organisation with increased, but still relatively limited, resources, NZSIS must leverage others' resources and reach in New Zealand to assist it to perform its role. A key enabler in NZSIS generating this support will be a wider public understanding and appreciation of its role. Direct Government support and involvement in any such initiative will be critical to its success.

The second area the Review considered involved NZSIS giving increased priority to the development and implementation of initiatives to identify emerging threats. Current investigative frameworks tend to focus on areas or individuals known to be of security concern, and, while remaining absolutely valid, can prove to be self-fulfilling. NZSIS needs to improve its ability to detect increasingly weak signals of potential security threats. In regard to lead generation, the Review has suggested NZSIS explore with Government its view and appetite regarding some level of data-mining. The Review understands there will likely be some reticence regarding this in New Zealand. In any event, there would be benefit in having a clearer Government view on its position to data-mining, if only to assist in informing

consideration of other lead generation possibilities. As noted earlier, closer connections with wider government, business and the public will also assist in this regard. Any programmes to enhance lead generation and discovery will need to be supplemented by new systems and processes to manage and investigate those leads including more direct access to data (and the associated human and technical resources).

The third area the Review has considered concerned widening NZSIS's direct access to Government data. Information is the 'lifeblood' of any security service and anything which can help investigators develop a more detailed understanding of a potential threat quickly is of critical importance. While the Government has recognised the need for NZSIS to have direct access to selected databases in the Intelligence and Security Act 2017 (ISA 2017), it remains the case that there are extended delays in obtaining much of what is required – at times more than 30 days. In rapidly evolving threat environments, a great deal can occur quickly and waiting for extended periods to progress an investigation can, and at some point will, have significant consequences. Consideration should be given to seeking amendment of the ISA 2017 to include a non-legislative process for adding further datasets to Schedule Two, as required. NZSIS should also look to identify those government data and information holdings critical to NZSIS's functions which might be included in any such change. Any such amendment would need to continue to recognise the need for appropriate safeguards regarding access to, and the use and storage of, such information and data.

Although the matter is outside NZSIS's mandate, the final area the Review has suggested for consideration relates to the criminalisation of a wider range of preparatory acts in respect of terrorism. While counter-terrorism legislation was passed in 2002, its sparing use against a backdrop of involvement by New Zealand citizens with Islamic State has highlighted difficulties in its operation. At times this means NZ Police and NZSIS are required to use specialised and scarce resources to monitor individuals for reasons of public safety. Accordingly, resources which could otherwise be utilised to identify and assess emerging or previously unidentified threats are used elsewhere. While not an exact percentage, the Review was advised that in more recent years perhaps up to one sixth of NZSIS's collection resources were devoted to such coverage. Accordingly, the Review has suggested NZSIS discuss with NZ Police its interest in jointly proposing legislation to criminalise a broader range of preparatory activities relating to terrorist activity.

The Review notes much of what it has recommended, or proposed for consideration, potentially poses significant implications for resourcing. Even with the significant budgetary increase NZSIS has received, these likely will be beyond NZSIS's current means.

Released by the Director-General of Security

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

In closing, no matter how many of the Review's recommendations are acted on, they cannot, sadly, provide a guarantee that attacks like those of 15 March 2019 will not occur again. What such changes can do, however, is provide an increased level of assurance to the Government and community that such terrorist activity is more likely to be identified and disrupted.

~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

Introduction

1. This report provides the findings and recommendations flowing from the Review commissioned by NZSIS Director-General Rebecca Kitteridge. The Review was commissioned to consider whether NZSIS's actions were reasonable and appropriate in the period leading to the 15 March 2019 terrorist attacks in Christchurch.

Background

2. Shortly before 1400 on 15 March 2019, 28 year old Australian citizen **the individual** allegedly entered the Al-Noor Mosque on Deans Avenue in Christchurch and fired upon those attending Friday Jumu'ah prayers. **the individual** then allegedly drove to Christchurch's Linwood Islamic Centre, where he again fired on those gathered. Although **the individual** was apprehended by NZ Police shortly after he left the Linwood Islamic Centre, 51 worshippers died and dozens of others were injured as a result of these attacks. Shortly after the attacks, the New Zealand Government announced **the individual** was not on any intelligence watch-lists. In classified reporting, NZSIS stated **the individual** was not known to NZSIS prior to 15 March 2019.¹

3. The fact that the New Zealand intelligence, security and law enforcement community (including NZSIS), had not identified and disrupted **the individual** prior to the attacks has led to public speculation on whether the policing and intelligence community had adequately focused on the threat posed by extreme right-wing (XRW) elements and lone actors. On 25 March 2019, the Government announced a Royal Commission of Inquiry tasked with considering what relevant state sector agencies knew about **the individual**'s activities before the attack; what, if anything, they did with that information; what measures agencies could have taken to prevent this attack; and what measures agencies should take to prevent such attacks in the future.² NZSIS has welcomed the establishment of the Royal Commission of Inquiry.

4. On 8 April 2019, the NZSIS instituted this Review of NZSIS's processes and decisions in the lead up to the Christchurch attacks. The Review is to determine what NZSIS could learn from the failure to detect **the individual** prior to the attacks and what, if anything, NZSIS could alter in the way it operates to ensure its is as well placed as possible to detect such planning in future.

s6a: refers to classified report

²(Appendix 2) Terms of Reference for a Royal Commission on the attack in the Christchurch Mosques on 15 March 2019
([Link](#))

5. s6a: describes name and job of Arotake Reviewer

Terms of Reference

6. Director-General Kitteridge issued detailed terms of reference for the Review's conduct. She directed the Review to:³

- a. Consider the NZSIS prioritisation of threats or potential threats and allocation of resources;
- b. Identify if there were any impediments to the gathering or sharing of information to by/with NZSIS that would have presented a reasonable opportunity for NZSIS to identify the offender(s)' attack planning or the threat he/they posed, such as legislative or intelligence sharing challenges amongst relevant state sector agencies; and
- c. Make recommendations as to what changes, if any, should be implemented to improve NZSIS systems or operational practices designed to identify such a threat and prevent such an attack. This may include changes within NZSIS and, where relevant, across legislative settings and operational practices in the wider security sector.

7. The terms of reference advised that the review occur over four stages:

- a. **Phase 1 - identification of material.** NZSIS undertook to provide the review team with full access to information. The review team has access to NZSIS databases to obtain information. The review team is also able to request relevant information be obtained for them from databases and email inboxes, and that searches are run for various terms. Post-attack investigative material can be provided to or be requested by the review team to add to their understanding;
- b. **Phase 2 - factual narrative/timeline.** NZSIS will work with the review team to produce a factual narrative that sets out the timeline of events/actions of the offender prior to the attack, together with any relevant NZSIS actions or decisions;

³ (Appendix 3) Terms of Reference for NZSIS Christchurch attack review, 8 April 2019 ([Link](#))

- c. **Phase 3 - assessment.** The Reviewer will lead a forensic review of NZSIS holdings to form an assessment of NZSIS decisions and actions as against the terms of reference; and
- d. **Phase 4 - lessons learnt, report and recommendations.** The Reviewer will provide the Director-General with a draft written report for comment which addresses these terms of reference. The Reviewer will provide the Director-General with the factual narrative. The Director-General will have the opportunity for comment (including as to factual and legal accuracy) on these documents prior to the finalisation of the written report. The Reviewer may provide the Director-General with interim recommendations prior to the provision of the draft or final report.

8. Director-General Kitteridge limited the remit of the Review, by directing that “the Review is not a disciplinary investigation and the Reviewer has no power to determine the fault or liability of any person (other than the alleged offender(s)).” Furthermore, the terms of reference confirmed that the purpose of the Review was “not to make adverse findings against any other Crown agency.”

Review Approach

9. The nature of any review involves a critical eye being cast over arrangements to identify opportunities for improvement. When read in isolation, and without detailing the achievements and successes of the organisation, reviews can appear unbalanced and to have been written in a harsh or unfair light. While this Review does make a range of recommendations it does so knowing NZSIS has achieved a great deal over an extended period of time - but perhaps at no time more than the past few years. Since 2014, NZSIS has been engaged in a continuous programme of major organisational renewal and change across all aspects of its operation. This four year programme (now in its third year) was necessary and important as it was required to establish the base from which NZSIS could grow and develop into the future. In the last three years NZSIS has:

- introduced new business and intelligence strategies and associated operating models;
- increased its staffing by more than half, including the work required to recruit, train and induct a range of staff generally new to intelligence;
- incorporated new legislation (and all the associated policy and procedures);

- begun building wider partnerships in Government (and beyond); and
- simultaneously managed a rapidly evolving and increasingly complex security environment in both its counter-terrorism and state intelligence remits.

When taken in that context, the recommendations made, while still considered important, take on a new perspective.

10. In accordance with the terms of reference, the Review was shaped around three key areas of exploration or questions. They were:

- a. What information *did* NZSIS hold about **the individual** at the time of the terrorist attacks on 15 March 2019 (if anything)?
- b. What *should* NZSIS have known about **the individual** at this time (if anything)? This included considering priority setting frameworks, the allocation of resources, investigational systems and practices, compliance frameworks, accesses to information and how NZSIS worked with its partners in the national security community.
- c. What *could* NZSIS have known about **the individual** at this time (if anything)? This considered whether changes in the settings or practices in place in the period leading-up to the attack (including policies, processes and legislation) could have substantively increased the likelihood of identifying **the individual** prior to the attack.

11. Further, in terms of the conduct of the Review, it is noted:

- It is understood there will be an external interest in the Review's considerations and recommendations. To assist with that understanding, extra material and context has been included in this report beyond that which would be normal for an internal review. Further, several areas of consideration in the Review are cast as questions which need to be answered. It is believed this structure will assist in understanding the report;
- The Review team formed its views and recommendations from discussions with NZSIS staff and a wide-ranging review of relevant NZSIS documentation (many of these documents are included in appendices to this report). It also met with a small number of external interlocutors and partners and took the opportunity to brief the Inspector-General of Intelligence and Security (IGIS) and, separately, her staff on the Review and its structure;

- To encourage wide staff participation in the Review process, a web page was established on NZSIS's Intranet (with a section on FAQs); staff were briefed during the Director-General's monthly 'Town Hall' meeting and encouraged to take part; and the Deputy Director-General messaged all staff encouraging them to participate.⁴ Staff members from within NZSIS's counter-terrorism investigations area were also briefed separately on the Review and similarly encouraged to contribute. Observations and recommendations in this Review should not be seen as criticism of NZSIS, NZSIS's partners nor any member of staff;
- In all, the Review team held 'one on one' discussions with around fifty members of staff from across NZSIS (several of those staff members were spoken with on multiple occasions). These staff members came from a range of managerial levels and from across disciplines including analysis, investigations, collection, legal, compliance, vetting and senior management. A small number of officers 'self-selected' to contribute to the Review and their willingness to do so was appreciated. The Review took a deliberate decision not to interview staff formally, or make contemporaneous records of each discussion, with the aim of encouraging staff to feel comfortable to come forward and speak freely;
- In several cases the recommendations or observations made in this report relate to work NZSIS is already undertaking or is in future work plans. Including them here does not indicate any concern, rather it is simply a way of noting the value in that work going forward;
- While many of the recommendations, if accepted by NZSIS, can be implemented from within the current budget, there are others which would be major programmes of work with the associated resourcing costs - for example those relating to improved capabilities to generate lead information and increased capability and capacity in virtual environments. These would have significant resourcing costs which, even given the significant budget increases NZSIS has enjoyed in recent years, would likely require additional supplementation;
- While the Review considers the underlying strategies, frameworks and systems which drive NZSIS's work, it only does that through the frame of NZSIS's counter-terrorism efforts. While the recommendations and observations included in this Review are likely to have application beyond the terrorism target area, this has not been tested;

⁴ (Appendix 3) AROTAKA - NZSIS internal Review (Email), 11 April 2019 ([Link](#))

- In some cases the report makes generalised comments regarding issues. It is likely there will be instances or situations where these generalisations are not always 'true'. At times this cannot be avoided when seeking to make observations about complex or highly detailed matters. It is done so with the aim of providing clarity in the report. That said, in respect of the question 'what *did* NZSIS hold in respect of ^{the individual,} the Review has been particularly forensic in its approach as the accuracy of this element is crucial to the Review; and
- As is the nature of all reviews, this report benefits from the sharpened clarity 20/20 hindsight can provide.

11. Finally, while this is an internal review, and perhaps it is not usual to do so in such a document, the Review team wishes to express its gratitude to the staff of NZSIS (and those we spoke to outside NZSIS) for the open, constructive and helpful way they have approached the Review and how each made time in their otherwise busy diaries to do so. In particular, the Reviewer would like to thank the small team who worked directly on the Review, including those involved in the search of NZSIS's intelligence holdings – their enthusiasm, energy, insights and commitment were invaluable.

NZSIS's Operating Context

12. Any review needs to be considered in the context of the time. A failure to do so can lead to views, judgements and recommendations which are unreasonable and that fail to recognise the realities of the operating environment.

13. The NZSIS performs a range of roles on behalf of the New Zealand Government, including those of both security intelligence and foreign intelligence services, and providing government-wide vetting services and protective security guidance. In doing so, NZSIS has a wider remit than most of its FIVE EYES partners. NZSIS's operating environment is made more complex by:

- Rapid organisational growth: following significant scoping work, known as the Strategic Capability and Resourcing Review (SCRR), the Government decided to invest \$178.7 million in the New Zealand Intelligence Community, over four years from 2016. This investment grows NZSIS's budget from an additional \$18.7 million in 2016/17 to an additional \$35.7 million by 2019/20, and entails expectations of commensurate increases in NZSIS capabilities. NZSIS's workforce will grow from 282 FTE in Financial Year 2016/17 to 424 FTE by the end of the 2019/20 Financial Year. To achieve this, NZSIS has undertaken a very substantive organisational renewal programme.

- Significant changes in legislation: a broad-based independent review of the NZSIS and the GCSB (the “Cullen-Reddy Review”) in 2016 prompted the Government to fundamentally redesign the legislation governing the two agencies, principally through the introduction of ISA 2017. In order to implement this new legislative framework, NZSIS was required to:
 - contribute to the development of Ministerial Policy Statements and the resulting Joint Policy Statements with the GCSB;
 - re-develop its internal policies and standard operating procedures for conformity with the new legislative and policy requirements; and
 - manage legal ambiguities while interpreting and implementing the new legislation and policies (typically in consultation with GCSB and the Inspector-General of Intelligence and Security (IGIS)).
- Marked changes in the national security threat environment: Global trends are more frequently impacting New Zealand, requiring NZSIS to respond to a broad range of national security threats, including:
 - the continuing appeal of terrorist violence, particularly driven by the rise of Islamic State group and its evolving terrorist modus operandi, as a tool to advance ideological, political or religious objectives within small, but significant, sectors of society;
 - a return of geostrategic competition and the rise of foreign espionage and interference in democratic processes in New Zealand, and among its friends and neighbours in the Pacific region; and
 - the need to protect sensitive government information from insider threats to ensure confidence with the Government and external partners which share their information with New Zealand Government agencies.
- The digital revolution: the rapid advancement of communications technology, particularly via the internet, has fundamentally changed the environment in which security harm can both be perpetrated and investigated. The digital revolution has required NZSIS to acquire new capabilities to overcome the ease with which those meaning to harm national security can conceal themselves and their activities online.
- National security becoming mainstream in government: national security issues are increasingly becoming ‘whole of government’ considerations rather than those which have historically been conducted at the margins of government (and normally shielded from public view). This development requires revised systems and processes, and cultural change in both the intelligence community and government more broadly.

Part 1. What holdings *did* NZSIS have in respect of [the individual]?

14. Shortly after the events of 15 March 2019, Prime Minister Ardern advised the New Zealand public that [the individual] was not the subject of New Zealand intelligence or law enforcement investigations. Similarly, Director-General Kitteridge publicly confirmed [the individual] was not known to NZSIS or its Australian counterpart, the Australian Security Intelligence Organisation (ASIO) prior to the attacks. These statements were based on searches of NZSIS information holdings, [s6a / s6b: operational information], based on the limited biographical information known about [the individual] at the time.

15. Subsequent investigations of [the individual] by authorities in New Zealand, and by its international liaison partners, have identified an extensive array of unique identifiers attributable to [the individual]. The Review considered it important to use these newly discovered identifiers to conduct a detailed search of NZSIS information repositories for any information NZSIS held in relation to [the individual] at the time the attacks occurred. Such a detailed and thorough search of NZSIS's holdings, though quite resource-intensive, was considered necessary given the purposes of the Review; the possibility that some piece of critical information might have been missed by NZSIS; and the public importance of the matters to be addressed by the Royal Commission.

16. The search was designed to provide a high level of assurance to NZSIS and the Royal Commission regarding what information the NZSIS did and did not hold.

17. As a result of these detailed searches, and input from NZSIS's staff, the Review has concluded [the individual] was not under investigation, nor the subject of any substantive lead information, at any time before 15 March 2019.

18. It is noted that the only information NZSIS held in respect of [the individual] before the attack related to his movements in and out of New Zealand – information that in itself was unremarkable and held in respect of every individual moving in and out of the country. Although held on a database owned by NZSIS, under NZSIS's direct access agreement with the Ministry of Business, Innovation and Employment, this information could only be used for data-matching purposes [s6a: operational information].

Question: How was the search of NZSIS records planned and conducted?

19. The search of NZSIS information repositories was the most forensic element of the Review, requiring bespoke IT solutions and unprecedented investigative accesses to NZSIS data stores. It was quite probably the most forensic search NZSIS has undertaken. In designing the search parameters and methodology, [s6a: describes international consultation]

s6a: describes international consultation

following which a detailed search protocol was developed for the project and endorsed by the Director-General.⁵ Although the search was to be thorough, the Reviewer decided that it must nonetheless be reasonable and proportionate in the context of timeliness for the Review and the impost on NZSIS's information technology areas which were required at the same time to support urgent ongoing investigative priorities.

20. In consultation with NZSIS's Knowledge Manager, IT experts and database users, the Review team identified all possible information repositories and assessed the likelihood that relevant information might be held there, the extent to which the repositories could be searched and the resources this required. These considerations were incorporated into an assessment of which repositories it would be reasonable and proportionate to search – but, generally speaking, the default position was to search where it was possible to do so.⁶ To manage the impact, a staged approach to the search was proposed, in which completion of each tranche would inform the next.

NZSIS Information and Data Repositories

s6a: describes NZSIS information and data repositories



21. The diagram above provides a simplified overview of NZSIS's information data repositories considered for in-depth searching for the Review.

⁵ (Appendix 5) AROTAKE: Request for endorsement of proposed search protocol (tranche 1), 3 May 2019 ([Link](#))

⁶ (Appendix 6) Appendix A – Information Repositories (AROTAKE) ([Link](#))

s6a: refers to information repositories



23. The Review team also ran a detailed search over NZSIS's low-side SEEMAIL email servers as a potential source of lead information from other government departments. SEEMAIL is used by NZSIS for low-side (up to RESTRICTED) emails for semi-secure messaging

with other New Zealand government departments. A 'litigation hold' has been in place for SEEMAIL since January 2015, which prevents emails from being permanently deleted.

24. s6a: describes system searches
[Redacted]

25. s6a: describes system searches
[Redacted]

26. Where possible within the varying search capabilities of the different information systems, the Review's search was limited to holdings prior to 1400 on 15 March 2019 [Redacted]
s6a: describes system searches
[Redacted]

27. Although information collected after the 15 March attacks is outside the scope of the Review's search, as noted earlier, this information was used to inform the search terms used. Working with the counter-terrorism investigative area, the Review team developed a comprehensive list of more than 270 search terms, ranging from highly specific to 'fuzzy' queries, seeking to ensure any traces of [Redacted] and his identifiers would be captured by the search.⁷ The search terms spanned various identifiers collected following the attacks, including s6a: describes details that were searched
[Redacted]

⁷ (Appendix 7) Appendix B - Discovery Search Terms (AROTAKE) ([Link](#))

s6a: describes details that were searched [REDACTED] as well as key phrases from his manifesto to confirm whether NZSIS had advance access to that document. With a mind to the many possibilities by which traces of [REDACTED] might appear in Service holdings, the search also used character-substitution 'wildcards' and metaphonic searches to maximise the breadth of capture. The searches were refined s6a: system [REDACTED] to test and adjust search-strings to ensure they were effective without producing prohibitively large numbers of possible hits. During this refinement process, a number of documents were identified which become markers for validating future searches.

28. The final search protocol was shaped s6a: staff positions [REDACTED] and the Reviewer, and authorised by Director-General Kitteridge. The Review team engaged with CT investigators to seek assurance of the accuracy and thoroughness of the list of search terms and also sought assurance from investigators separate from the CT investigations area, to ensure that nothing had been overlooked. IT experts responsible for the information repositories provided significant and open assistance to the Review team, ensuring the holdings were in the most searchable form (e.g. re-indexing holdings), testing the searches and repeating them where necessary to ensure the accuracy of the results. Where there were concerns regarding the use of classified search terms s6a: search terms [REDACTED] to search unclassified networks, NZSIS moved data from the unclassified system to a classified network where it could be securely searched.

Question: Were there any limitations or restrictions in respect of the searches?

29. The Review team's search of NZSIS information repositories was limited by factors including legislative restrictions, technological issues, and decisions made not to search areas where there was an extremely low likelihood of relevant material being held, particularly where those searches would have included a high resource cost, diverting staff from other high priority matters (i.e. the search would not be reasonable or proportionate).

30. An example of a repository of information the Review team decided was not reasonable or proportionate to search was the collection of external hard-drives seized under NZSIS's warranted powers for entirely separate purposes (notably counter-espionage) given it was considered very unlikely to contain information relevant to this Review.⁸

31. The Review team was also unable to search information held by NZSIS collected for vetting purposes s6a: systems [REDACTED]

⁸ (Appendix 6, page 4). Appendix A – Information Repositories (AROTAKE) ([Link](#))

Section 220 of ISA 2017 provides that information obtained by, or disclosed to, the NZSIS for the purpose of a security clearance assessment may be used only for the following purposes: the security clearance assessment, any other security clearance assessment, and counter-intelligence.⁹ As informing the Review and the Royal Commission of Inquiry do not fit within any of these purposes, security clearance information was necessarily excluded from the search.

32. Upon further enquiry by the Review team, it became clear that, even in the absence of legislative barriers to searching security clearance information, a large portion of this information would have been significantly arduous to search. s6a: information source that was not reviewed

[REDACTED]

33. s6a: describes steps taken to ensure no relevant information was missed, despite not searching information source referenced in para 32

[REDACTED]

⁹ (Appendix 8) ISA 2017 - Counter intelligence is defined in section 220 as meaning "...the intelligence activities carries out to identify and counteract the threat, or potential threat, of unauthorised disclosure of official information by a person who holds, or has held, a New Zealand Government-sponsored national security clearance.
([Link](#))

34. The Review team also did not search the dated paper files held by NZSIS. This decision was made because of the age of this information (pre-dating ^{the individual}'s living in New Zealand) and therefore the limited likelihood there would be information of relevance. This would also have amounted to a significant and disproportionate resource cost.

35. The Review also appealed to NZSIS employees to come and speak to the Review team should they have any recollection or concern that might, with the benefit of hindsight, have been connected with ^{the individual}. With the exception of one staff member who recollects seeing ^{the individual}'s Facebook handle earlier (which is addressed in detail below in the section regarding material potentially relating to ^{the individual}), no such recollections or concerns were reported.

36. ^{s6a: systems excluded from search}
[Redacted]

37. ^{s6a: systems excluded from search}
[Redacted]

38. NZSIS is required to have robust retention and destruction processes and NZSIS staff are regularly reminded of the importance of not retaining information which is not relevant to national security (e.g. information incidentally collected about third parties). Accordingly, it is possible, although considered unlikely, that NZSIS could have incidentally collected

information in respect of the individual but not retained that information as it had no obvious nexus to security.

Question: What information did those searches produce and how was it assessed?

39. The search commenced on 8 May 2019 with a detailed search s6a: system as it existed at 1400 on 15 March 2019. In parallel, searches were conducted of DMS, the File Stores and emails. The absence of known results identified during the refinement process or excessively large hit-rates caused the Review team to question the search results in these systems. Over a number of adaptations, access limitations and differences in the search parameters within these other databases were identified and overcome. s6a: systems

[REDACTED] However, these results were nonetheless acceptable as they confirmed the searches were working by returning highly relevant results related to NZSIS's post-attack investigations. These date-stamped results (i.e. those post 1400 on 15 March 2019) were excluded. When thousands of records were received, many of which related to 'fuzzy' search terms, these were processed by a small team with suitable authorisations to access the wide array of holdings.


40. The search results were processed on the basis of their date relevance (did NZSIS hold the information prior to the attacks?) and relevance to the individual and his unique identifiers (did the information relate to a known identifier?). Lastly, the results were assessed for whether they contained derogatory information which might have constituted lead information for further assessment by the counter-terrorism investigative team.

41. The Review has maintained a detailed record of the searches conducted, the search hits returned and its assessment of those results. A summary of the Review's detailed search follows:¹⁰

s6a: describes search types and results

¹⁰ (Appendix 9) AROTAKE: Discovery Search Results, completed 21 June 2019 ([Link](#))

s6a: describes search types and results



42. The large number of search hits was a consequence of the deliberately 'fuzzy' search-strings used in the search. These were expected to return significant numbers of false positives for triage (as they did) in an effort to ensure the search was sufficiently comprehensive to capture any trace of **the individual** and his unique identifiers.

43. The Review team maintained a record of search hits in the NZSIS Document Management System. These are available to the Review team and a small number of additional senior NZSIS staff including the Knowledge Manager; they will be maintained for at least the duration of the Royal Commission.

Question: What material in NZSIS records relates, or potentially relates, to

the individual?

44. The searches of the material held by NZSIS up to 1400 on 15 March identified no derogatory data related to **the individual** which might have warranted further investigation. The search did highlight 32 travel records **s6a. system**, which were inaccessible to NZSIS's investigators due the constraints of NZSIS's direct access agreement with the Ministry of Business, Innovation and Employment (which is responsible

for Immigration New Zealand).¹¹ As ^{the individual} was not a person of interest to NZSIS prior to the attack, his presence in ^{s6a: system} did not trigger advanced passenger processing (APP) alerts to inform NZSIS of his travel. Moreover, the ^{s6a: system} hits only recorded ^{the individual's} check-in for flights to or from New Zealand and retained his passport details for immigration purposes. The data on ^{the individual} was no different to that collected on all international airline passengers. The ^{s6a: system} results did not include information which would reasonably have triggered further investigation by NZSIS, even had it been accessible.

^{s6a: describes operational steps taken after the attack}

12

45. The searches did reveal a small number of potential hits which, for the sake of completeness, warrant elaboration:

^{s6a: describes a range of false positive hits}

^{s6a: operational information and details}

s6a: describes a range of false positive hits



46. The Review's separate enquiries with the counter-terrorism investigative unit revealed a small number of other leads which possibly related to the individual:

- The Review was advised of a lead (with the potential to be in respect of the individual) received from s6a: describes Operation Gallant Phoenix, an intelligence fusion centre based near Amman, Jordan

[redacted] One lead, received in November 2018, related to a New Zealand

(possibly Dunedin) based IP address (122.61.118.145) active sometime between October 2016 and late 2017.¹⁴ The IP address had been used to access online files related to guerilla warfare tactics, Al-Qaeda leader Ayman al-Zawahiri and Norwegian right-wing extremist Anders Behring Breivik. The counter-terrorism unit's attempts to identify the IP address's user were unsuccessful. On 4 December 2018, the telecommunications company responsible for the IP address confirmed it no longer had access to the subscriber data. As such, the identity of the subscriber could not be recovered nor could the location of IP address at the time in question. **s6(a) operational detail**

[REDACTED] The Review considers NZSIS's actions in respect of this lead were both reasonable and appropriate.

- A NZSIS staff member advised the Review he recalled having information brought to his attention, possibly detailing a social media posting made by a “@Barry Harry Tarry”. The officer's memory had been triggered during investigations following the 15 March attacks which confirmed **[REDACTED]** used the Facebook handle “@Barry Harry Tarry”. The staff member recounted the posting was of a right-wing nature but that it did not indicate any imminent threat or potential attack. In the absence of any lead information and the ubiquity of such postings on online, the officer recalled no further action being taken on the information. The Review team conducted an additional search to ascertain whether the staff member's recollection was correct but no reference to the Facebook handle was found in NZSIS repositories prior to the attacks. The Review cannot discount, however, the possibility NZSIS officer saw tangential information related to **[REDACTED]** (namely a Facebook user name). Even should the staff member's recollection be correct, the comparatively benign nature of what he recalls, combined with the formerly unknown significance of “@Barry Harry Tarry”, means there would have been little, if any, reason to pursue the matter further. It is noted no other staff working in this area at the time have similar memories.
- The counter-terrorism unit also brought to the Review's attention a member of the public's claim that they had forewarned the New Zealand Government and media organisations about the Christchurch attacks (Lead number 359). The lead had been investigated and closed after finding the claim to be inaccurate and not from a credible source. The counter-terrorism unit provided the Review with

s6a: operational information

details of its investigation and conclusions.¹⁵ Upon review of the information and NZSIS's actions in triaging the lead, which made no mention of [redacted], the Review is satisfied NZSIS's officers acted reasonably in closing the lead.

¹⁵ s6a: operational information [redacted]

Part 2. What *should* NZSIS have known about the individual?

47. Having conducted a thorough search of NZSIS information repositories and collated information volunteered by staff, the Review has achieved a high degree of confidence that no derogatory information, which should have caused NZSIS to investigate the individual and discover his intentions, was overlooked by NZSIS.

48. The next question is one of whether it is reasonable to expect that NZSIS should have identified the individual prior to the attack.

49. To determine this, it could be argued that every element of every NZSIS business process needs to be considered or dissected given it is the operation of these processes in concert which produces the effect Government seeks: the protection of New Zealand's national security in a free and open democratic society. This would constitute a major endeavour requiring a considerable period to complete and not be practical in the time available. Accordingly, this Review has confined its scope to focus on what the Review believes were the key elements of NZSIS's systems and processes relevant to NZSIS's priority setting and intelligence operations. These include NZSIS's:

- priority setting systems (strategic to operational) and the resultant priorities relating to both its organisational renewal and intelligence activities, with a particular focus on counter-terrorism;
- resource allocation against these priorities;
- legislative and compliance frameworks;
- partnership arrangements; and
- investigative model, the associated operational and investigational frameworks and the investigation of extreme right wing activities and target discovery programme.

Part 2.1. NZSIS Priorities and Priority Setting

50. As noted earlier, NZSIS is engaged in a wide ranging business renewal programme which began around five years ago. Any consideration of organisational priorities must occur in light of NZSIS's reform of its business model.

Business Renewal

51. In 2014, the New Zealand Intelligence Community (NZIC) was the subject of a critical but constructive State Services Commission-led Performance Improvement Framework (PIF) Review, which acknowledged the scale of the challenges facing NZSIS and the need for "ruthless prioritisation" of its work. The Review made a number of recommendations for strengthening the NZIC's organisational foundations in order to advance operational efficiency and effectiveness. Following this 'autumnal' PIF Review,¹⁶ NZSIS embarked on a renewal programme, adopting a new organisational strategy, s6a: Project name. At the end of 2014, Cabinet approved additional funding for increased NZSIS capability and capacity to respond to the threat posed by foreign terrorist fighters and other violent extremists, particularly following the rise of Islamic State (or Caliphate) in Iraq and Syria. [REDACTED]

s6a: information about operational funding decisions
[REDACTED]
[REDACTED]

52. s6a: project names the NZIC sought to achieve levels of investment which were better attuned to Government expectations of the agencies. The Strategy, Capability and Resourcing Review (SCRR) provided Government with a detailed picture of the agencies' potential value, if suitably funded, in delivering a range of security and intelligence services. This led Cabinet to approve a four year NZIC investment programme as part of Budget 2016 in order to address financial pressures, and enhance the NZIC's capability and capacity to deliver on New Zealand's security and intelligence requirements. The NZIC received investment of \$178.7 million, over four years from 2016, designed to establish a limited set of new capabilities.¹⁷ The investment would assist the Government to mitigate its most critical (non-natural hazard) national security risks and stabilise the NZIC in the face of significant cost pressures.

53. This investment programme necessitated the NZIC, including NZSIS, to prioritise fulfilling Cabinet's SCRR expectations within the four year period, alongside its continuing

¹⁶ (Appendix 14) A reference to the PIF's predominantly red and amber coloured scorecard in which no parts of the NZIC were rated as 'strong' or 'well-placed' across all PIF areas; see: Performance Improvement Framework: Review of the Agencies of the Core New Zealand Intelligence Community (NZIC), March 2014 ([Link](#)).

¹⁷ s6a: references classified document

national security and intelligence responsibilities. While recognising the need to expand its investigative and intelligence collection capabilities, the strategy initially prioritised ensuring the organisation's enabling functions were effective and resilient, so as to support subsequent growth 'on the front line.' These enabling functions were critical to recruit a modern, skilled TOP SECRET workforce and to develop the systems required to enable their work. The revised business model was an important step in building the Government's confidence that NZSIS was transitioning into a modern organisation capable of meeting the Government's requirements within evolving legislation and compliance frameworks.

54. NZSIS recognised its existing business model was inadequate to meet the challenges of a quickly changing operating environment, including evolving national security threats and rapid technological advancement. In recognition it undertook a deliberate redesign and rebuilding of its underlying intelligence operating model and organisational structure (Projects AGUERO ^{s6a: project name}).

55. ^{s6b(i): describes information provided by international partners}



56. **Given the priorities decided under SCRR (and its associated requirement for planning and resources) were a part of Cabinet approved processes, they are considered beyond the purview of this Review.** The Review notes the organisational renewal is ongoing and will necessarily continue to draw upon NZSIS's limited resources, which otherwise might be dedicated elsewhere in the organisation. However, as NZSIS's enabling systems mature, it may be possible to reallocate resources from enabling to intelligence functions.

Question: How are NZSIS's strategic intelligence priorities decided?

Renewal of Intelligence Processes

57. While NZSIS's organisational renewal sought to ensure NZSIS became an increasingly strong and well-managed organisation, NZSIS also identified the requirement to significantly revamp its intelligence processes to meet NZSIS's statutory objectives:¹⁸

The principle objectives of the intelligence and security agencies are to contribute to –

¹⁸ (Appendix 8) s. 9, ISA 2017 ([Link](#))

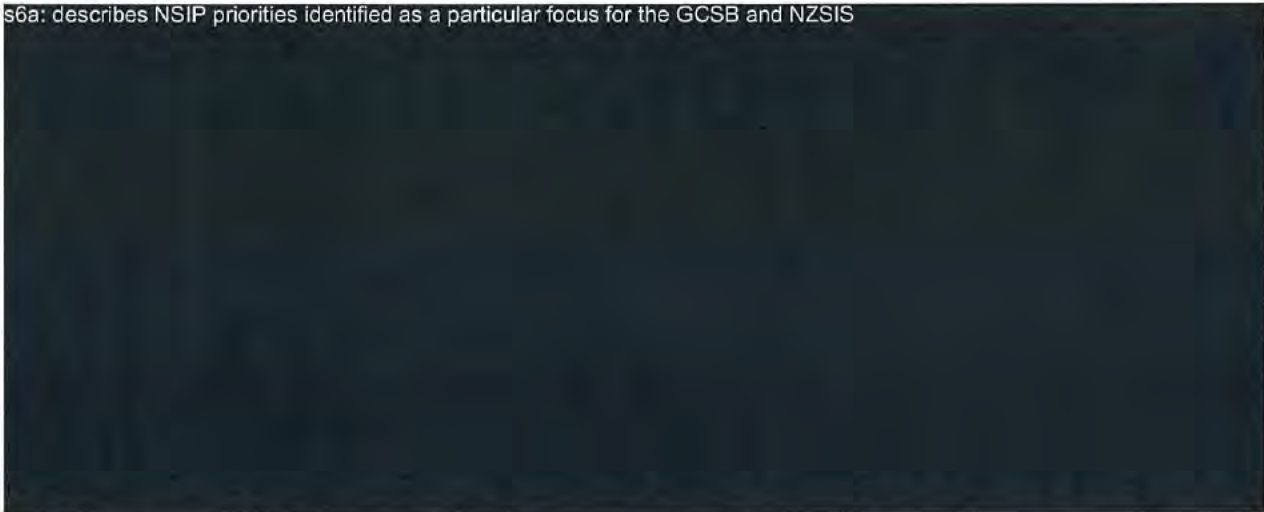
- (a) *the protection of New Zealand's national security; and*
- (b) *the international relations and well-being of New Zealand; and*
- (c) *the economic well-being of New Zealand.*

58. Reform in this regard involved significant change in both NZSIS's external and internal environments.

External Processes

59. While NZSIS's objectives are set-out in legislation, external processes and systems provide NZSIS's high level intelligence priorities. These are developed annually by DPMC, approved by Cabinet, and referred to as the National Security and Intelligence Priorities (NSIPs). The first NSIPs issued in December 2018 identified sixteen priorities. While there is no hierarchy for these priorities (all are important), six were identified as of particular focus for the GCSB and NZSIS (see figure below) due to their requirement for more intrusive covert intelligence collection capabilities and assessment activities.¹⁹

s6a: describes NSIP priorities identified as a particular focus for the GCSB and NZSIS



60. The NSIPs framework has been evolving over recent years, alongside the development of DPMC's National Security Group, and at present the mechanism for interpreting the counter terrorism NSIP into more detailed information requirements (previously a Priority Coordination Group) is not operating. This appears to have led to a temporary gap in the national prioritisation framework's ability to articulate mid-level, enduring (or thematic) intelligence requirements. These are important in guiding investigative and collection focus across the NZIC. It is understood new processes designed to fill this gap are being implemented.

¹⁹ (Appendix 16) NSIPS Supporting Organising Framework, December 2018 [ERS-18-SUB-0026] ([Link](#))

Internal Processes

61. Once the Government's NSIPs are set NZSIS interprets these high level priorities through two prisms – strategic assessments produced by the National Assessments Bureau (NAB), the Combined Threat Assessment Group (CTAG) and through NZSIS's own strategic analysis capability, as well as through the ten-year NZSIS operational strategy, STERLING.

62. In terms of the first prism, New Zealand has a developing strategic assessment community. At its centre is NAB which provides detailed strategic-level analysis for senior government leaders and policy-makers. Under SCRR, the role of NAB has been bolstered within the National Security System to broaden its focus from external, largely foreign policy considerations to a greater role in national security matters, including terrorism. In November 2018, following wide consultation, NAB published a key guidance document to inform the NSIPs.²⁰ CTAG also performs an important function in analysing threat intelligence and formulating threat levels to inform government risk management responses to specific events or locations. By contrast to NAB, the CTAG role is more evaluative of the current threat environment than predictive. CTAG periodically produces national terrorist threat assessments for New Zealand, in which the organisation describes the New Zealand threat environment or 'threatscape'.

63. Since late 2015, NZSIS has been developing its own complementary strategic analysis capability following a review of the NZIC's security intelligence operating model (AGUERO). AGUERO noted the need for NZSIS to have a dedicated capability to assess New Zealand's evolving 'threatscape', including early identification of emerging issues and what these mean for NZSIS's investigative efforts:²¹

The strategic intelligence function would be complementary to the higher-level national assessments function undertaken by the DPMC (National Assessments Bureau). The key focus of the new function would be on the practical, real-time understanding of security intelligence issues as they are occurring or emerging within New Zealand. This should have the added benefit of helping leads analysts know where to focus effort, i.e. it would provide a more evidence-based framework for making initial triaging decisions (i.e. where to focus effort).

²⁰ s6a

²¹ (Appendix 18) Project AGUERO: Review of the New Zealand Intelligence Community's Security Intelligence Operating Model, September 2015 ([Link](#))

64. The second prism, NZSIS's operational strategy (STERLING) has provided a long-term pathway for prioritising, coordinating, and resourcing NZSIS's investigative and intelligence collection activities since 2016. The strategy is shown in diagrammatic form on the following page. Of particular relevance to the Review, STERLING required NZSIS to undertake a deliberate prioritisation of the organisation's nine long-term strategic goals, of which the top three were identified as:

Goal 1: NZSIS has mitigated espionage and hostile foreign intelligence threats

Goal 2: NZSIS has successfully mitigated serious domestic terrorism threats

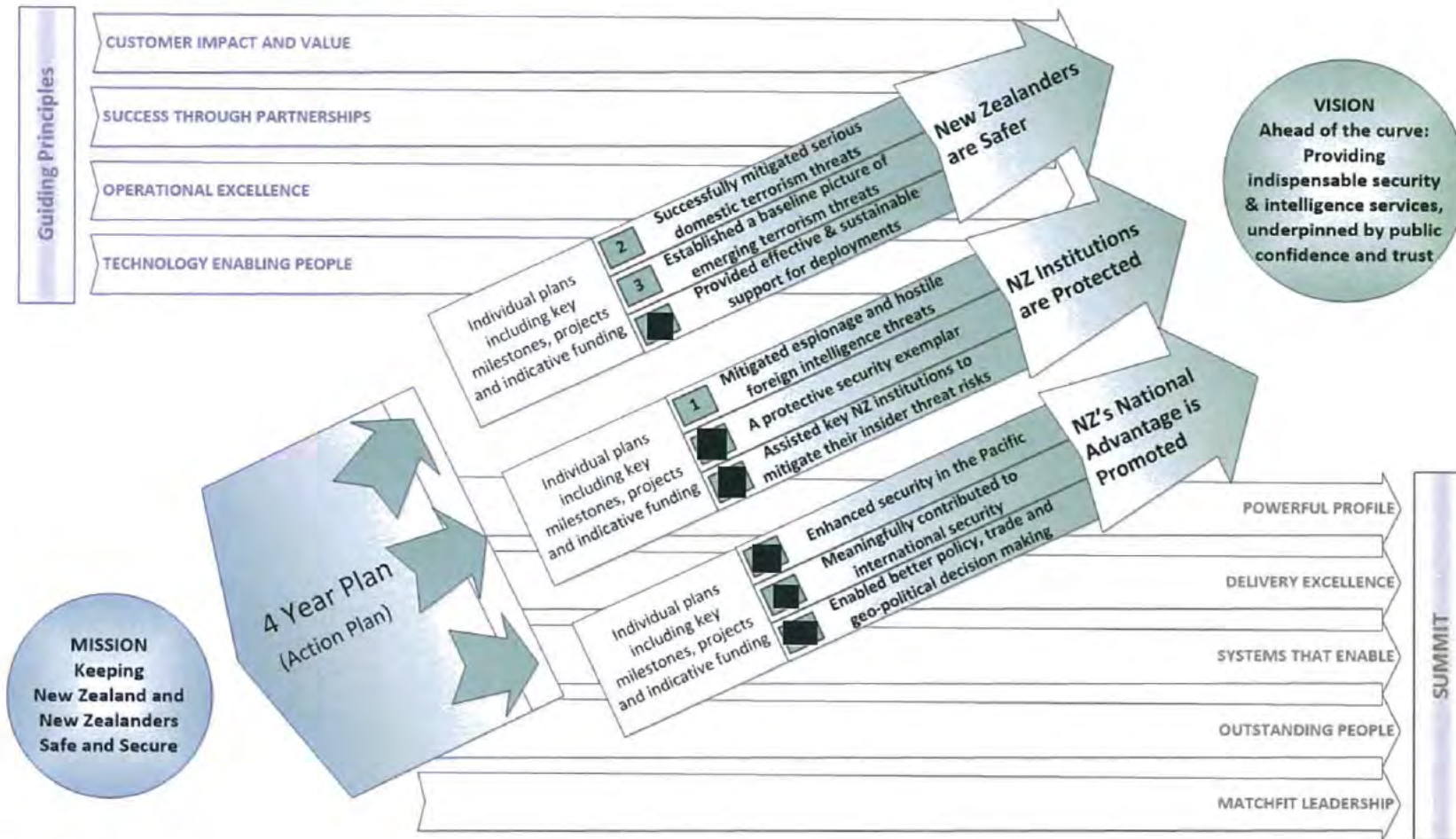
Goal 3: NZSIS has established an effective baseline picture of emerging terrorism threats

65. The STERLING strategy provided "strong guidance for strategic planning purposes and for determining the individual and collective action plans that will arise from [the] Strategy".²² It directed NZSIS widen its view on security threats with particular focus on greater exploration of those emanating from state actors and to scan the horizon for emerging threats as resources permitted.

66. This focus resonated with growing concern within Government and the New Zealand public regarding activities by foreign state actors to interfere in New Zealand's political system and unduly influence its foreign policy settings. s6a: describes classified NZSIS activity

[REDACTED]

²² (Appendix 19) Project STERLING: The NZSIS 10-Year Operational Strategy, June 2016 ([Link](#))



Project STERLING: NZSIS's ten-year operational plan prioritised its nine operational 'goals'.²³

²³ (Appendix 19) Project STERLING: The NZSIS 10-Year Operational Strategy, June 2016 ([Link](#))


Investigative Priority Setting Framework

67. NZSIS has been refining its investigative prioritisation process in recent years in an effort to strike the right balance between urgent information requirements and ensuring important but longer-term requirements are also addressed. The process also attempts to minimise human bias while preserving flexibility to reflect the professional instincts of experienced officers. The solution has been an objective 'weighting' model calculating a variety of inputs to produce an overall threat or risk score, which then informs discussion at regular s6a: describes NZSIS operational structure meetings s6a.²⁴


s6a: threat matrix / weighting model




s6a: describes operational processes



68. The s6a: process is limited to investigations, which hold a formal status and relate to known threats, or likely threats, to national security ('known knowns'). s6a: operational process



s6a: operational information



69. NZSIS's counter-terrorism unit reviewed and redesigned its leads management process in 2018.²⁶ s6a: operational process

Since February 2018, the unit has processed leads in a DMS-based workflow system, which allows investigators to process leads in one central location and provides a clear path for documenting decisions and actions undertaken for each lead.

Collection Priority Setting

70. s6a: operational process

71. s6a: process is an important, but not exclusive, tool for determining how collection resources are allocated. In 2015, AGUERO established a central Collection Hub:²⁷

This hub – in effect a 'portal' between the investigation and collection parts of the business – would be responsible for receiving questions from investigators, producing collection plans and commissioning specific capabilities to answer these questions... The collection hub would prioritise individual collection plans based on a consistent prioritisation framework, drawn from that used by the thematic teams.

72. The Collection Hub was the subject of a review in 2018, following which it has refined its processes and the scope of its role as a portal to collection resources.²⁸

s6a: operational process

s6a: operational process

²⁷ (Appendix 18) Project AGUERO: Review of the New Zealand Intelligence Community's Security Intelligence Operating Model, September 2015 ([Link](#))

²⁸ (Appendix 21) Collection Hub Review 2018, 18 April 2018 ([Link](#))

Question: Do NZSIS's prioritisation processes work effectively and have they produced appropriate focus?

National Security and Intelligence Priorities

73. With the issue of New Zealand's 16 strategic intelligence priorities in late 2018, the Government deliberately focused the NZIC on (but not limited it to) six main security and intelligence areas of responsibility. In light of its legislative functions and unique 'value-add', NZSIS has been especially focused on four: Foreign Interference (including espionage), Terrorism, Pacific Regional Security, and New Zealand's Strategic Interests [REDACTED]

s6a: classified information about NZSIS focuses

[REDACTED] Of themselves, however, the NSIPs are insufficient to guide the day-to-day priorities of NZSIS's intelligence functions.

Interpreting National Security and Intelligence Priorities

74. As highlighted above, NZSIS interprets the NSIPs through strategic assessments produced by NAB, CTAG and NZSIS's strategic analysis area. NAB has performed a central role in the framing of the NSIPs and its assessments provide more granular insights as to the varied threats to New Zealand's security that can be gleaned from the NSIPs alone. NAB's November 2018 assessment²⁹ detailed a wide array of security challenges, including those posed by state actors and by terrorism.

State Intelligence: Countering foreign espionage and interference

75. The NSIPs identify high-level requirements in respect of protecting New Zealand from foreign inference, including threats of espionage. Counter-espionage and interference has long been a core responsibility of the NZSIS and is identified as a key priority for the NZIC, and particularly NZSIS, through secret intelligence collection and reporting.³⁰

76. This importance is also reflected in NZSIS's operational strategy (STERLING), in which the mitigation of espionage and hostile foreign intelligence threats is noted as NZSIS's highest priority.³¹ The high priority placed on countering such threats has been informed by high-level strategic analysis. s6a: describes classified analysis

[REDACTED]:³²

²⁹ s6a [REDACTED]
³⁰ (Appendix 16) NSIPS Supporting Organising Framework, December 2018 [ERS-18-SUB-0026] ([Link](#))

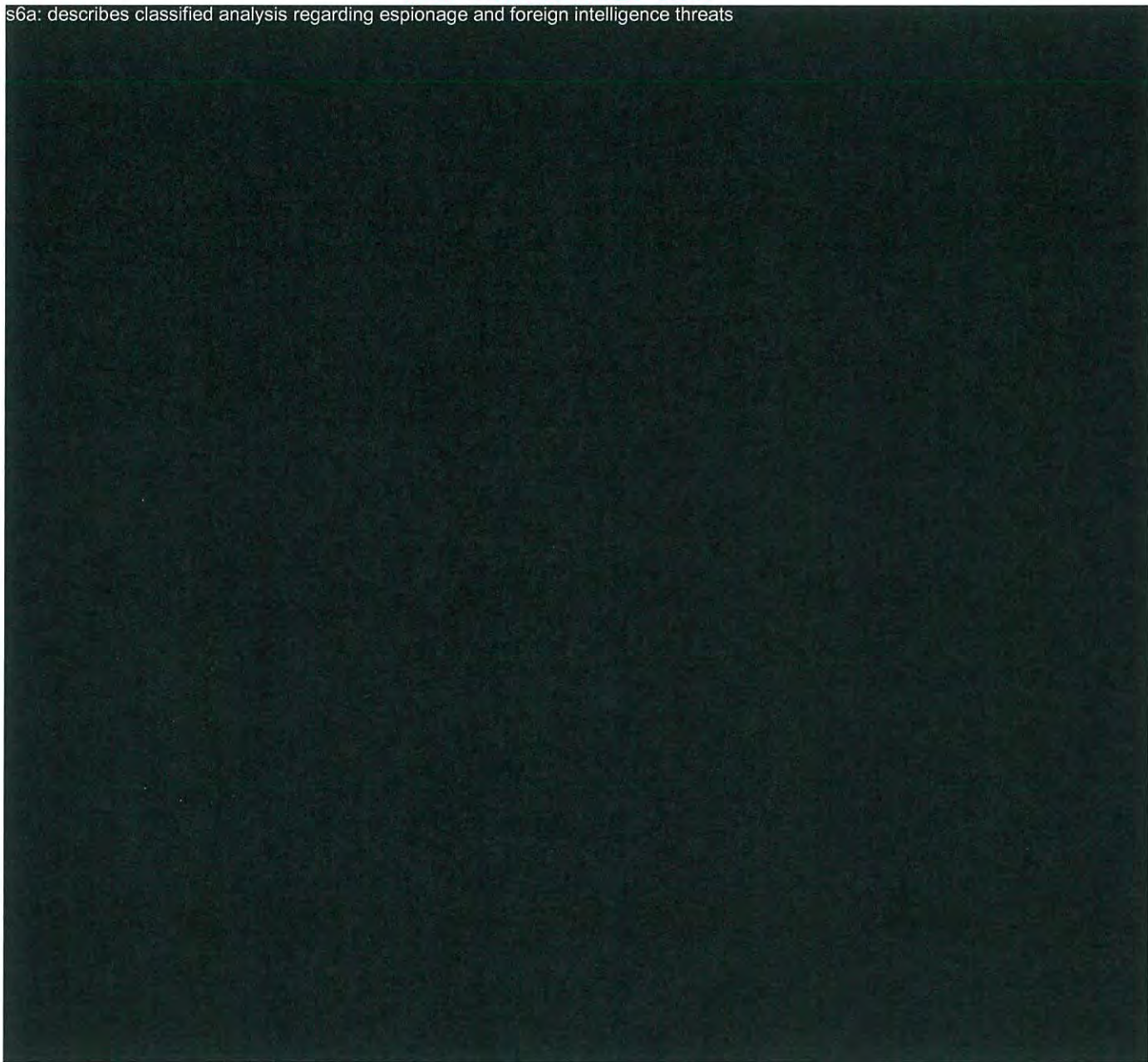
³¹ (Appendix 19) STERLING Goal 2: NZSIS has successfully mitigated serious domestic terrorism threats; see: Project STERLING: The NZSIS 10-Year Operational Strategy, June 2016 ([Link](#))

³² s6a [REDACTED]

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a: describes classified analysis regarding espionage and foreign intelligence threats



79. With continuing threats to New Zealand's interests from capable foreign state actors, s6a: classified assessment and elevating concerns among Western democracies regarding the stability of the global rules-based order, NZSIS's focus on state intelligence investigations has been appropriate.

s6a: references classified reports

~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

80. In recent years, perhaps the greatest challenge in NZSIS's efforts to appropriately prioritise and resource its state intelligence investigations has been the urgent need for NZSIS to respond to terrorist threats. Potential threat-to-life investigations related to the Islamic State were, understandably, prioritised above the important but more long-term threats to New Zealand's economy and democracy from foreign interference and espionage. AGUERO and STERLING sought to ensure an appropriate balancing of the 'urgent' with the 'important'. Accordingly, the Review considers NZSIS's deliberate prioritisation of resources into these state intelligence threat investigations was warranted, reasonable and commensurate with the threat posed.

s6a: describes a case study of a state intelligence investigation regarding a foreign intelligence officer visiting New Zealand

Counter-Terrorism

81. The NSIPs confirm terrorism as a priority intelligence requirement for the Government and, like foreign interference, a key priority for the NZIC's secret intelligence capabilities.³⁵ Informed by a variety of domestic and foreign strategic assessments, NZSIS's STERLING operational strategy also places counter-terrorism efforts at the top of the organisation's priorities behind only the mitigation of espionage and hostile foreign intelligence threats. NZSIS's counter-terrorism strategy is not limited to the investigation of known terrorist threats or potential threats,³⁶ but extends to identifying and understanding emerging threats.³⁷

82. Following the 11 September 2001 terrorist attacks in the United States, and a decade of Al-Qaeda directed or inspired global terrorism, New Zealand's terrorist threat environment has been dominated by the threat of violent Islamist extremism. This has been heavily reflected in strategic assessments s6a: describes authors of strategic assessments

. A comparative lull in the Al-Qaeda threat was broken with the rise of Islamic State in 2014. Through until early 2018, NZSIS's investigative resources on counter-terrorism were fully engaged on the investigation of credible threats from New Zealand supporters of Islamic State to either participate in hostilities abroad (notably in Syria) as members of a designated terrorist organisation or, if unable or unwilling to travel,

³⁵ (Appendix 16) NSIPS Supporting Organising Framework, December 2018 [ERS-18-SUB-0026] ([Link](#))

³⁶ (Appendix 19) STERLING Goal 2: NZSIS has successfully mitigated serious domestic terrorism threats; see: Project STERLING: The NZSIS 10-Year Operational Strategy, June 2016 ([Link](#))

³⁷ (Appendix 19) STERLING Goal 3: NZSIS has established an effective baseline picture of emerging terrorism threats; see: Project STERLING: The NZSIS 10-Year Operational Strategy, June 2016 ([Link](#))

to mount, encourage, support or mount terrorist attacks or undertake activities in support of terrorism in New Zealand. Given the rudimentary attack methodologies used successfully by Islamic State supporters in the United Kingdom, Europe and Australia including knife attacks and driving vehicles into pedestrians, these New Zealand-based subjects of investigation were capable of rapid escalation to violence and required close attention.

83. Continuing Islamic State-related threats prompted CTAG to raise New Zealand's national terrorism threat level from VERY LOW to LOW in 2014 (a significant change for a country unaccustomed to the threat of terrorism).

s6a: describes details about specific terrorism threats

[REDACTED]

s6a: describes an Islamic State-related case study, including details about the nature of operational activity

[REDACTED]

84. The focus of NZIC strategic assessments, informed by an unprecedented level of domestic Islamic State-related threats, reinforced NZSIS's primary counter-terrorism focus on Islamist extremism, specifically Islamic State and its adherents. Despite this focus, the NZIC was aware of trends in international right-wing ideology and their potential to drive changes in New Zealand's threat environment before the 15 March 2019 terrorist attacks. The CTAG national threat assessment for New Zealand noted the concerning trend of right-wing extremism but considered the possibility of an attack by an extreme right-wing lone actor to be remote.

85. Strategic assessments, including the CTAG's January 2018 analysis of New Zealand's terrorism threat environment, have made regular note of the possibility of an attack by an unknown lone actor:³⁸

CTAG assesses there are also individuals in New Zealand for whom the extent of their radicalisation and mobilisation to violence may not be fully known by law enforcement and security agencies. There is a realistic possibility an unknown lone actor could move from radicalisation to action, without intelligence forewarning, and potentially in a short timeframe.

While those inspired by Islamic State's sophisticated propaganda and its use of secure online forums for radicalising their supporters around the world were a natural focus for NZSIS, the experiences of other Western countries show lone actors can emerge from any number of extreme religious, ideological or political motivations,³⁹ such as the Oklahoma City bombings in the United States, mass-shootings perpetrated by Anders Breivik in Norway and Alexandre Bissonette in Canada, or Darren Osbourne's vehicle attack on worshippers at Finsbury Mosque in the United Kingdom.

s6a: describes an Islamic State-related case study, including details about the nature of operational activity

86. Although the threat of a 'lone actor' attack remains a common concern among Western (and other) security services, detecting and disrupting such threats has been notoriously difficult using traditional investigative models. Ordinarily, the perpetrators' real-world social isolation and ability to anonymise their online activities weakens the threat signals security services typically rely upon for lead generation, and often frustrates traditional intelligence collection methods. Moreover, their emulation of Islamic State's rudimentary modes of attack allows lone actors to mount attacks with little or no warning.

³⁸ (Appendix 26) CTAG Threat Assessment: The New Zealand terrorism threat environment (082/18/TA), dated 16 January 2018 (DMS60-8-1105) ([Link](#))

³⁹ (Appendix 27) Age of the Wolf: A Study of the Rise of Lone Wolf and Leaderless Resistance Terrorism, 15 February 2015 ([Link](#))

87. The Review concludes NZSIS was not unduly focused on the threat of Islamist extremism in the two years leading up to 15 March 2019. Decisions, informed by credible strategic assessments, had to be taken about which threats to prioritise. These decisions meant emerging threats from rising right-wing extremism and lone actors could only realistically be pursued as additional resources became available.

88. This occurred with the induction and training of a cadre of new NZSIS investigators in March-April 2018, [REDACTED]

s6a: describes organisational structure

[REDACTED] As the result of a deliberate decision, the counter-terrorism unit expanded its focus to pursue wider baseline coverage and discovery efforts aimed at identifying and assessing previously unidentified terrorist threats. By mid-2018, the counter-terrorism unit had instituted a new work programme [REDACTED]

s6a: operational detail

[REDACTED] for baseline and discovery projects [REDACTED]

s6a: operational detail

[REDACTED] investigations and leads processing. Among the new priorities was a baseline project on the threat of right-wing extremism in New Zealand.

s6a: table with top 20 investigations as at 11 February 2019 (extant 15 March 2019)

89. In terms of NZSIS's intelligence priorities at the time of the 15 March attacks, there was a clear correlation between the Government's high-level NSIPs and the associated areas of organisational focus within its intelligence function – in particular counter terrorism and state intelligence. Considering the intelligence prioritisation frameworks in place, the Review considers the focus of NZSIS's intelligence function was appropriate at the time of the Christchurch terrorist attacks. In line with its STERLING goals, nine of the top 20 investigations related to State Intelligence threats, while eight (including the two highest ranking investigations) related to counter-terrorism efforts.⁴⁰ NZSIS commitment of approximately 50 percent of its investigative resources to state intelligence (NZSIS's highest priority) and slightly less to counter-terrorism was consistent with the deliberate decisions in its STERLING operational strategy and the Government's NSIPs.

90. While counter-terrorism efforts were focused primarily on Islamic State and other Islamist extremist threats, as resources increased and the threat from ISIS in New Zealand stabilised, NZSIS re-prioritised counter-terrorism resources towards the identification of previously unknown terrorist threats. In line with STERLING Goal 3 (emerging terrorism threats), the objective of the change was to establish broad baseline understandings of

⁴⁰ s6a: classified reference

diverse threats, against which to monitor for change, and discover new lead information pertaining to specific threats. As will be addressed in detail later, this initiative included a focus on the assessed rise of right-wing extremism.

Question: What issues exist within the current intelligence prioritisation process?

91. An important element of NZSIS's reform programme has related to how NZSIS interprets the high-level NSIPs and sets its investigative and operational priorities. While those priorities relating to NZSIS's enabling frameworks are Government mandated, those relating to NZSIS's areas of specific intelligence focus are internally generated. These internal processes are reasonably well developed, being informed by NZSIS's strategic analysis capability and CTAG threat assessments and through NZSIS's operational strategy (STERLING). Lower level prioritisation processes to inform investigative priorities, and to a lesser extent leads, also exists.

92. The Review considers NZSIS's prioritisation processes are broadly correct and in alignment with Government priorities and strategic assessments. As for any prioritisation system undergoing change, NZSIS is not without areas which might benefit from further development. These relate to:

- The lack of clearly articulated 'enduring' or 'thematic' information requirements: while the NSIPs provide high level direction regarding priorities, there is a gap in the translation of NSIPs into mid-level enduring or thematic information requirements. s6a: operational details about information requirements and priority setting



- NZSIS-wide understanding of the value of strategic analysis: NZSIS's foresight and investment in developing its own strategic analysis capability (outside the SCRR funding programme) is commended. However, this remains a fledgling capability whose role in guiding NZSIS's intelligence functions does not yet appear to be fully embedded. It will be important that NZSIS continues to build a wider understanding of how to use NZSIS's and products produced by the area including in the development and shaping of the enduring/thematic information requirements recommended above;

- The intelligence prioritisation framework: the current ^{s6a} process, while a laudable effort, would benefit from further refinement. ^{s6a: operational details about intelligence prioritisation}

[Redacted]

- ^{s6a: operational detail about prioritisation}

[Redacted]

- The priority given to producing and disseminating lower-classification level reporting: in order to have increased impact with domestic partners, particularly New Zealand Police, NZSIS needs to ensure that analytical and investigational reporting reaches as broader readership as possible. It is important that efforts continue to produce such material at very low levels (or no) classification and as necessary find alternate mechanisms to get that reporting to customers.

Recommendations - It is recommended NZSIS:

1. Produce and regularly review enduring information requirements, particularly in terms of emerging areas of security threat;

2. Continue to build understanding across NZSIS of the critical role played by strategic analysis in the priority setting processes.
3. Review and adjust, as necessary, NZSIS's threat/risk assessment processes underpinning the ~~s6a~~ to better reflect the changing terrorist *modus operandi* whereby the capability to undertake an attack must now be presumed as a given.

Question: Did these issues substantively impede the discovery of ~~the individual~~

93. The Review does not believe the issues identified above substantively impacted on NZSIS's likelihood of identifying ~~the individual~~ attack planning.

94. Even given some issues surrounding the absence of enduring or thematic information requirements, the importance of discovery and baselining work was highlighted as NZSIS's third highest priority in its intelligence strategy and resources were made available to pursue this priority directly ~~s6a: operational structure~~. The fact that extreme right wing concerns had been highlighted in strategic assessments, ~~s6a / s6b(l): classified assessment~~ and were included in the baselining programme provided further indication that the system was operating appropriately.

95. Further, it is considered that potential issues surrounding the resourcing of lead generation were unlikely to have impacted on the identification of ~~the individual~~. As Part 1 of this report confirmed, NZSIS had no derogatory information regarding ~~the individual~~ prior to the 15 March 2019 attacks. NZSIS's investigation of the extreme right wing is considered later in the Review and it indicates that ~~the individual~~ left very little by way of signal or leads to suggest he was considering an act of terrorism. It is considered that in the lead up to the attack his planning was such that he was highly unlikely to come to the attention of officials in a way which would have lead to the intrusive investigation necessary to identify his intent.

Part 2.2. NZSIS Resource Allocation

Question: How are decisions made on resourcing NZSIS's Intelligence Directorate?

96. By world standards, NZSIS is a small service with a broad and diverse mandate. This, combined with its ambitious business renewal programme, can make resourcing decisions difficult. Balancing a requirement to develop and build resilient and credible corporate foundations while fulfilling NZSIS's intelligence functions, means that not everything can be a priority.

97. Under SCRR, NZSIS has received substantial Government investment in its staffing and capabilities. As highlighted, this has resulted in NZSIS redesigning its organisational processes and structures in the pursuit of greater efficiency and resilience. This renewal prioritised NZSIS's enabling functions – a well-reasoned decision based on the number of factors already outlined.

98. This section of the report will not address the allocation of resources across the entire NZSIS and the rationale for those decisions. Instead the Review has focused on the allocation of resources to NZSIS's intelligence function, namely the Intelligence Directorate, to consider whether these decisions adequately reflected NZSIS's priorities and were reasonable in the context of NZSIS's rapid growth, and its intelligence priorities.

99. In December 2017, NZSIS published its implementation plan for refreshing the organisation's corporate and change governance structures.⁴¹ The plan included the establishment of a 'Workforce Board', overseen by NZSIS's Capability Committee. The Board is responsible for monitoring workforce planning "to ensure NZSIS grows in a balanced, carefully phased way and that workforce growth is sustainable."⁴²

⁴¹ (Appendix 29) **S6a** Implementation: Refreshing corporate and change governance: Decision Paper, December 2017 ([Link](#))

⁴² (Appendix 30) Principles for Monitoring the NZSIS Workforce Plan – as at 31 August 2018, 31 August 2018 ([Link](#))

Workforce Board

Purpose and functions

The new Workforce Board will support the Capability Committee through supervising planning and policies for workplace relations, talent attraction, retention, management, performance, remuneration and incentives. It will primarily be an advisory committee, seeking ratification for its recommendations from the Capability Committee.

The Workforce Board will exemplify the separation of governance and management responsibilities. It will work closely with ICSS People & Capability to ensure relevant outsourced functions continue to be managed to meet the NZSIS's needs.

The Workforce Board will also:

- act as the main conduit to the NZIC Strategic Workforce Governance Group, with which it will share some members
- take on any outstanding responsibilities of the Delivering Growth Working Group once the latter is wound down.


Membership

s6a



Meeting schedule

Meetings will be held monthly.

100. Growth for a security and intelligence service is difficult. Workforce planning is complicated by long lead times from the start of the recruitment process to starting necessary vetting processes, which leads to higher than usual attrition rates among prospective employees. Additionally, many of the specialist skills NZSIS requires are not available in the open labour market. NZSIS must develop its workforce's specialist skills internally, at times from a low base, imposing a significant training burden on the organisation. Internal training courses are often intensive (often over weeks or months), with high qualification ('pass') standards and at times, significant failure rates – 

s6a: operational details

⁴³

101. Accordingly, workforce growth can be unpredictable and, at times, unbalanced. Despite this, Cabinet's approved SCRR 'scenario three' envisioned an ambitious growth rate to achieve specific capability 'bricks' or improvements over its four-year timeframe (see figure below detailing SCRR growth highlights).⁴⁴

⁴³ (Appendix 30) Principles for Monitoring the NZSIS Workforce Plan – as at 31 August 2018, 31 August 2018 ([Link](#))

⁴⁴ (Appendix 31) Highlights of SCRR Growth: Building Trust and Confidence through the First Four Years of Scenario Three to 2020, April 2019 ([Link](#))



Highlights of SCRR Growth

Building Trust and Confidence
through the First Four Years of Scenario Three to 2020

see: details about operational capabilities




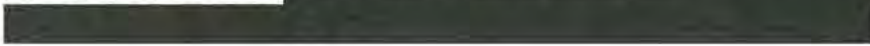
Highlights of SCRR Growth: The New Zealand Intelligence Community has grown its capabilities substantially under the SCRR investment programme⁴⁵

⁴⁵ (Appendix 31) Highlights of SCRR Growth: Building Trust and Confidence through the First Four Years of Scenario Three to 2020, April 2019 ([Link](#))

s6a: details of operational capabilities

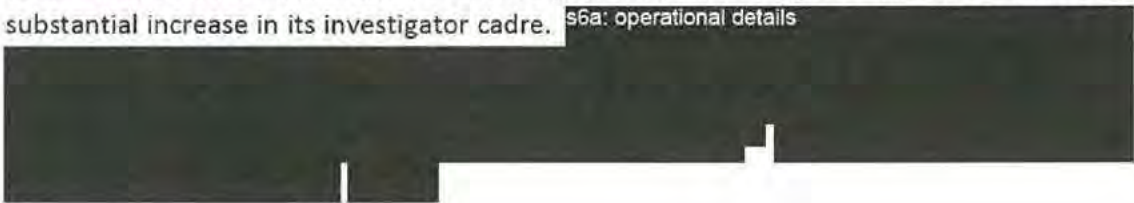


103. As previously highlighted, domestic threat operations are not limited to counter-terrorism, but also include counter-espionage and foreign interference, and 'insider threats'. It was necessary, and reasonable, for NZSIS to divide its growing investigative resources across all three areas, s6a: details of operational prioritisation


Investigative Resources

104. In accordance with NZSIS's STERLING priorities, the Intelligence Directorate pursued a substantial increase in its investigator cadre. s6a: operational details



NZSIS Organisational Chart

s6a: operational details



s6a: operational details



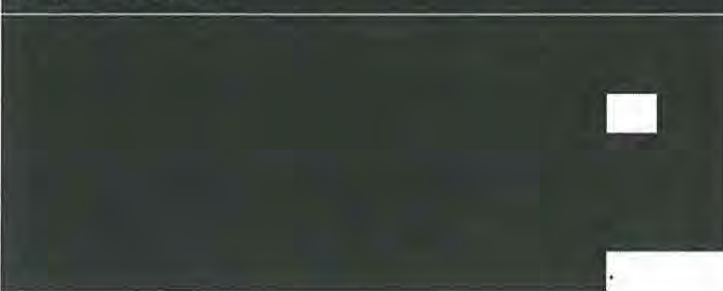
105. s6a: operational details



Analytical Resources

106. NZSIS's post-SCRR development of an internal strategic analysis capability was also nurtured during 2018.

s6a: operational details



NZSIS Organisational Chart

Engagement, Analysis and Reporting

s6a: organisational chart



107. The strategic intelligence analysis team had partnered its analysts with specific thematic areas and investigative teams, such as counter-terrorism, for building subject matter expertise. However, following a review of its operating model in 2018, the team moved to a new model centred on collaborative projects rather than subject matter portfolios. The new model was intended to give the team the flexibility to respond to evolving priorities and contribute efficiently and effectively

s6a: operational details

Given the resourcing of the area, this was a reasonable decision.

Intelligence Collection Resourcing

108. As highlighted above, NZSIS's s6a prioritisation of investigations was paired with the Collection Hub's processes for managing the tasking and deployment of NZSIS's collection resources. These systems help to ensure that:

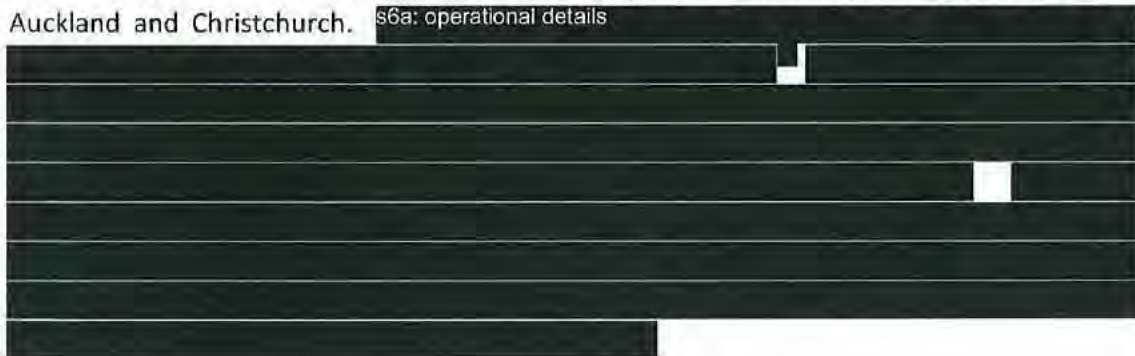
- urgent investigations did not always trump those that were important;
- NZSIS maintained the flexibility to take advantage of emerging intelligence opportunities; and

- NZSIS maintained high levels of flexibility to adapt to changing security circumstances and requirements.

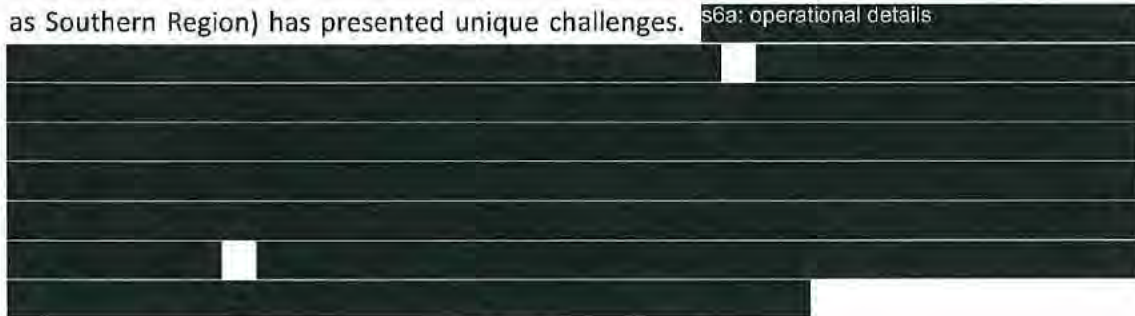
109. ~~s6a: operational details~~


Regional Office Resources

110. In addition to its headquarters in Wellington, NZSIS maintains regional offices in Auckland and Christchurch. ~~s6a: operational details~~



111. By contrast, NZSIS's maintenance of a fully operational office in Christchurch (known as Southern Region) has presented unique challenges. ~~s6a: operational details~~



⁴⁹ (Appendix 33) See for example: Auckland: SLT Discussion, 25 October 2018 ([Link](#))

112. s6a: operational detail . s6a: operational details

Question: Were these resourcing decisions effective?

113. At the strategic level, NZSIS's total staffing numbers broadly align with Government agreed priorities and expectation for growth under SCRR. Despite the SCRR funding (in fact, because of it), NZSIS experienced wide-ranging resource pressures and competing tensions, notably the need to build enabling functions while also preserving its operational capabilities. NZSIS's planned approach saw enabling functions grow first. As the Review has already noted, this was a reasonable decision. Although it arguably delayed the arrival of 'front-line' capabilities, the organisation was better placed to raise, train and sustain those capabilities when the time came. NZSIS's shift in priority towards investigative and operational staffing was apparent in the scale of its recruitment and training of additional investigators throughout 2018.

114. Building the Intelligence Directorate's capability following NZSIS's organisational renewal was planned and appropriate. The Intelligence Directorate's resourcing is broadly in accord with its workforce planning, s6a: operational details

115. The decision to invest in NZSIS's strategic intelligence analysis capability was a sound one, which, once fully embedded, should generate improved efficiencies for NZSIS and heightened assurance for Government that NZSIS's intelligence function is focused where it needs to be. The Review notes that in the absence of dedicated SCRR funding this initiative was arguably at the expense of other capabilities prioritised under NZSIS's initial SCRR implementation plans. However, it does not appear that the recruitment of investigators was constrained by this decision. The Review notes that while experiencing a substantial increase in numbers in 2018, half NZSIS's investigative staff had less than one year's

s6a: operational details regarding workforce planning

experience at the time of the 15 March 2019 attacks – markedly diluting the group’s average experience levels. This was a natural and inescapable consequence of NZSIS’s rapid growth and strategic workforce sequencing decisions, but will be less consequential within 2-3 years as investigative experience is developed. ~~s6a: operational details~~

116. Within the counter-terrorism unit there was an appropriate and justifiable focus on Islamic State related investigations, in light of the threat the group and its adherents posed and evidence of attacks and attack planning throughout the world. It is noted, however, this focus was not all-encompassing and NZSIS was alive to the possibility of non-Islamic extremist threat.

117. Upon the arrival of additional investigative resources ~~s6a: operational details~~, and apparent stabilisation of the threat posed by Islamic State adherents, NZSIS’s deliberate decision to expand its focus through discovery and baseline programmes was well-considered. As will be addressed in detail later in the report, the counter-terrorism investigative area dedicated ~~s6a: operational details~~ capacity to projects aimed at identifying residual risks and to generating leads and developing baseline understanding of wider domestic, global and thematic threats and their significance for New Zealand. The inclusion of right-wing extremism in this baselining programme was consistent with trends identified in some domestic and international strategic analysis and liaison reporting. By March 2019, the baseline review of right-wing extremism in New Zealand was one of the unit’s more advanced projects.

118. ~~s6a: operational details about allocating collection resources~~

[REDACTED]

Question: Are there resourcing matters which would benefit from reconsideration?

119. The Review made a deliberate decision not to comment on staffing levels across NZSIS. It is likely each work area could make a case, often compelling, for increased resources. This decision was based primarily on the fact that the Review team had spoken to only a select sample of staff, and to recommend increased staffing in those areas, without considering the needs of others was problematic. That said, through its enquiries, the Review has identified a small number of areas where it is of a view that serious resourcing questions warrant further consideration.

120. There are two broad resourcing themes for NZSIS's consideration:

s6a: specific details about staffing pressure points



Released by the Director-General of Security

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a: specific details about staffing pressure points



~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

Released by the Director-General of Security

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a: specific details about staffing pressure points



~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

- Inefficient use of resources: the very limited direct access to data causes inefficiencies and a lack of timeliness. Lead intelligence is often fragmentary, and in need of clarification and context for better decision-making.

s6a: operational details about accessing information



- Direct access to data and information: there are data-sets which legislation has explicitly authorised NZSIS to access, under direct access agreements, pursuant to Schedule 2 of ISA 2017. The Review notes, in nearly two years since the legislation was enacted, direct access to two data-sets (both held by NZ Police) have yet to be achieved. Moreover, other than for access to Financial Intelligence Information (in a separate NZ Police database), the purpose for NZSIS's direct access is limited to obtaining information about people and locations posing a possible physical threat to NZSIS personnel, not advancing NZSIS's intelligence function. This seems unduly limiting and should be revisited as part of a review of ISA 2017.

- Monitoring rather than investigating

s6a: operational details




Recommendations - It is recommended NZSIS:

s6a: operational details about capabilities



s6a: operational details about capabilities




Question: Did resourcing decisions substantively impact on NZSIS's ability to identify the individual?

121. The Review concluded that decisions surrounding resources were reasonable and broadly aligned with NZSIS's planning parameters. While projected staffing numbers are slightly behind within the Intelligence Directorate this is understandable given the particular difficulties and issues of recruiting and training staff generally new to an intelligence environment.

122. The Review did identify a small number of staffing pressure points (and no doubt there are more) and areas where for a range of reasons, including those beyond NZSIS's control, resource usage might be considered inefficient.

123. s6a: operational details



124. That said, it is considered highly unlikely extra permanent staffing in the South Island would have substantively increased the likelihood of NZSIS identifying the individual's planning, although this possibility cannot be entirely discounted. As detailed later in this report, subsequent investigations revealed the individual left very little by way of signal or leads to suggest he was considering an act of terrorism. It is considered that, even if there had been significantly greater NZSIS resources in the South Island, the secrecy involved in the individual's planning was such that he was highly unlikely to come to the attention of officials in a way which would have lead to the intrusive investigation required to identify his intent.

Part 2.3. NZSIS Legal and Compliance Frameworks

Question: How does NZSIS regulate its activities?

Significant Developments in Legal and Compliance Frameworks

125. As set out in more detail below, during the past five years NZSIS has been through a significant period of review in regard to its legal and compliance frameworks. The development of these new frameworks and their implementation into NZSIS has required particular effort and focus and added to NZSIS's already significant change programme. Key developments have included:

- An Independent Review of Intelligence and Security in New Zealand by Dame Patsy Reddy and Sir Michael Cullen in 2016 (the Cullen-Reddy report);
- Major legislative change resulting in the introduction of ISA 2017 (incorporating 4 acts into one);
- The development and issue of 12 new Ministerial Policy Statements (MPSs) setting out the Minister's expectations in regard to otherwise lawful activities;
- The development, promulgation and training of staff in respect of the external and internal policies needed to implement the new legislation;
- NZSIS becoming a Government Department (part of the state sector);
- Increased oversight by the IGIS; and
- NZSIS is now subject to more privacy principles under the Privacy Act 1993 than was the case before the new legislation came into force.

Independent Review

126. Changes to the law in 2013 required the Government to carry out periodic reviews of intelligence and security agencies, the legislation governing them and their oversight legislation.⁵¹ In 2015, the New Zealand Government commissioned an independent review of NZSIS and GCSB. The purpose of the review was to determine whether:

⁵¹ (Appendix 34) Section 21 Intelligence and Security Committee Act 1996 ([Link](#))

- a. the legislative frameworks of the agencies were well placed to protect New Zealand's national security, while protecting individual rights; and
- b. the existing oversight arrangements provided sufficient safeguards at an operational, judicial and political level to ensure the agencies act lawfully and maintain public confidence.

127. The Cullen-Reddy report contained 107 recommendations, most notably a proposal to replace the legislation governing the agencies and their oversight agencies with a single Act and authorisation regime.⁵² The report expressed concern about unnecessary barriers to co-operation between the intelligence and security agencies, and with other public sector agencies, such as New Zealand Police.

128. Other recommendations included:

- institutional arrangements, with a view to bringing the intelligence agencies into the normal state sector arrangements, with exceptions as appropriate;
- ensuring all activities are the subject of clear legal authorisation;
- addressing a number of issues in legislation for the first time, including bringing HUMINT activities within the legislative framework and providing for certain issues relating to access to and sharing of information; and
- enhancing oversight and safeguards through strengthening and clarifying the Inspector-General of Intelligence and Security's oversight of the agencies, expanding the role of the Intelligence and Security Committee, and provision for a judicial role within the warranting and authorisation framework.

The Intelligence and Security Act 2017

129. In response to those recommendations the Government passed the Intelligence and Security Act 2017 (ISA 2017)⁵³ into law on 28 March 2017. ISA 2017 came into force in two stages, the initial provisions on 1 April 2017 and the majority on 28 September 2017. ISA

⁵² (Appendix 35) Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand (Cullen-Reddy Report), 29 February 2016 ([Link](#))

⁵³ (Appendix 8) ISA 2017

2017 combined together the legislation governing both of the security and intelligence agencies and their oversight bodies,⁵⁴ and made changes to a number of others.⁵⁵

130. The purpose of ISA 2017 is described as “to protect New Zealand as a free, open and democratic society.” New Zealand’s intelligence and security agencies’ (GCSB and NZSIS) three principal objectives⁵⁶ are to contribute to the protection of New Zealand’s national security,⁵⁷ the international relations and well-being of New Zealand and the economic well-being of New Zealand. NZSIS and GCSB’s shared key functions⁵⁸ are intelligence collection and analysis; protective security services, advice and assistance; co-operation with NZ Police and the New Zealand Defence Force to facilitate the performance of NZ Police and New Zealand Defence Force functions; and co-operation with other entities to respond to imminent threats to life and safety of certain persons.

131. As recommended in the Cullen-Reddy review, the agencies are subject to increased oversight. The Intelligence and Security Committee has primary responsibility for parliamentary oversight of the agencies. The Committee may now be comprised of between five and seven members including the Prime Minister and the Leader of the Opposition.

132. ISA 2017 has also made the agencies subject to almost all of the Information Privacy Principles in the Privacy Act 1993⁵⁹ which are subject to oversight by the Privacy Commissioner.⁶⁰

133. ISA 2017 provides for greater oversight by the IGIS (further detail below), who has significant powers of inquiry.

Warrants

134. The agencies can seek a warrant under ISA 2017 to authorise certain activities that would otherwise be unlawful (for example, search and seizure, intercept of private communications, surveillance in a private place). The primary forms of warrants are Type 1

⁵⁴ ISA 2017 replaced the New Zealand Security Intelligence Service Act 1969; the Government Communications Security Bureau Act 2003; the Inspector-General of Intelligence and Security Act 1996 and the Intelligence and Security Committee Act 1996.

⁵⁵ For example, amendments were made to the Customs and Excise Act 1996; Immigration Act 2009; Passports Act 2002 and the Privacy Act 1993.

⁵⁶ Section 9 ISA 2017.

⁵⁷ “National security” is not defined in ISA 2017.

⁵⁸ Sections 10, 11, 13 and 14 ISA 2017. The GCSB has an additional function of providing information assurance and cyber security activities under section 12 ISA 2017.

⁵⁹ (Appendix 36) Privacy Act 1993

⁶⁰ NZSIS was always subject to oversight by the Privacy Commissioner but previously had more exemption from the privacy principles than is currently the case under ISA 2017.

and Type 2 warrants⁶¹ and, in some circumstances, the agencies can request a warrant against a class of persons.⁶² Class warrants enable the agencies to seek authorisation to target individuals whom fit within a class or group of people, for example, individuals NZSIS assess to be officers of a particular foreign intelligence agency, who have travelled or likely will be travelling to New Zealand.

135. If seeking authorisation to collect information about, or to do any other thing directly in relation to, New Zealand citizens and permanent residents, NZSIS must seek a Type 1 warrant. Before signing a warrant, the Minister and a Commissioner of Intelligence Warrants (a former High Court Judge) must be satisfied that the issue of the warrant will enable the intelligence and security agency to carry out an activity that is necessary to contribute to the protection of national security; and “identifies, enables the assessment of, or protects against” any of the seven listed “harms” (including terrorism or violent extremism, espionage directed against New Zealand, threats to information infrastructures, has the potential to damage New Zealand’s international relations or economic well-being etc.).

Ministerial Policy Statements (MPS)

136. ISA 2017 requires the responsible Minister to issue Ministerial Policy Statements (MPSs) to guide the agencies on lawful activities they can undertake without the authorisation of a warrant. Some examples of areas ISA 2017 requires the Minister to issue an MPS on are:

- requesting information from private and public sector agencies;
- collecting information lawfully from persons without an intelligence warrant or authorisation (i.e. human intelligence collection methods);
- conducting surveillance in a public place;
- obtaining and using publicly available information;
- cooperating with an overseas public authority;
- providing advice and assistance to an overseas public authority; and
- sharing intelligence with an overseas public authority.

⁶¹ There are also practice warrants (sections 88-101 ISA 2017) and agencies may request “urgent” and “very urgent” authorisations (sections 71 – 82 ISA 2017).

⁶² For national security warrants and activities in relation to persons associated with foreign governments or designated terrorist entities see section 53(b) ISA 2017.

Policies

137. To support the introduction of the new legislative regime, NZSIS implemented a range of internal policy and procedural documents to guide staff on how to conduct day-to-day business and adhere to ISA 2017, other legal obligations and the MPSs. Approximately 50 new policies and processes have been introduced to NZSIS since April 2017 in response to, or in anticipation of, the new Act. In addition to this, existing processes and policies required review to ensure that they were consistent with the new legislation and the MPSs. There are also a range of operational policies which seek to provide increased clarity to what can be ambiguous (or difficult to interpret) legislative principles.

Direct Access Agreements

138. ISA 2017 provides for the agencies to negotiate agreements to directly access certain public sector databases where the information is relevant to their functions and is required on a frequent basis.⁶³ The Minister responsible for NZSIS/GCSB and the Minister responsible for the agency holding the database must jointly determine the terms of the direct access agreement relating to that specific database and both Ministers must be satisfied there are adequate safeguards to protect the privacy of individuals. The Minister must consult with the IGIS and the Privacy Commissioner before entering into a direct access agreement.⁶⁴ Under the terms of the existing Direct Access Agreements, amongst other requirements, NZSIS employees are required to complete training before they can directly access another agency's information and must record the purposes for access to enable auditing of NZSIS's use of this information.

Restricted Information

139. ISA 2017 provides a process somewhat akin to a warrant where the agencies can request permission from the Minister Responsible for NZSIS and a Commissioner of Intelligence Warrants to access information that is one of the four types of 'restricted information' under ISA 2017⁶⁵ (for example, tax or adoption information). Before granting permission, the Minister and Commissioner must be satisfied of certain matters, including that the privacy impact of permitting access is proportionate to the purpose for which the restricted information is sought.

⁶³ See schedule 2 of ISA 2017, databases listed include: birth, civil union, death, marriage and name change information held by the Registrar-General; citizenship information held by the Secretary for Internal Affairs; Information collected by the Ministry of Business, Innovation, and Employment in connection with the performance or exercise of a function, duty, or power under the Immigration Act 2009; Information about border-crossing etc. held by New Zealand Customs Service; and financial intelligence information held by New NZ Police and information about people and locations identified as posing a possible physical threat to GCSB or NZSIS employees.

⁶⁴ Sections 126, 127 and 128 ISA 2017

⁶⁵ See section 135 ISA 2017

Access to business records of telecommunications networks and financial service providers

140. ISA 2017 provides that the Minister Responsible for NZSIS and the Commissioner of Intelligence Warrants may issue an approval to an agency to access business records (about an identifiable individual). This is known as a Business Record Approval. Business Record Approvals set out the general situations in which a Director-General of an agency may issue a direction to a telecommunications network operator or financial services provider to provide documents to the agency in question. 'Business records' is defined in ISA 2017 as information such as customer or subscriber information, bank account or credit card details, call associated data and details of mobile data usage (but does not include the content of emails, messages, phone conversations etc.).

141. Before the Minister and Commissioner issue an approval to access business records, they must be satisfied that, amongst other things, the privacy impact of obtaining the business records in the circumstances does not outweigh the importance of the agency performing the function for which the records are sought. The agencies are also required to keep a register (which the responsible Minister and IGIS can inspect) of business records directions given in reliance on a Business Record Approval.

142. NZSIS does not obtain bulk-data en-masse through business records. As set out above information collection is tightly regulated and is only in respect of identifiable individuals. The agencies are unable to directly access or use this business approval process to access the content of telecommunications, the content of cloud storage servers and web browsing history (for which warranted authorisation would be required).

Compliance with New Zealand law and human rights obligations

143. ISA 2017 includes an explicit requirement that the agencies must act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.⁶⁶ This includes a requirement that, before providing intelligence to an overseas recipient, the Minister must be satisfied that the relevant agency will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand.⁶⁷

144. The MPS on *Cooperation with overseas public authorities*⁶⁸ addresses the agencies' cooperation and sharing information (including intelligence) with overseas public authorities. The MPS states NZSIS officers, in making decisions related to foreign cooperation, must have regard to the following principles: legality, human rights obligations, necessity, reasonableness and proportionality, protections for New Zealanders, information management and oversight.

⁶⁶ Section 17(a) ISA 2017

⁶⁷ Section 10(3) ISA 2017

⁶⁸ (Appendix 37) Ministerial Policy Statement Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities ([Link](#))

145. The Minister has designated s6a: details about Minister-approved countries as “approved parties”.⁶⁹ This means that (unless there is a specific indication that human rights breaches may occur, or have occurred) NZSIS can share all forms of intelligence with the government agencies of these countries without further assessment of the risk that doing so will contribute to human rights violations.

146. The MPS requires the agencies to have a human rights policy setting out the factors that must be considered when assessing whether a real risk of human rights breaches may exist in connection with cooperation with overseas public authorities. All employees of the agencies are required to receive training on all the relevant law, policies and procedures in relation to the agencies’ human rights obligations.

147. The agencies’ *Joint Human Rights Policy*⁷⁰ sets out the levels of decision-making for each type of activity that may involve foreign cooperation. The greater the level of risk, the more senior the level of approval required for a particular activity. For example, the Minister must approve the highest level of risk such as where there is a substantial likelihood of torture or similar mistreatment in providing information to an approved party; or in receiving information that may have been obtained from such ill-treatment.

Inspector-General of Intelligence and Security

148. The purpose of the oversight of both agencies is described in ISA 2017 as “...to provide for the independent oversight of intelligence and security agencies to ensure that those agencies act with propriety and operate lawfully and effectively.”⁷¹ To achieve this purpose, ISA 2017 provides the IGIS with functions, duties or powers to ensure that the agencies “conduct their activities lawfully and with propriety”; ensure that complaints relating to the agencies are independently investigated; and advise the New Zealand Government and the Intelligence and Security Committee on matters relating to the oversight of the agencies.⁷²

149. The Inspector-General of Intelligence and Security (IGIS) has extensive oversight powers over the agencies and reports directly to Parliament.

150. All authorisations are subject to post-issue review by the IGIS (meaning the IGIS reviews every warrant issued). This involves NZSIS informing the IGIS a warrant has been issued and providing the opportunity to review the warrant application (including the

s6a: details about Minister-approved countries

(Appendix 38) Joint Policy Statement: JPS-006 Human rights risk management policy ([Link](#))

⁷¹ Section 156(1) ISA 2017

⁷² Section 156(2) ISA 2017

intelligence case in support of the application), before meeting with NZSIS's Legal Team. At these meetings the IGIS will raise any queries, such as in regard to the necessity, proportionality or legality of NZSIS seeking to use the authorised activities to meet particular intelligence requirements. NZSIS will generally seek to address any concerns raised by the IGIS in subsequent applications. However, if NZSIS and the IGIS cannot come to an agreement on the correct legal interpretation of an important matter, NZSIS will seek and apply an authoritative legal opinion from the Solicitor-General. The Review has been advised that there have been significant and ongoing discussions between NZSIS and the IGIS regarding the required content of warrant applications since the new legislation came into force.

Question: How effective is NZSIS's regulatory framework?

151. Given its intrusive powers, NZSIS recognises the importance of effective oversight which is critical for NZSIS to maintain the trust of the New Zealand Government and the public. As a security intelligence service, the NZSIS relies heavily on the support of the wider community in achieving its functions.

152. The new legislation and the accompanying MPSs and various internal policy documents have been a significant change to NZSIS's core business. The implementation of the new legislation, combined with significant growth of staff numbers (there are now a larger number of investigators and case officers with limited experience due to the recent rapid growth), has amounted to a not insignificant increase on the pressure placed on NZSIS's in-house legal team. Legal consultation was, and continues to be, required on the development of new policies to ensure compliance with the new legislation and MPSs etc. and, understandably, the requirement for legal advice has increased as NZSIS needs to apply the law to new fact scenarios and to train new employees. In addition to this, significant legal resource is required to engage with IGIS inquiries about the lawfulness and propriety of NZSIS's compliance with the new regulatory framework. The courts are not developing precedents in regard to the interpretation of this area of law, so disagreements as to the interpretation of the law do occur, such as between NZSIS and the Office of the IGIS; between the GCSB and NZSIS legal teams, and even within NZSIS.

153. While the legislation has acted as a critical enabling tool in some respects (for example, the ability for NZSIS to obtain class warrants) and has resulted in positive developments and improved collaboration between the NZIC agencies, there continue to be significant areas of ambiguity.

154. s6a: describes reasons for ambiguity and the operational impact

s6a: describes reasons for ambiguity and the operational impact



The Review

notes that a key finding of the Cullen-Reddy report was that:⁷³

...lack of clarity in the [previous] legislation means the Agencies and their oversight bodies are at times uncertain about what the law does and does not permit, which makes it difficult to ensure compliance. Critical reviews in the past have led the Agencies, particularly the GCSB, to take a very conservative approach to interpreting their legislation... this overtly cautious approach does mean that the GCSB is not as effective or as efficient as it could be. The [new] legislation needs to set out clearly what the Agencies can do, in what circumstance and subject to what protections for individual.

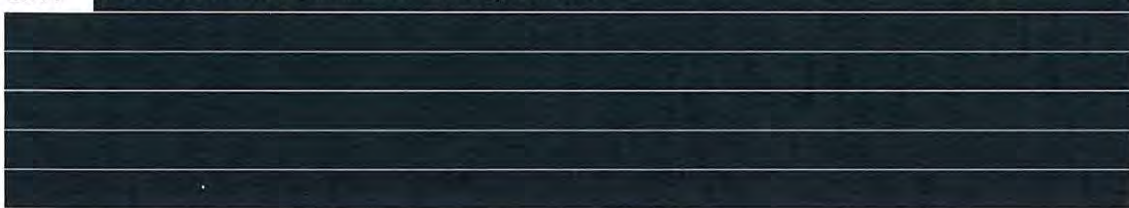
155. Despite the change in legislation, such clarity remains elusive. NZSIS staff need a clear understanding of the limits as to what is authorised under the legislative and compliance regime, and confidence to operate up to those limits set by government.

Question: Are there issues within the current regulatory framework?

156. Unlike law enforcement agencies which are typically (although not exclusively) focused on holding people to account for their past actions, the purpose of a security intelligence service is to pre-emptively identify threats to national security in order for the Government to act to prevent the anticipated harm occurring. As such, NZSIS's investigations are necessarily predictive and pre-emptive, rather than retrospective.

Warrant thresholds

157. s6a: describes thresholds for seeking warrants



⁷³ (Appendix 35) Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand (Cullen-Reddy Report), 29 February 2016 ([Link](#))

s6a: describes thresholds for seeking warrants

158. ISA 2017 requires a warrant application to set out “details of the activity proposed to be carried out”.⁷⁴ This means that more detail is required in the warrant application than was previously provided under the old legislation.

s92(h): describes Crown Law advice regarding ISA 2017

159. The Review team has examined the length of 21 warrants NZSIS have applied for between June 2018 and May 2019.⁷⁶ The average length for the 21 warrant applications was 29 pages, with an average of 12 pages setting out the intelligence case and an average of 31 reference documents attached per application. This amounts to a significant body of work by the Intelligence Directorate, Legal, and the Director-General; and of course an application and folder of intelligence references of this size requires a significant amount of review time for the Minister and the Commissioner. The Review understands that the length of the warrants have grown over time since ISA 2017 came into force, at least partly as a result of NZSIS seeking conform with Crown Law advice and prevent criticism of NZSIS during subsequent review of the warrant application by the IGIS.

160. s6a / s92(ba)(i): describe NZSIS staff view regarding the IGIS and impact on NZSIS activities

. The IGIS helpfully provided a written response confirming she was aware of this view and that her predecessors were hampered in their ability to exercise oversight (due to a lack of resourcing). However, following the ‘reset’ of the intelligence and oversight function following the Dotcom matter in 2012/13, reflected in both additional resources and clear Government and public expectations as to the thoroughness and rigour of oversight, the Office of the IGIS is now better resourced. As at March 2019, the IGIS advised that her Office consisted of an Inspector-General, Deputy Inspector-General, four Investigators (3.6 FTEs), a security/IT Manager and an executive assistant. Accordingly, the IGIS now has sufficient resources to review every intelligence warrant issued and a range of operational activities, as well as

⁷⁴ Section 55 ISA 2017

⁷⁵ Subject to Legal Privilege – Crown Law advice dated 11 September 2018.

⁷⁶ Training warrants were excluded from the assessment

investigate complaints and initiate own-motion inquiries. However, she noted her office do not have sufficient resources to scrutinise every decision and every action of the agencies.

161. The IGIS considers that the agencies have struggled to respond to the more extensive and persistent oversight that has been required of them in the last five years, both in terms of adequately resourcing their response to oversight and in dealing with what close scrutiny requires of them in practice. In the IGIS's view "...complaints within NZSIS that oversight created uncertainty, or imposed ambiguous or unworkable demands, reflected Service staff dislike of oversight, reluctance to change their practice, and/or lack of the wherewithal to make the changes required."⁷⁷

162. The Review notes that in its discussions with NZSIS staff it formed the view that wide and healthy support exists at all levels regarding the need for ongoing oversight of the NZSIS's activities and for the NZSIS and its staff to be accountable.

163. Whatever the reasons, whether justified or not, the view among those engaged in NZSIS's intelligence functions exists and has a material impact on the confidence with which the investigations teams go about their work s6a: describes impact on operational activity

164. There would be significant value in more formally clarifying warrant thresholds with those involved in the authorisation and review process (Minister/Commissioner/IGIS) and their views regarding the material they, the decision makers, need to inform their judgements (something perhaps akin to explanatory memoranda). This would best include the use of case studies to illustrate where the thresholds rightly sit and seek views on the depth of intelligence case needed to meet the legislative test. Such a document would likely assist in setting a common understanding among staff and better ensure they are using the appropriate level of investigatory and operational aggression. This would also be useful for training purposes.

165. The Review notes that in terms of the 'correct length' of a warrant application there is clearly no single template or a 'one size fits all' solution. That said, there should be clear cut cases where the nature of the security concern provides a clear basis for the use of more

⁷⁷ On 20 June 2019, the IGIS received an advance copy of sections referring to her Office within the Review's draft report. On 21 June 2019, the IGIS provided comment on the draft sections and offered suggestions, including the quoted remarks; RE: AROTAKE Report - section relating to OIGIS - my only suggestion is in green (Email), 21 June 2019 12:29pm.

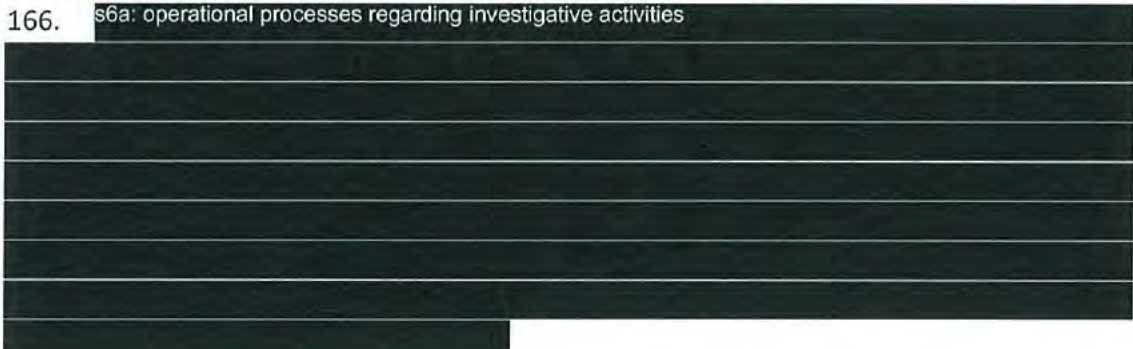
intrusive powers (and, as such, it is expected limited additional information would be required beyond establishing the situation exists), for example:

s6a: describes cases of security concern that would justify the use of more intrusive powers



Investigative thresholds

166. s6a: operational processes regarding investigative activities



167. As will be detailed later in this Review, subsequent investigations have revealed few indicators of ^{the individual}'s plans for the 15 March attacks. The leads which have been identified (post-attack) are weak and likely would have elicited little, if any, investigational activity by NZSIS or its partners. Considering where investigational thresholds rightly sit in future and ensuring staff are aware of the thresholds will be an important step.

MPSs/JPSs

168. NZSIS's MPSs and internal policy documents were produced at short notice and, at times with insufficient understanding of their implications for NZSIS's operational realities. As they were finalised quickly and very shortly before the ISA 2017 came into full force, the operational areas were not fully cognisant of the implications for their day-to-day business. This placed additional stress on those teams. In the Review's opinion, the MPSs in particular will benefit from the mandated review and redrafting scheduled for 2020, in consultation with the particular operational areas affected. By this stage, the Royal Commission's findings will be able to inform the redrafting process.

169. However, two areas which may benefit from earlier revision would be those governing the Human Rights Risk Assessment (HRRRA) framework and NZSIS's access to open-source (publicly available) information.

170. An area which has been the subject of frequent comment in discussions with staff relates to the processes (and associated resource cost) surrounding HRRAs. Prior to seeking or exchanging information on individuals, NZSIS must complete human rights risk assessments for the country, and for each authority in that country, with which they wish to co-operate (if from 'non-approved' countries).

171. While complicated processes associated with HRRAs were repeatedly raised as an issue by staff, the Review believes the current MPS appears reasonable and workable. Perhaps, however, the way it is being used or interpreted is creating significant extra overhead. A possible remedy would be for NZSIS to seek to have the Minister categorise more countries as 'approved parties'. The Review also believes that centralising NZSIS's process for considering the human rights credentials of candidate countries and authorities would be useful, with that area being responsible for ensuring these assessments are kept up-to-date and available to be drawn upon by NZSIS staff as required.

Direct Access, Restricted Information and Access to business records of telecommunications networks and financial service providers

172. Information and data are key enablers of NZSIS's intelligence function. [REDACTED]
s6a: operational processes [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

173. Despite ISA 2017 providing for NZSIS to negotiate direct access agreements for access to certain databases with specified agencies, not all of these are currently in place. In particular, there is no direct access agreement with NZ Police. Direct access to information, particularly police information, is crucial in the context of counter-terrorism due to the importance of being able to act on leads quickly. The Review recommends that direct access negotiations in respect of the outstanding datasets (both held by NZ Police) are moved forward as a priority. The Review notes, however, that Schedule 2 of ISA 2017 (which specifies the data repositories NZSIS may negotiate access to), notes that NZSIS direct access to the NZ Police database may only be for 'financial intelligence information' or 'information about people and locations identified as posing a possible physical threat to GCSB or NZSIS

employees.' There is no broad provision for accessing this information for purposes such as 'to assist NZSIS to fulfill its statutory functions' or for 'counter-intelligence purposes'.

s6a: operational processes

174. The Review also notes that a change to the ISA 2017 is required to add further datasets to the Schedule. Scheduling amendments to existing legislation, particularly in busy legislative agendas, is frequently difficult and often subject to extended delays. In the Review's mind this is unnecessarily restrictive and limits NZSIS's ability to respond quickly. Accordingly the Review recommends that NZSIS include in its legislative change agenda a mechanism to add/remove datasets from Schedule Two of the ISA 2017 by a process which does not include the requirement for legislative change and to allow for expanded use of those datasets subject to appropriate oversight and review.

Recommendations - It is recommended NZSIS:

1. Test NZSIS's view of warrant thresholds with the Minister, Commissioner of Intelligence Warrants and the IGIS, particularly the circumstances in which more intrusive powers are warranted and the level of detail they require to inform their judgements and decisions;
2. Test NZSIS view on investigative thresholds with the Minister in light of the changes in the security environment which make it increasingly difficult to identify signals of emerging security concern;
3. Continue to work within the current MPS framework, but with some changes to HRRRA policy processes, with a view to pursuing the required amendments during their scheduled review in 2020; and
4. Advancing direct access negotiations as a priority in respect of the outstanding datasets identified in Schedule 2 of ISA 2017.
5. Seek legislative amendment to the current mechanism for adding/removing datasets from Schedule 2 of ISA 2017 with an Act of Parliament, subject to appropriate oversight and review.

Question: Did these issues substantively impact NZSIS's ability to identify ^{the individual}?

175. While the Review has identified several areas in NZSIS's regulatory framework that could benefit from review, it is considered that these issues did not substantially impact on NZSIS's ability to identify ^{the individual}. As was ascertained from the mock investigation exercise (detailed later) exploring what investigative steps would have been taken had NZSIS received any (or all) of the leads that post-attack investigations identified, it is unlikely (even with all of the leads combined) that the threshold would have been met for a warrant. Current indications are that the only likely way that NZSIS would have possibly identified ^{the individual}'s intentions (and thus seek to disrupt his plans or share the intelligence with NZ Police), were if authorisation was granted to search and seize material from his private computer where he was drafting his manifesto.

Part 2.4. NZSIS Partnership Arrangements

176. Throughout most of their history, Western security and intelligence services have operated as largely self-contained entities with limited connections to wider government. At times, their closest natural partners were their counterpart services in other countries, especially among the FIVE EYES. This is no longer the case. Internationally, national security issues are part of mainstream business for many government departments and businesses. This trend was perhaps first driven by terrorism concerns following the 11 September 2001 attacks in the United States, exacerbated by the significant growth in cyber attacks by state actors, and most recently by acts of foreign interference by foreign governments in national political processes. In many countries national security is now a government-wide priority, and security and intelligence services cannot be effective if isolated from the rest of government, business and the wider public.

177. Under NZSIS's organisational renewal strategies, greater transparency, integration and cooperation have been strong themes. NZSIS's most recent Annual Report stressed the importance of maintaining a "powerful profile":

The NZSIS's domestic and international partnerships help to manage complex threats and deliver the intelligence and security objectives set by Government. Maintaining a powerful domestic and international profile will help ensure:

- *Customers value the NZSIS's advice and expertise.*
- *The public are aware of the work of the NZSIS and the value we add.*
- *International partners recognise the value the NZSIS adds to international security.*
- *The NZIC's collaborative approach is seen as an exemplar in Government.*
- *The NZSIS is seen as responsive to media requests.*
- *The NZSIS is seen as a desirable place to work, attracting skilled and talented staff⁷⁸*

Question: How does NZSIS engage with its partners?

International Liaison

178. NZSIS is a net beneficiary and a longstanding member of the FIVE EYES group of security and intelligence agencies, but it has growing relationships with partner organisations around the world, s6a: information about international partners. Via NZSIS, international partners provide the Government with insights on

⁷⁸ (Appendix 39) Classified NZSIS Annual Report 2018 ([Link](#))

global trends and developments which increasingly stand to impact New Zealand and New Zealanders. The global nature of modern national security threats and New Zealand's unprecedented connectedness to the world will almost invariably see global trends become domestic issues. s6a & 6b(i): describes international partner reporting

179. NZSIS's international counterparts also provide access to unique and sophisticated capabilities and technologies ordinarily well beyond NZSIS's means, offering the Government both significant capabilities and savings. New Zealand contributes to global security on a niche basis, contributing to a common picture of global trends, from NZSIS's unique perspective.

Domestic Partnerships

180. NZSIS's domestic partners also benefit from a range of international partnerships, each with their own areas of expertise and value to New Zealand. However, these relationships cannot replicate the unique intelligence sharing arrangements NZSIS has with its international partners. As such, NZSIS has a valuable role in connecting domestic partners with the international intelligence community.

181. Following the 11 September 2001 attacks, the global threat of terrorism required a significant change in NZSIS's approach and a greater engagement with other government departments, especially NZ Police, Immigration and Customs. Despite this, these relationships remained largely transactional and, therefore, fragile. The perceived diminishing of the threat from Al-Qaeda and its affiliates from around 2009 to 2013 saw a lull in NZSIS's relationship with NZ Police until the rise of ISIS in 2013. Resurgence in counter-terrorism cooperation required NZSIS to cooperate in unprecedented ways with law enforcement, and this new more open engagement continued with growing national concern about foreign state interference in New Zealand's democratic system.

182. An important element to NZSIS's increasingly collaborative approach to national security issues has been the concept of a joint DPMC-GCSB-NZSIS core New Zealand intelligence community. The 2014 PIF considered the performance of the community as a whole and the responding SCRR initiative was a joint effort by the three organisations to align their functions, capabilities and objectives. This was further reinforced by the Cullen-Reddy review and the subsequent community-wide ISA 2017. The National Security Group

s6a & s6b(i): references international partner reporting

of DPMC has made a significant effort to grow cooperation and partnership within both the core NZIC and the wider intelligence community. This is a positive development, but not one without issues.

Question: Does NZSIS effectively use its partnerships?

183. The Review found that in recent years there has been significant improvement in cross-agency cooperation across a range of NZSIS activities, including information sharing, including details of investigations and leads, as well as in joint exercises. There is an improved (if still patchy) understanding within NZSIS and NZ Police of each other's roles in national security and relationships at all levels appears to be productive. While NZSIS is advancing beyond merely transactional relationships, it is yet to break out of a traditional model of partnership, in which agencies operate in parallel rather than a truly joint fashion. A number of factors, detailed below, contribute to limiting NZSIS (and NZ Police and other enforcement agencies) gaining maximum benefit from their relationships.

184. A notable gap in NZSIS's repertoire of partnership arrangements lies in its limited engagement with wider government, the business community and the general population, particularly with respect to sharing NZSIS's national security concerns and requirements in a manner which gains traction with those sectors. Relationships such as these are becoming increasingly important to modern security services. They act not only as enablers to inform government, business and the community regarding the national security issues important to them, but they also enable and empower each to recognise and report on matters of potential security relevance.

185. NZSIS would significantly improve its ability to fulfil its national security mandate through developing closer relationships with these groups. This should range from the potential for significantly enhanced lead generation, to better protection of New Zealand business interests and intellectual property, to more informed development of policy across government.

Question: What issues arise in NZSIS's partnerships?

186. NZSIS's partnerships, particularly with NZ Police on counter-terrorism matters, are increasingly positive and productive. However, the present state of cooperation between the NZSIS and the NZ Police falls short of the true partnership, ^{s6a: describes international cooperation}

. The Review considers that the partnership is constrained by three factors:

- Cultural hurdles: NZSIS's inter-agency relations are largely based on productive personal relationships, which would benefit from greater formalisation to ensure

their resilience and longevity. s6a: describes cultural hurdles in NZSIS/NZP partnership

[REDACTED]

s6a: describes cultural hurdles in NZSIS/NZP partnership

[REDACTED]

s6a: describes cultural hurdles in NZSIS/NZP partnership

[REDACTED]

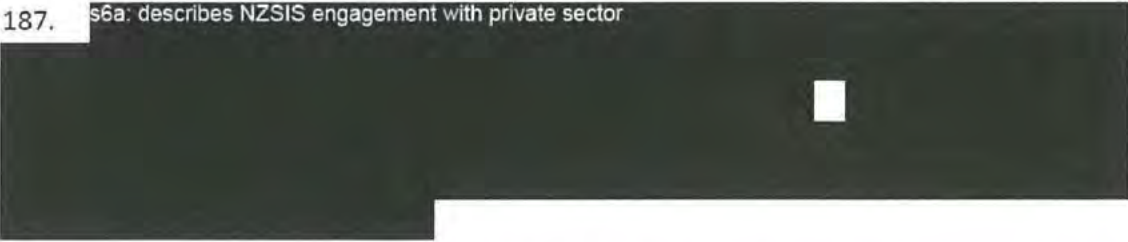
- Technical barriers: s6a: describes technical barriers

[REDACTED]

- Legal constraints: The Review recognises there are legal constraints placed on the sharing of information between government agencies for compliance with privacy

laws and investigative proportionality. Despite this, the Review notes the authority given to the intelligence and security agencies for seeking direct access agreements to specified databases.⁸⁰ As noted earlier, not all permissible accesses have been negotiated, notably with NZ Police for access for health and safety purposes (namely “information about people and locations identified as posing a possible threat to [NZSIS] employees”) and financial intelligence holdings.

187. s6a: describes NZSIS engagement with private sector



188. Similarly the New Zealand public would benefit from greater awareness of NZSIS's work and requirement for public support to achieve its mission. The Review notes that NZSIS, particularly Director-General Kitteridge, has assured the public about the lawfulness of NZSIS's operations and the importance of its work for the nation's security. With this as a foundation, it may be possible for commentary to move towards a new narrative in which the community is made more aware of national security issues. For any such change to be successful it would require the direct support and involvement of Government. This will be covered in more detail later in the report.

Recommendations - It is recommended NZSIS:

1. Ensure partners in the 'wider' New Zealand national security community have a clear understanding of NZSIS's role and requirements;
2. Ensure that, while continuing to encourage the development of personal relationships with partner agencies, this is appropriately balanced with more formal and institutional cooperation frameworks;
3. Produce and disseminate intelligence reporting and NZSIS's information requirements at the lowest feasible classification (particularly in respect of counter-terrorism);
4. Produce unclassified material on likely indicators of security relevant

⁸⁰ Schedule 2, ISA 2017

activity, wherever possible, to those who have significant dealings with the community;

5. s6a: recommendation related to classified systems
[REDACTED]
6. Build feedback loops where other parts of government provide information to NZSIS in order to shape what they provide and encourage further involvement.
7. Consider developing security briefings to allow staff greater confidence in sharing information and requirements in order to have greatest impact on cooperation while preserving security.

Question: Did partnership issues substantively impede NZSIS's discovery of the individual

189. The Review considers it unlikely that any of the matters identified above impeded NZSIS's ability to identify the individual in advance of his attacks on 15 March 2019. However, there is a remote possibility – albeit one that cannot be completely discounted - that greater engagement could have generated information resulting in the identification of leads relating to the individual. Should such a lead have been identified, it is considered unlikely that it would have reached the threshold for a more intrusive investigation. Post-attack investigations of the individual activities reveal that the individual tradecraft, especially online, was such that he left little to be discovered during the period in which he planned the 15 March attacks.

Part 2.5. NZSIS Investigative and Operational Frameworks

Question: What Frameworks does NZSIS Use?

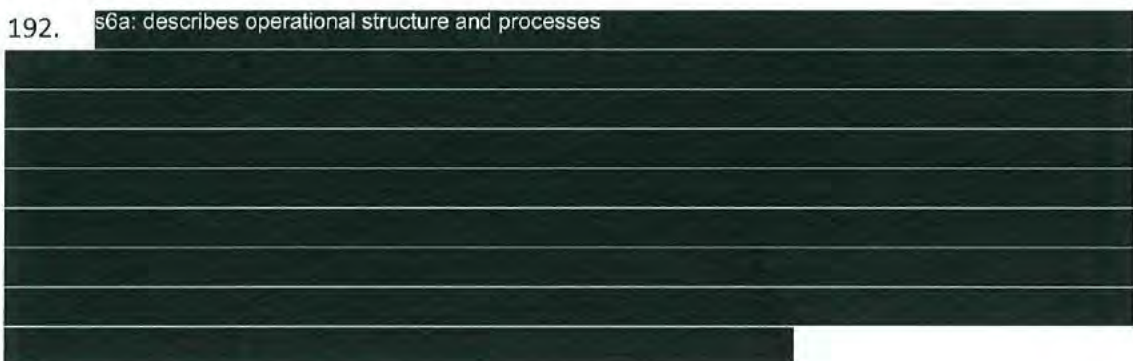
190. NZSIS has long-standing practices with respect to the investigation of threats and the collection of information in order to meet its statutory functions.⁸¹ In recent years NZSIS has sought to increasingly formalise these practices and better define its processes to ensure their effectiveness, efficiency and compliance with New Zealand law.

Process Reform

191. s6a: describes operational structure and processes



192. s6a: describes operational structure and processes



Investigative Model

193. AGUERO and s6a: project name embedded NZSIS's dedicated strategic analysis capability and the Collection Hub, which allowed investigative teams to "move up the value chain" to focus on their efforts on assessing whether individuals or groups are of genuine national security concern, rather than considering strategic trends or coordinating tactical activities.⁸³ While these changes improved the efficiency of the model, altered some role responsibilities and encouraged greater oversight, the fundamental characteristics of NZSIS's classical investigative model remained. The term 'classical' in this sense is not intended to be pejorative. NZSIS's closest international partners and foreign police forces use very similar

⁸¹ (Appendix 8) section 10, ISA 2017.

⁸² (Appendix 41) s6a Review: Proposal for Change, 31 May 2017 ([Link](#))

⁸³ (Appendix 18) Project AGUERO: Review of the New Zealand Intelligence Community's Security Intelligence Operating Model, September 2015 ([Link](#))

models, but are increasingly recognising the model's limitations in rapidly evolving security intelligence environments. Security services need to be cautious not to over-invest investigation and collection capabilities in areas of known security concern, although this is a difficult equation given the demand for resources generated by known security threats and the risks of under-resourcing NZSIS's response to those threats.

194. A classical investigative model well-suited to STERLING Goals 1 and 2 (mitigation of espionage and foreign interference and mitigation of terrorist threats) is geared towards responding to 'knowns'; processing information through a typically linear workflow until the lead is either discounted as a threat or resolved through government or other's intervention. The classical model begins with lead information. This information can arise from a variety of domestic and foreign sources, but will often come from outside NZSIS. The classical investigative model is not well configured for discovery of its own leads and, where it does, these tend to be within the same thematic area (i.e. investigations of Sunni Islamist extremism are more likely to generate leads on other Islamist extremists). Despite its limitations, the classical model does provide a point of focus which allows staff to build a formidable depth of subject matter expertise.

195. In the event information does enter NZSIS's workflow, the information begins as a lead ('known unknowns'). These leads are processed through established business rules and foundational enquires are conducted to validate the lead information. [REDACTED]

s6a: describes process for investigating lead information

[REDACTED]

196. Once a lead has been validated as a probable threat to national security, it will be progressed through a formal commencement of investigation process. If approved, the investigator will identify intelligence gaps and produce a list of specific information requirements. The investigation will also be assessed for its priority [REDACTED]

s6a: operational process

s6a: describes operational processes



197. In order for lead information to be shared with NZSIS, the holder of the information must recognise its significance to national security, be aware of NZSIS's mandate, be willing to share the information and know how to communicate it. In New Zealand's security environment prior to the events of 15 March 2019, the potential for relevant information to never make it to the start-gates of NZSIS's classical model was significant. As will be addressed elsewhere in this report, such a model is inherently dependent on the quality of its partnerships, not only with national security agencies but with wider government, business and the public.

Discovery and Baseline Projects

198. In accordance with its pre-emptive role in national security, NZSIS considers one of its most important 'value-adds' to be in the identification of hitherto unknown threats (as opposed to leads). This objective is encapsulated in STERLING Goal 3 (emerging terrorism threats), which stresses the importance for NZSIS to:⁸⁴

...understand what is the norm within the NZ threat environment and thereby embed an ability to identify changes to the norm that may signify emerging security issues (Priority 3), which in turn enable efforts to combat violent extremism (Priority 2). By understanding emerging terrorism threats it enables us to be better positioned to mitigate serious domestic terrorism threats.

199. Accordingly, as resources have allowed, NZSIS has prioritised the development of discovery and baseline understandings of a range of counter-terrorism threats, beyond a focus on those already known to exist. In mid-2018 the counter-terrorism team took the

⁸⁴ (Appendix 42) Project STERLING Strategic Goal Implementation Plan, March 2018 ([Link](#))

deliberate decision to diversify its focus to proactively identify and understand emerging threats. As highlighted, this initiative was facilitated by the introduction of additional investigative staff ~~s6a: operational details~~

~~[REDACTED]~~

200. ~~s6a: describes focus of investigative resources~~

~~[REDACTED]~~

~~s6a: table outlining allocation of investigation efforts~~

~~[REDACTED]~~

201. In July 2018, the counter-terrorism unit produced a basic but sufficient Discovery Strategy, which stressed the need for discovery efforts:⁸⁵

CT Unit continue to assess there are individuals in New Zealand for whom the extent of their radicalisation and mobilisation to violence may not be fully known. There is also a realistic possibility an unknown lone actor could move

⁸⁵ (Appendix 43) Counter Terrorism Unit Discovery Strategy, 16 July 2018 ([Link](#))

from radicalisation to action, without intelligence forewarning, potentially in a short timeframe.

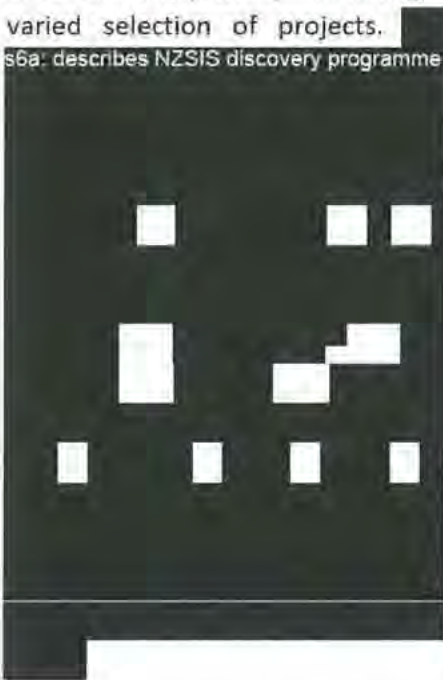
202. The strategy provided the unit with a framework for proposing, authorising and recording discovery projects, with distinct priorities (such as residual risk) allocated to each of the counter-terrorism teams.

NZSIS Discovery Projects - Overview

This team-level approach saw the unit progressively refine the focus of its discovery work,⁸⁶ initiating a varied selection of projects.

s6a: table of NZSIS Discovery Projects

s6a: describes NZSIS discovery programme



203. The Discovery Strategy also outlined a unit-wide baselining effort, involving:⁸⁸

...analysis to establish a baseline picture of emerging terrorism threats to New Zealand... with the objective of understanding the New Zealand baseline picture based on our current holdings, the development of information requirements and outreach opportunities.

⁸⁶ (Appendix 44) Discovery Questions, June 2018 ([Link](#))

⁸⁷ (Appendix 45) Discovery (PowerPoint), September 2018 ([Link](#))

⁸⁸ (Appendix 43) Counter Terrorism Unit Discovery Strategy, 16 July 2018 ([Link](#))

204. The baselining programme also drove the unit's reinvigoration of threat-agnostic counter-terrorism information requirements ^{s6a: operational details}

[REDACTED]

205. In this respect, the Review notes that NZSIS's Investigations Group is well-advanced in a process of refreshing its investigations framework and staffing ^{s6a: project name},⁹⁰ following a review of the existing model ^{s6a: project name}⁹¹. During this period NZSIS's Investigations Policy was suspended and replaced with Interim Guidance on the conduct of investigations.⁹² This guidance has ensured that investigative practices continue to follow due process and respect for relevant legislation and policy, notably Ministerial Policy Statements, and guidance relating to necessity, proportionality, oversight and risk. While the policy is an important foundational document, the Review notes that its recommendations in this report, if accepted, may require further amendment to the draft policy framework. Similarly, the Royal Commission's findings and recommendations may also require adaptation of NZSIS's investigative and operational frameworks.

Question: Are these systems effective in pursuing national security investigations?

206. The Review considers the investigative and operational frameworks used by NZSIS in its 'classical model' to be broadly effective, particularly with respect to known individuals or groups of security concern ('known knows'). ^{s6a: describes operational activity}

[REDACTED]

In the context of NZSIS's terrorism environment and priorities, it was reasonable for NZSIS to expend the resources it did on the mitigation of known threats. A focus on managing the most urgent threats, although likely at the expense of building a more broad-based understanding of the terrorism threat environment, is not unreasonable for a security intelligence service with limited resources. Such a focus was

⁸⁹ ^{s6a} [REDACTED]

⁹⁰ ^{s6a} [REDACTED]

⁹¹ ^{s6a} [REDACTED]

[REDACTED]

⁹² (Appendix 48) NZSIS Investigations interim guidance, 13 June 2018 ([Link](#))

⁹³ (Appendix 49) New Zealand Terrorism Update: June-August 2018, 5 September 2018 ([Link](#)); ^{s6a}

[REDACTED]

consistent with the on-the-ground realities and prevailing strategic assessments which stressed threats from Islamist extremism (although not being unsighted on emerging threats from non-Islamist extremism).

207. As highlighted above, NZSIS's resourcing priorities and decisions were reasonable, but nonetheless left the organisation with limited capacity to effectively fulfil its diverse intelligence responsibilities. The Review notes that NZSIS's Intelligence Directorate was aware of these limitations and responded by broadening its focus, including to right-wing extremism, as soon as additional resources and the immediacy of Islamic State-related threats permitted. By late 2018, NZSIS's strategic terrorism assessment reported that the "overall appeal of Sunni Islamist terrorist groups appears to be waning".⁹⁴ Moreover, the report noted that:⁹⁵

Non-Islamist terrorist threats from extreme political, religious and issues-motivated groups are plausible in New Zealand, especially given heightened political partisanship internationally and the spread of disinformation online. Various radical groups are present in New Zealand, some of which have extreme elements that could plausibly turn violent; however, terrorist acts by them are currently not expected.

208. Despite the absence of enduring information requirements or comprehensive strategic assessment regarding non-Islamist extremism, which might have otherwise directed NZSIS's efforts against emerging terrorist threat, NZSIS's counter-terrorism unit deliberately diversified its focus in early 2018. This renewed baseline and discovery work furthered NZSIS's STERLING Goal 3 objectives and was an appropriate use of its new resources, although this work will take time to bear fruit.

209. While NZSIS's 'classical model' did not prevent the counter-terrorism unit's baselining and discovery efforts, these efforts highlighted some of the model's inherent limitations. NZSIS's implementation plan for STERLING Goal 3 identified the need to adapt and develop capabilities to effectively know and understand the New Zealand terrorism threat environment, especially:⁹⁶

Establish indicators and tripwires: Identify the means by which we will detect emerging threats; develop methodical real-world and online environmental

⁹⁴ (Appendix 50) New Zealand Terrorism Update: September-November 2018, 4 December 2018 ([Link](#))

⁹⁵ (Appendix 50) New Zealand Terrorism Update: September-November 2018, 4 December 2018 ([Link](#))

⁹⁶ (Appendix 42) Project STERLING Strategic Goal Implementation Plan, March 2018 ([Link](#))


scanning processes; develop requirements; engage with relevant communities; engage the NZ public; collect the right information; identify intent and capability; understand, recognise and react decisively to indicators.

210. While the orientation of NZSIS's investigative and operational frameworks towards responding to and mitigating known threats is reasonable, NZSIS needs to continue its efforts to achieve the objectives of STERLING Goal 3, so as to provide the Government a higher level of assurance that it will detect and mitigate future terrorist threats.

Question: What was NZSIS doing regarding Right-wing extremism?

211. In May 2018, NZSIS initiated a baseline review of extreme right-wing ideology and adherents in New Zealand. While there were some initial changes in staffing, the project was led by the same officer from mid-2018.

212. s6a: operational details



s6a: operational details; including overview of current intelligence picture on extreme right-wing groups



~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a: operational details about right-wing extremism investigation efforts




~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a: operational details about right-wing extremism investigation efforts



~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

Released by the Director-General of Security

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a: operational details about right-wing extremism investigation efforts



~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

s6a & s6b(i): operational details about right-wing extremism investigation efforts

217. s6a: operational details about right-wing extremism investigation efforts

An extreme right-wing inspired attack on a mosque was one of the two scenarios discussed during a detailed counter-terrorism response tabletop exercise between NZ Police and NZSIS in October 2018.¹¹⁸ This exercise was designed to increase inter-agency understanding of their respective processes and capabilities in response to terrorist attack scenarios, and identify gaps hindering collaboration.¹¹⁹

218. The exercise's right-wing extremist attack scenario has a significant resemblance to the 15 March attacks on worshippers at the Al Nur mosque in Christchurch:

Scenario 2: Christchurch

- A van has veered off the road and onto a foot path hitting a number of pedestrians leaving the An Nur [Al Noor] Mosque after evening prayers. Emergency services are attending;
- Initial (police and media) reporting indicates approximately 10 people have been injured; three fatally;
- Witness reports indicate the driver, a man aged in his twenties with a shaved head, escaped seemingly uninjured and ran from the scene across Hagley Park.

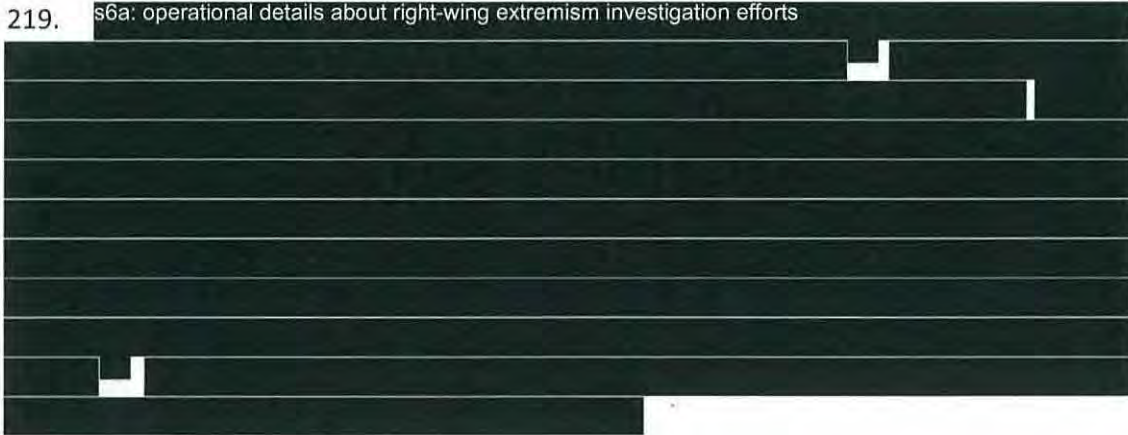
s6a: classified reference

¹¹⁸ (Appendix 57) XRW Exercise ([Link](#))

¹¹⁹ (Appendix 58) CT Table Top Exercise (Notes), 3 January 2019 ([Link](#)); also see: CT Tabletop Exercise Oct 2018 (PowerPoint) ([Link](#))

It is noted that the choice of this scenario was not driven by any intelligence reporting but rather reflected open-mindedness towards the possibility of an attack targeting New Zealand's Muslim community.

219. s6a: operational details about right-wing extremism investigation efforts



220. NZSIS's baselining efforts also generated or investigated a number of leads relevant to right-wing extremism, s6a: details about leads relevant to right-wing extremism

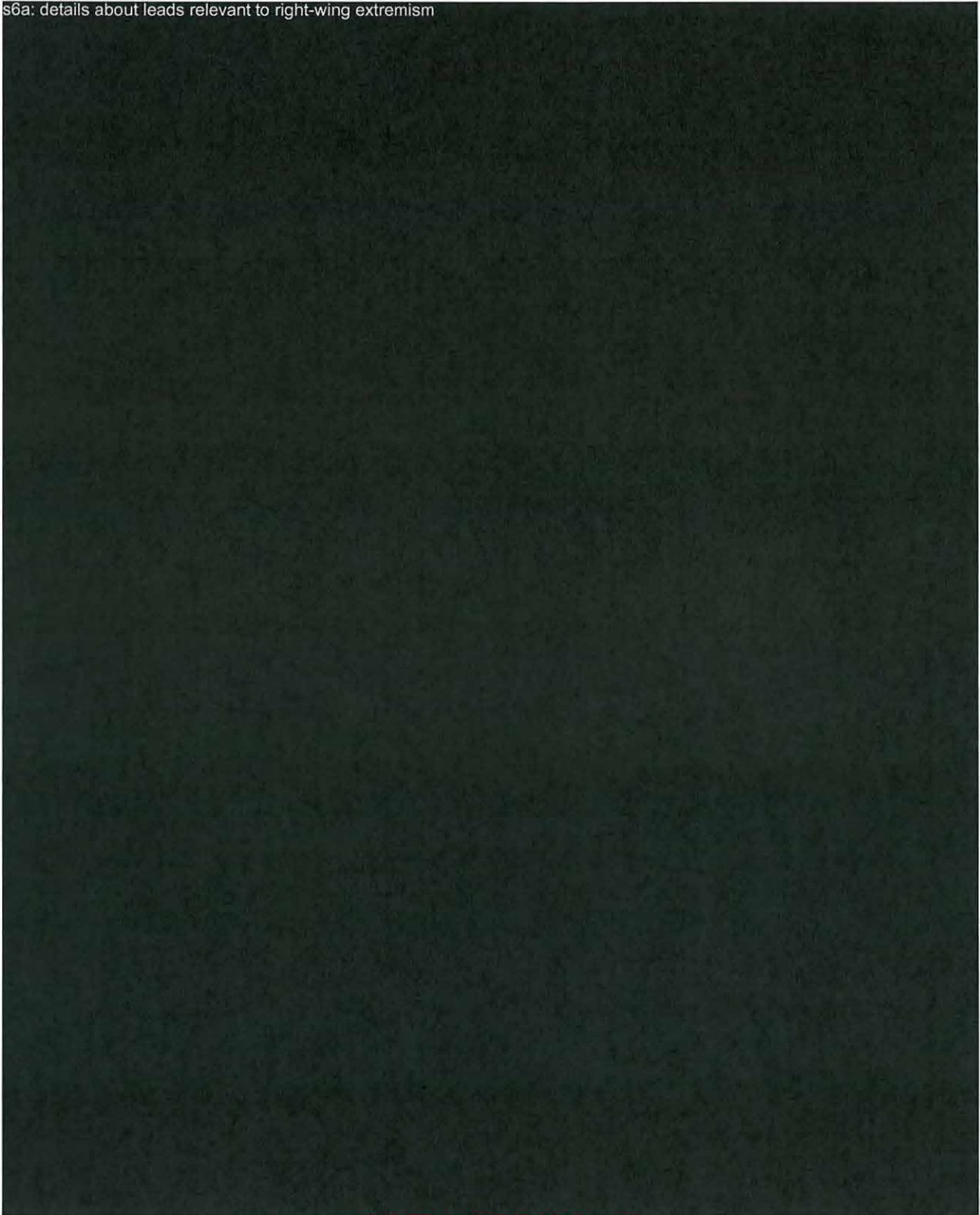


Released by the Director-General of Security

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a: details about leads relevant to right-wing extremism



~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

s6a: details about leads relevant to right-wing extremism

222. NZSIS's work on the extreme right-wing in New Zealand remained in its early stages at the time of the 15 March 2019 attacks. s6a: describes the focus of NZSIS's work on extreme right-wing in New Zealand

However, investigations after the attacks revealed that the individual's direct connection to the New Zealand extreme right-wing community, which was understandably the focus of NZSIS's baseline review, was negligible, if not non-existent.

Question: Are there issues within current systems?

223. As detailed in previous sections, while the Review considers NZSIS's investigative and operational frameworks to be reasonable within its current priorities and operating circumstances, NZSIS needs to continue to be cognisant of the limitations of this 'classical model', particularly when it comes to lead generation. The Review considers there are aspects of NZSIS's existing frameworks which may benefit from further consideration.

- Limitations in the acquisition and generation of lead information: s6a: describes operational processes

s6a: classified reporting

- The lack of ready access to external information and data: s6a: describes operational processes
[Redacted]

- Thresholds for investigations: s6a: describes operational processes
[Redacted]

- Thresholds for warrants: s6a: describes operational processes
[Redacted]

Recommendations - It is recommended NZSIS:

1. Afford, where possible, increased priority and resources to the generation and management of lead information to support the identification of emerging threats.
2. Delay work on the investigative policy update until the conclusion of the Royal Commission.

Question: Did these issues substantively impact NZSIS's ability to identify ~~the individual~~

224. It is considered very unlikely that the earlier development of NZSIS's discovery and baseline programmes areas would have had a tangible impact on its ability to identify ~~the individual~~. Despite this positive development in NZSIS's effort to scan the horizon for new threats, NZSIS could only devote modest resources to its understanding of right-wing extremism ~~s6a: operational processes~~

225. ~~the individual~~ was a lone actor with no identified nexus with the New Zealand right-wing extremist community. NZSIS's fledgling baseline review and its existing leads generation mechanisms did not acquire information on ~~the individual~~ and, as such, he was never the subject of initial lead enquiries or detailed investigation. Accordingly, the question whether ~~the individual~~ should have been investigated is moot – there was no trigger for such an investigation. Were lead information on ~~the individual~~ acquired prior to the attacks, the question of whether ~~the individual~~ should have been investigated depends upon the nature of the lead information.

226. ~~s6a: operational details~~

227. This gives rise to a separate question, outside the consideration of right-wing extremism investigations, as to whether the signals of ~~the individual~~ activities which did exist prior to the attacks (although unknown to NZSIS at the time but discovered through post-attack investigations) could have led to an investigation of his activities.

Part 2.6. Mock Investigation Exercise

228. The Review attempted to test NZSIS's investigative and warrant thresholds through a mock investigation based on information not known to NZSIS prior to the 15 March attacks, but which was revealed in the post-attack investigation of the individual.

Notional Lead Information

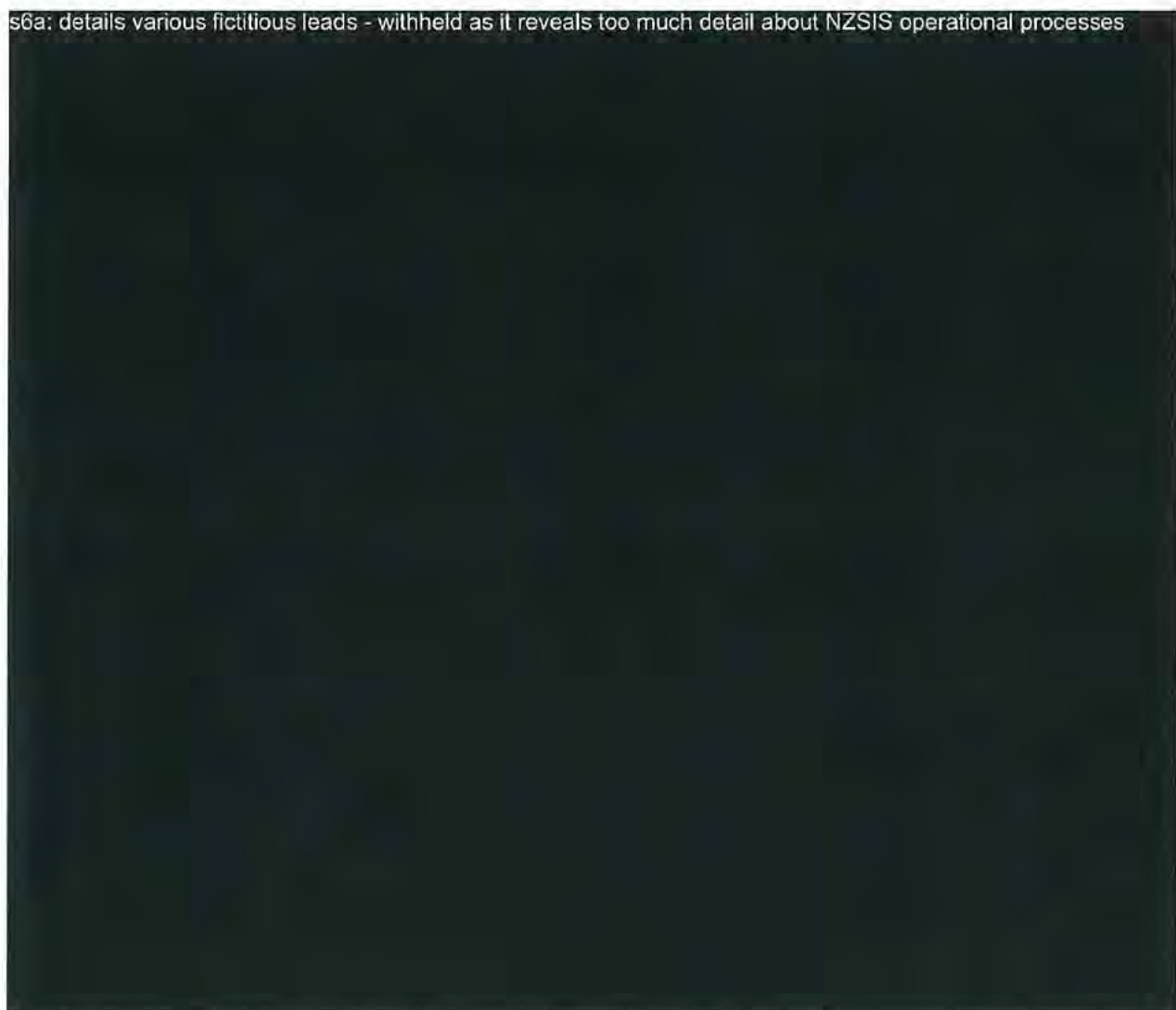
229. The Review team, in consultation with NZSIS's counter-terrorism unit, compiled a selection of 'fictitious leads' based on factual information which could have plausibly been shared with or discovered by NZSIS. It is important to note that these 'leads' were considered to represent the primary indicators of security relevant activity by the individual in the lead up to the attack (short of what was included in his 'manifesto'). Further it was noted this information could have only been generated by very high levels of intrusion into privacy, unprecedented levels of investigative resourcing across the New Zealand Government and high levels of international cooperation.

230. The 'fictitious leads' were:

s6a: details various fictitious leads - withheld as it reveals too much detail about NZSIS operational processes



s6a: details various fictitious leads - withheld as it reveals too much detail about NZSIS operational processes



231. For the purposes of the mock investigation, the Review considered that the most likely (if not only) way NZSIS could have discovered ^{the individual} [redacted]'s plans to conduct his terrorist attacks would have been via his manifesto (*The Great Replacement*). From what is now known of ^{the individual} [redacted]'s drafting of the manifesto, NZSIS would have had to gain a warrant [redacted] s6a: describes operational activity [redacted] in order for NZSIS to acquire a copy of the document sufficiently in advance of the attacks for action to be taken against him. The Review considered it implausible for NZSIS to have reacted, in cooperation with NZ Police, in response to ^{the individual} [redacted]'s deliberate dissemination of his manifesto or his 8chan 'farewell' posting online in the period immediately before his attacks.

Conduct of the Exercise

232. The mock investigation was structured in three sessions:¹²⁶

- a. When considering the individual leads in isolation what would NZSIS have done in response?
- b. When considering the lead information in their totality could NZSIS have gained a warrant s6a: describes operational activity [redacted] before 15 March 2019?
- c. s6a: describes operational activity [redacted]

233. s6a: describes the make-up of the exercise team [redacted]

Session 1: Consideration of Individual Leads

234. The participants considered each individual lead on its merits and in the context of the time in which it would have been received to determine what NZSIS *should* have done in response. s6a: detail about NZSIS operational processes [redacted]

235. Upon review, and following detailed discussions of NZSIS's processes and priorities, none of the leads were strong enough to move directly to the opening of a formal investigation. s6a: details about processing of lead information [redacted]

[redacted] The group was uniform in its view that none of the leads, individually, would justify the use of intrusive warranted

¹²⁶ (Appendix 64) AROTAKE: Mock Investigation Exercise ([Link](#))

powers, nor the provision of substantial intelligence collection assets. The Review concurs with this view.

236. s6a: details operational steps for verifying lead information



Session 2: Considering the Leads in Totality

s6a: describes the variety of leads, and how they would be considered by investigators if received in totality



s6a: continued

239. When considering these s6a pieces of lead information together, the participants resolved that at most they would justify the commencement of an investigation, but the case still fell well short of generating the intelligence case necessary (necessity and proportionality elements) required for a warrant application. The participants judged that the information still lacked a clear nexus to New Zealand's national security, meaning that its priority s6a would be low, as too its likely priority for targeted collection resources.

Session 3: Changing NZSIS's Investigative and Operational Settings

240. With respect to what NZSIS *could* have done, the participants identified two areas in which NZSIS's ability to identify the individual, or similar lone actors, from weak lead information might have been increased:

- Data-matching: s6a: details how data-matching would work
[Redacted]
- Efficient access to data: s6a: describes current processes and efficiency improvements for accessing data
[Redacted]
- Warrant thresholds: s6a: describes current threshold for obtaining a warrant
[Redacted]

Released by the Director-General of Security

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a: continued



~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

Part 3. What *could* NZSIS have known about the individual?

242. This part of the Review looks to identify potential changes to high level processes and settings which may enable NZSIS (and the wider national security community) to identify threats, the likes of the individual, into the future. Several recommendations relate to initiatives which are of a scale or complexity (including consideration of legislative amendment) which are beyond the ability of NZSIS acting alone to change.

243. At this stage, and given the timeframes available, these issues have not been worked through or developed. All will require a great deal more work and design before they could go forward. In any case an important part of further considering and socialising any changes are the co-design processes needed to further develop such initiatives.

244. The initiatives included in this section have been informed by conversations with staff members; representatives of NZSIS' national partners and NZSIS documentation. [REDACTED]

s6b(i); describes another source of information for the review

[REDACTED]

[REDACTED]

245. It is again noted that the focus of this Review has been into the counter-terrorism related elements of NZSIS's operation and not those relating to state intelligence and foreign intelligence investigations. While I believe the recommendations and views in this section will have wider application, particularly in the state intelligence space, this has not been subject of direct investigation.

246. Finally, no matter how many of the Review's recommendations are acted on they cannot, sadly, provide a guarantee that attacks like that of 15 March will not occur. What such changes can do, however, is provide an increased level of assurance to the Government and community that such terrorist activity is more likely to be identified and disrupted. As noted earlier in this report, it is understood that any changes in settings which impact on individual privacy must be in accordance with the social contract which exists between the Government and the people of New Zealand.

Consideration 1: Building National Security Understanding across Government, Business and the Community

247. Throughout most of their history, Western security and intelligence services have operated as largely self-contained entities with limited connections to wider government. At times, their closest natural partners have been their counterpart services in other countries,

especially among the FIVE EYES. National security matters were not part of mainstream government business but rather regarded as anomalous and managed quietly through special arrangements and channels. This is no longer the case. Internationally, national security is part of mainstream business for many Governments, their departments of state and businesses. This trend was perhaps first driven by terrorism concerns following the 11 September 2001 attacks in the United States, exacerbated by the significant growth in cyber attacks by state actors, and most recently by the rise of Islamic State inspired terrorism and acts of foreign interference in national political processes by foreign governments. In many Western nations national security is now a government-wide priority, and security and intelligence services cannot be effective unless they are closely connected with government, business and the wider public.

248. While security and intelligence services (and their governments) have had to adapt to this new reality the rate of adaptation has not been uniform – and in some countries, where national security issues have been less evident or compelling, change has been slower.

249. s6a: describes international context



250. Following the attack in Christchurch and concerns regarding Islamist terrorism, foreign interference and cyber attacks in New Zealand, it may now be time for national security issues to be more transparently a part of the public debate in New Zealand.

What is Proposed?

251. The Review suggests NZSIS determine the Government's appetite regarding greater transparency to the public in respect of national security issues. [Redacted]

Released by the Director-General of Security

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

s6a / s6b(i): describes initiatives by international partners



~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

s6a / s6b(i): continued

Why is it Important?

252. For NZSIS to continue to be more effective it will need to increasingly expand understanding and support for its role across government, business and the community. A failure to do so will likely leave it relatively isolated and operating in the space security services have historically filled. National security is now a whole of government issue, and such engagement would also acknowledge the important role business and the public can perform in leads generation.

253. Further, as an organisation with increased, but still relatively limited resources, NZSIS must leverage the resources and reach of others in New Zealand to assist it perform its role. This includes those in Government, business and the community. A key enabler in NZSIS generating this support will be a greater understanding and appreciation of its role.

What Would Need to Occur?

254. In the first instance it would be necessary to determine the level of Government support for such an initiative – this will be a critical enabler and a clear understanding of the Government's view would assist in planning any strategy to move such an initiative forward.

Who are the Key Stakeholders?

255. The primary stakeholder is the New Zealand Government for without its firm support and direct involvement in any such initiative, it is unlikely to be effective – there would likely need to be clear and unambiguous support, at least at ministerial level, if not beyond. There are many other stakeholders but three groups in particular would include the CEO/Secretaries of New Zealand Government departments and agencies; the CEOs of significant companies in New Zealand and the nation's media.

Are there Likely to be Significant Resourcing Implications?

256. A strategy or programme designed to better engage wide cross sections of New Zealand in respect of national security would have costs, some potentially significant. Such an endeavour could not be done in the margins of other activities and it would need to be planned and resourced accordingly. That is not to suggest that all elements of any such initiative would have to occur concurrently, but rather that there would need to be a clear longer term strategy rather than an ad hoc or piecemeal approach.

Consideration 2: Enhanced Lead Generation by NZSIS

257. Bearing in mind the resourcing issues, which are addressed below, the Review **recommends that NZSIS seek to give increased priority to the development and implementation of initiatives to better enable NZSIS to identify emerging threats to security.** Current investigative frameworks tend to focus on areas or individuals known to be of security concern, and, while remaining absolutely valid, such frameworks can prove to be self-fulfilling.

258. As with its counterparts around the world, NZSIS needs to improve its ability to detect increasingly weak signals of potential security threats. Signals of security relevant activity are becoming more fragmentary as those engaged better understand and evade security service and police intelligence capabilities. Further, those involved are frequently rapid adopters of new technology and use this to hide or disguise their activity at a pace Governments struggle to overcome.

What is Proposed?

259. The Review suggests leads generation initiatives worthy of further consideration might include, but would not be limited to:

- As noted in the last section discussing with Government, in the context of the social licence it enjoys with the New Zealand community, **what actions and processes might be appropriate to better inform New Zealand citizens regarding the national security issues impacting on the nation.** It is envisaged an increased level of transparency with the population regarding national security issues and threats might encourage a greater confidence and willingness within the community to engage with authorities to report matters of potential security concern;
- **Exploring the Government's view and appetite regarding some level of data-mining** aimed at identifying emerging threats. The Review understands there will be some reticence regarding the use of such capabilities in New Zealand but, in any case, it considers there would be likely benefit in having a clearer Government view on that position, if only to assist in informing consideration of other lead generation possibilities;
- **Developing and implementing strategies to build a significantly greater understanding of NZSIS, its role, responsibilities and requirements across government agencies throughout the country.** The aim would be to build the ability (and willingness) of those agencies to identify security relevant issues and

behaviours, and advise relevant authorities, including the NZSIS. This would necessarily include a greater outreach function for NZSIS and production of security advice at the lowest feasible classification level; and

- **Consider the best strategies, within the available resourcing envelope, to better engage businesses in New Zealand** with the aim of encouraging those businesses to become more aware of threats to national security and providing an avenue to communicate any such concerns.

260. Any programme, or range of programmes, put in place to enhance lead generation and discovery will need to be supplemented by **new systems and processes to manage and investigate those leads (and the associated human and technical resources).** [REDACTED]

s6a: describes current programme

[REDACTED] It is envisaged that, in building any new capability, attention would need to be given to:

s6a: describes ways to enhance lead generation

Why is it Important?

261. A primary function of security services is to identify previously unidentified sources of security threat and to prevent harm occurring. To do so there is a requirement to continually develop and refine the systems used by services to identify those engaged in security relevant activity.

What Would Need to Occur?

262. Like other recommendations made in this report a first step would be to engage with the Government to determine its appetite to pursue different courses of action. Techniques such as data mining have been subject to wide debate across the world particularly in regard

to views of unwarranted intrusion into privacy. Other lead generation methodologies, while viewed as less invasive, will also have opponents.

263. Whatever the outcome of these discussions, it will be beneficial to generate community support for initiatives and seek to generate community trust that lead generation initiatives are being pursued appropriately and subject to necessary oversight.

Who are the Key Stakeholders?

264. The Government is the key stakeholder. Others with significant interests will include the IGIS and Privacy Commissioner and those organisations which have a particular interest in privacy issues. It is expected that New Zealand's media would also have a particular interest.

Are there Likely to be Significant Resourcing Implications?

265. There are potentially very significant resourcing implications (human, technical and physical) associated with significantly enhanced leads generation.

Consideration 3: Wider Direct Access to Government Data

266. With the introduction of the ISA 2017 the Government recognised the need for NZSIS to have direct access to selected data sources to enable it to fulfill its legislated role. That legislation identified selected data-sets from five agencies: the Registrar-General; the Department of Internal Affairs; Ministry of Business, Innovation and Employment; New Zealand Customs and NZ Police. Importantly while direct access to certain data was mandated in the ISA 2017, the legislation did not include any process (short of legislative change) to add further datasets to those identified in the 2017 legislation.

267. It is noted, despite significant work having been invested, that not all the agreements necessary to allow this access have been struck to-date and, as recommended earlier in this report, it is considered important that these are pursued as a matter of priority. This should include reconsideration of the purposes this data can be used for – for example the current limits on the use of policing data covered under direct access arrangements appear very limiting.

268. Consideration should be given to amending the ISA 2017 to include a non-legislative process for adding further datasets, as required, to Schedule Two. Any such amendment would need to continue to recognise the need for appropriate safeguards regarding access to, and the use and storage of, such information and data.

Why is it Important?

269. Information is the 'lifeblood' of any security service. As noted earlier, signals of intelligence activity are becoming increasingly weak, well hidden and fragmentary. Further, matters of potentially significant security concern can develop at a much faster pace – in counter-terrorism the trend is for individuals to radicalise more quickly and move to action in shorter timeframes.

270. Given the above, anything which can help investigators develop a more detailed understanding of a threat more quickly is of critical importance. s6a: operational process

[Redacted]

271. s6a: operational details

[Redacted]

272. What is being proposed in this recommendation is not for wider access to data (although that is a consideration in other recommendations) but rather enabling NZSIS to get more rapid access to some of the data sources it can already access – even though the manner in which that currently occurs is within an increasingly dated framework.

273. This is also important in respect of a recommendation to develop a wider and more systematic process to generate, develop and investigate lead information. The arguments for improving the development of lead intelligence are made separately, but should that recommendation be supported it will only be effective if NZSIS has in place systems which can facilitate its access to information and data.

274. Finally, NZSIS is a small service and must use its resources as efficiently as possible.

s6a: operational process

[Redacted]

275. This is not to suggest that all such information should become available via direct access – there will always be some types of information because of their sensitivity or the intrusion they pose into privacy where it will remain important and appropriate to seek access on a transactional basis through direct human interaction.

What Would Need to Occur?

276. What is proposed would require legislative amendment.

277. That, however, would not be all. To get the maximum utility from any such initiative NZSIS would also need to consider the ICT and compliance implications ^{s6a: operational detail} [REDACTED]. NZSIS would also need to ensure that any such access was fully auditable to both ensure it was being used correctly and, importantly, so that NZSIS can reassure the data's owner, the government and wider community that it was being used appropriately and in line with the government's and community's expectations.

Who are the Key Stakeholders?

278. As with any legislative change the Government and the Parliament of New Zealand are the key stakeholders. Others who will have a significant interest include the agencies and authorities which own the information and data; the IGIS and Privacy Commissioner and those organisations which have a particular interest in privacy issues. It is expected that New Zealand's media would also have a particular interest.

Are there Likely to be Significant Resourcing Implications?

279. Any legislative change generates work and this would be no different. However the greatest resourcing considerations will likely relate to the cost of developing the information technology infrastructure required to deliver data and information to NZSIS and the cost of the associated auditing capability.

Consideration 4: Criminalising a Wider Range of Preparatory Acts in Respect of Terrorism

280. The New Zealand Government recognised the requirement to introduce this type of legislation with the passing of the Terrorism Suppression Act 2002. It criminalised a range of activities including financing terrorism; recruiting for a terrorist organisation; participating in a terrorist group and the harbouring or concealing of terrorists. While the legislation has been in force for an extended period, covering the entire period of the rise of Islamic State and its caliphate, the legislation has been used very sparingly.

281. s6(a) operational detail

Anecdotally, and from discussions with senior New Zealand Police officers, the current legislation is difficult to use. Prosecutions of those seemingly on a pathway to mounting an attack have more been around subsidiary criminality (such as the possession of objectionable material) rather than 'acts in preparation' type criminal offences found in legislation in some other jurisdictions.

282. The difficulties in achieving prosecutions means NZ Police and NZSIS have been required to invest significant highly specialised and scarce resources monitoring the activities of individuals primarily for reasons of public safety. This means collection resources which could otherwise be utilised to identify and assess emerging or previously unidentified threats are used elsewhere.

283. Using NZSIS resources in this way not only impacts on its ability to conduct other investigations but also brings with it a range of other issues, including health and safety.

s6a: operational details

284. s6a: operational details

What is Proposed?

285. The Review suggests that NZSIS discuss with NZ Police its interest in jointly proposing legislation to criminalise a broader range of preparatory activities relating to terrorist activity.

286. In other international jurisdictions 'acts in preparation' legislation criminalises activities typically evident in the lead up to a terrorist incident. By way of example, in an Australian context, this includes:

- Manufacturing explosives;
- Making and loaning travel documentation;
- Advocating terrorism (up to 5 years);
- Providing or receiving training (up to 25 years);
- Possessing things connected with terrorist acts (up to 15 years);

- Collecting or making documents likely to facilitate terrorist acts (up to 15 years); and
- Directing the activities of a terrorist organisation (up to 25 years).

The above examples are only seeking to illustrate what has occurred elsewhere. Any such extension of legislation in New Zealand would need to be driven by the national context.

Why is it Important?

287. Such legislation would be important for a number of reasons including:

- It would provide a clear warning to extremists of the potential personal implications of moving towards terrorist violence. In some cases it might discourage individuals from even starting down that pathway;
- It would improve New Zealand Police's ability to prosecute those moving towards terrorist violence in the earlier stages of their attack planning, rather than the current requirement to monitor them until they meet the existing threshold for a terrorist or criminal offence; and
- It would, therefore, likely free up resources in security and policing, otherwise committed to monitoring these individuals of concern, and allow these resources to be focused on identifying sources of previously unidentified threat or harm – in the fields of both counter-terrorism and state intelligence.

What Would Need to Occur?

288. Legislative change would be required.

Who would be the Key Stakeholder?

289. NZ Police would have to be the driving force behind any recommendation. As noted above, with any legislative change the Government and the Parliament of New Zealand are the key stakeholders. Others who will likely have a significant interest include the legal fraternity; civil liberties organisations and the IGIS. It is expected that New Zealand's media would also have a range of views on any such proposal.

Are there Likely to be Significant Resourcing Implications?

290. Most costs would be met by those outside NZSIS. While there would likely be some cost to NZSIS (principally in executive/policy functions) there would also likely be a resource saving in terms of there being less requirement to direct investigative/collection resources to filling what has been, at times, coverage focused on public safety (rather than investigation).

Recommendations

292. This review has necessarily had a specific focus and a short timeframe due to NZSIS's objective of quickly identifying any major issues with extant processes and systems, as well as NZSIS's intention to provide the results of the Review to the Royal Commission. Significant matters for further consideration tend to have arisen in the context of the third major review element 'what *could* NZSIS have done'. Given the speculative nature of this question, Part 3 of the review was always going to be the least 'forensic'. Should NZSIS, or perhaps the Royal Commission, decide to pursue all or any of the recommendations, each will require significantly greater research and consideration than was able to be considered in the short timeframe. This is particularly the case where a recommendation has the potential to impact New Zealand's wider national security architecture or requires legislative change.

293. Further, it would be incorrect to assume there are not other areas of NZSIS's operations which might be enhanced or improved - although the Review is not suggesting that this is the case. Rather, it is important to note that the issues identified and recommendations made were the result of a specific focus.

294. What follows is a single 'listing' which brings together the recommendations made at various points throughout this report.

NZSIS Priorities and Priority Setting

Intelligence Prioritisation

295. NZSIS has significantly revamped and improved its priority setting frameworks over the last three years. It has created and refined a long-term operational strategy (STERLING) which meshes with the Government's new system for setting the country's high level NSIPs and includes processes which link NZSIS's operational strategy directly to its capability development and investment cycles. NZSIS has also created a strategic analysis capability which will play a pivotal role in translating the Government's high level intelligence requirements to a more workable and focused level.

296. NZSIS recognises that any prioritisation system remains a work in progress and, while not considered to be major issues, the **Review recommends that NZSIS further strengthen its intelligence prioritisation frameworks by:**

- **Instituting a programme to ensure the production, review and update of enduring (or thematic) information requirements occurs at least every twelve months.** These information requirements are a critical tool in shaping NZSIS's

investigation and collection work, particularly in terms of identifying emerging areas of security threat;

- Continuing to seek to **produce information requirements at the lowest possible classification to facilitate sharing** with wider government (and beyond, as appropriate). To enable this, it may be necessary to produce information requirements for the same thematic area at more than one classification level;
- **Reviewing, and as necessary adjusting, the threat/risk assessment processes that inform decisions** s6a: operational detail

[REDACTED]

- **Continuing efforts to build understanding across NZSIS of the critical role played by strategic analysis in the priority setting processes.** For some time NZSIS has, necessarily, had a significant investigative and collection focus on matters involving known threats. A wider and more in-depth understanding of the broader threat environment will further enable investigative and collection activities, and enhance NZSIS's ability to identify and prevent security harm.

NZSIS Investigative and Operational Frameworks

Leads Generation

297. The Review **recommends that NZSIS seek to give increased priority to the development and implementation of initiatives to better identify emerging threats** to security. Current investigative frameworks tend to focus on areas or individuals known to be of security concern, and, while remaining absolutely valid, such frameworks can prove to be self-fulfilling.

298. As with its counterparts around the world, NZSIS needs to improve its ability to detect increasingly weak signals of potential security threats. Signals of security relevant activity are becoming more fragmentary as those engaged in hostile activity better understand and evade security service and police intelligence capabilities. Further, those involved are frequently rapid adopters of new technology and use this to hide or disguise their activity at a pace Government's struggle to overcome. The Review suggests leads generation initiatives worthy of further consideration might include, but would not be limited to:

- Discussing with Government, in the context of the social licence it enjoys with the people of New Zealand, **what actions and processes might be appropriate to better inform New Zealand citizens regarding the national security issues impacting on the nation.** It is envisaged an increased level of transparency with the population regarding extant national security issues and threats might encourage a greater confidence and willingness within the community to engage with authorities to report matters of potential security concern;
- **Exploring the Government's view and appetite regarding some level of data-mining** aimed at identifying emerging threats. The Review understands there will be some reticence regarding the use of such capabilities in New Zealand but, in any case, considers there would be likely benefit in having a clearer Government view on that position, if only to assist in informing consideration of other possibilities;
- **Developing and implementing strategies to build a significantly greater understanding of NZSIS, its role, responsibilities and requirements across government agencies throughout the country.** The aim would be to build the ability (and willingness) of those agencies to identify security relevant issues and behaviours, and advise relevant authorities, including the NZSIS. This would necessarily include a greater outreach function for NZSIS and production of security advice at the lowest feasible classification level;
- **Consider the best strategies to better engage business in New Zealand** with the aim of encouraging those businesses to become more aware of threats to national security and providing an avenue to communicate any such concerns;
- **Accelerating work** currently underway in NZSIS's counter-terrorism investigations team **to develop baseline understandings of national and international extremist and terrorist entities**, particularly those which have an identified interest or connection to New Zealand or its interests; and
- **Accelerating work** currently in progress **under NZSIS's counter-terrorism 'discovery' programme** to identify methods, using established indicators, to identify otherwise unknown individuals and groups of security concern.

299. Any programme, or range of programmes, put in place to enhance leads generation and discovery will need to be supplemented by **new systems and processes to manage and investigate those leads (and the associated human and technical resources)**. Current programmes appear to be largely extensions of methodologies which have been in use to investigate lead intelligence for some time. It is envisaged that, in building any new capability, attention would need to be given to:

- An arrangement where there is a **clear shared agreement across key agencies regarding respective roles in developing, investigating and managing leads;**

- s6a: proposal for new system
[Redacted]

- s6a: proposal for improved capabilities
[Redacted]

300. Any such initiative could include a shared physical presence of responsible agencies or be virtual in nature. It is noted that, at a conceptual level, what is being suggested is not markedly different to the logic underpinning CTAG.

[Investigational and Operational Policy Frameworks](#)

301. Over the last few years NZSIS has devoted significant effort to the development of its investigative and operational policy frameworks. These are an important step in further professionalising NZSIS's operation. The Review notes the ensuring importance of training programmes and initiatives, such as discovery projects, aimed at encouraging staff remain open-minded to lead intelligence which suggests threats outside what is considered to be the norm.

302. s6a: operational details
[Redacted]

303. In terms of investigational policy, the Review notes NZSIS has been operating on interim guidance since mid-2018. Plans to update these frameworks have been on hold pending the outcomes of the s6a [redacted] review (which is focused on business improvement in NZSIS's operational and investigational areas) and the further bedding in of ISA 2017, related Ministerial Policy Statements and NZIC and Service policies. This was a pragmatic approach and sensible use of resources. While the s6a [redacted] work is now nearing completion, and could be a trigger for further work on the investigational policy update, **the Review recommends that, unless necessary, work be delayed on the investigative policy update until the conclusion of the Royal Commission.**

[Access to Information and Data](#)

304. Information and data are key enablers of NZSIS's intelligence function. s6a: [redacted] operational details [redacted]

305. The ISA recognises NZSIS's need to have direct access to government data and enables this through direct access agreements for datasets as identified in Schedule Two of the legislation. NZSIS has negotiated direct access in respect of four of six of these datasets and the **Review recommends that direct access negotiations in respect of the outstanding datasets (both held by NZ Police) are moved forward as a priority. Further the current limits on the use of that police data appear unnecessarily restrictive and would benefit from reconsideration.**

306. The Review also notes that a change to the ISA 2017 is required to add further datasets to the Schedule. Scheduling amendments to existing legislation, particularly in busy legislative agendas, is frequently difficult and often subject to extended delays. Given Parliament has recognised the need for NZSIS to have direct access to certain data (subject to various conditions and safeguards) it would seem that some other non- legislative process for adding (or removing) relevant datasets is warranted. **The Review recommends that NZSIS include in its legislative change agenda a mechanism to add/remove datasets from Schedule Two of the ISA by a process which does not include the requirement for legislative change and to allow for expanded use of those datasets subject to appropriate oversight and review.**

NZSIS Resource Allocation

307. It was not the purpose of the Review to review and recommend resource allocations across NZSIS's many important business units and as such the Reviewer has not sought to form a broader view on the matter. However, with respect to NZSIS's investigative and lead generation capabilities the Review considers two areas warrant renewed consideration or attention:

- *Systems and processes* - where current systems or processes absorb resources in a manner disproportionate to the extent these systems and processes contribute to NZSIS's legislated mission; and
- *Specific resource pressures* - where there appear to be significant resource pressures in respect of a specific function.

Systems, Processes and Using Resources More Effectively

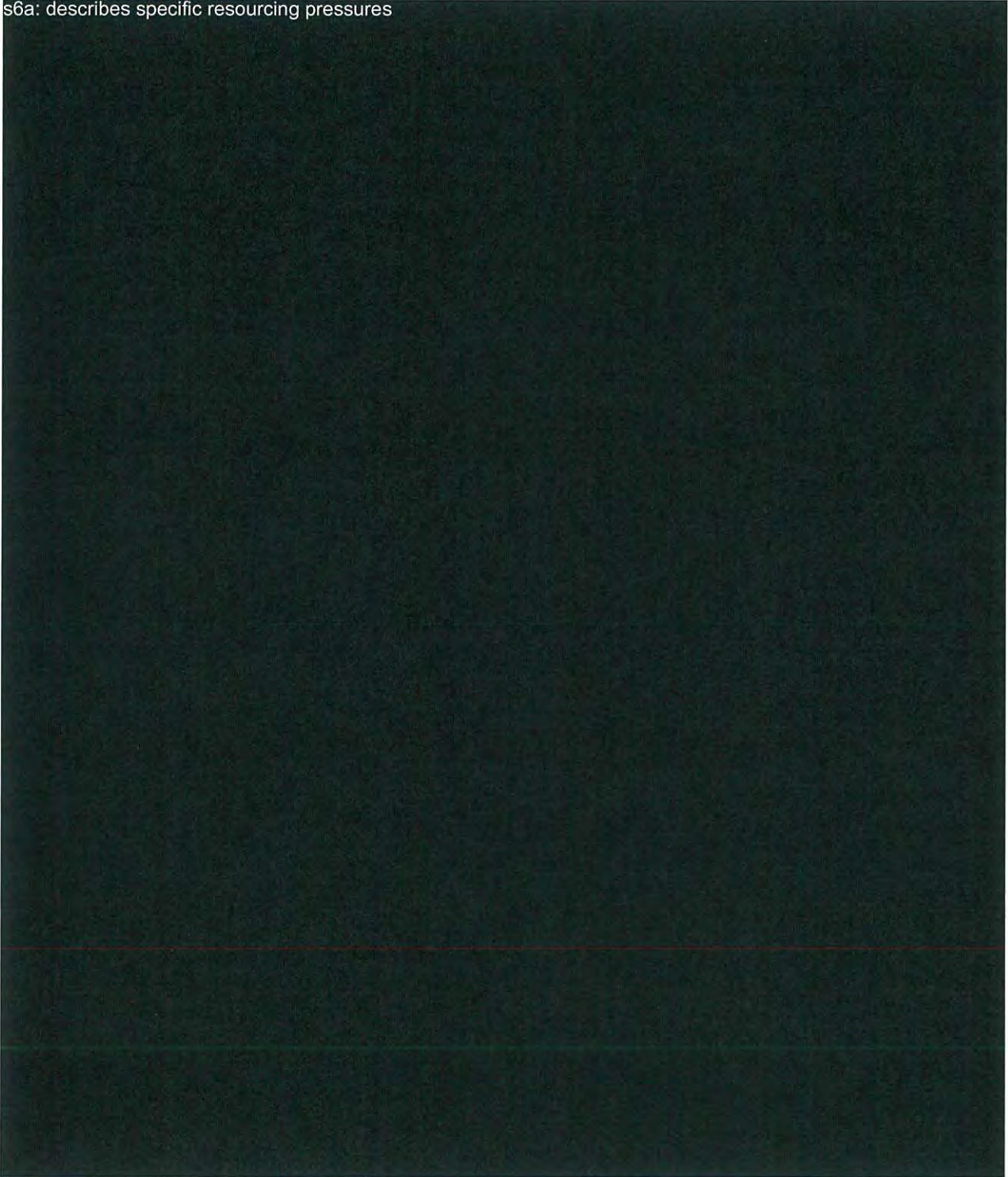
308. The Review notes NZSIS, in concert with NZ Police, expends significant levels of collection resources to monitor, rather than investigate, counter-terrorism targets that are assessed to have formed, or be close to forming, the intent to undertake a terrorist attack. Other governments, including in Australia, have criminalised a range of terrorism-related preparatory activities in their criminal codes. Such legislation has allowed Australian police services to charge persons for offences relating to acts in preparation for a terrorist act, when otherwise their actions would escape criminal sanction (other than potentially in relation to minor offences or at times unrelated criminal activity).

309. The Review believes it is likely similar legislation would assist in addressing this issue; reduce the risk to community safety and release NZSIS (and NZ Police) resources to identify and investigate other matters of potential security concern including yet to be identified threats. The identification of emerging threats is at the heart of a security service's function. Accordingly, the **Review recommends NZSIS seek the views of NZ Police regarding a joint approach to Government in respect of acts in preparation type legislation in New Zealand.**

310. An area which has been the subject of frequent comment in discussions with staff relates to the processes (and associated resource cost) surrounding Human Rights Risk Assessments (HRRAs). The Review believes the current policy framework appears reasonable and workable but perhaps is being used or interpreted in a way which is creating significant work. **The Review recommends NZSIS reassess its current HRRAs processes with a particular focus on seeking Ministerial approval for more countries and authorities in those countries and centralising NZSIS's process for considering the human rights credentials of candidate countries and authorities.**

Specific Resourcing Pressures

s6a: describes specific resourcing pressures



NZSIS Legislative and Compliance Frameworks

Removing Ambiguity

314. NZSIS has experienced very significant legislative and policy changes over the last two years. This has resulted in ambiguity among staff regarding the interpretation of these changes (legislative and policy), which has generated uncertainty, particularly among newer or more junior staff regarding what is, or is not, appropriate. s6a / s92(ba)(i): describes impact of operational ambiguity

[REDACTED]. Removing, or at least reducing this ambiguity, would be a valuable step in building confidence in staff regarding the methodologies available to them to identify and investigate matters of potential security concern and reduce the likelihood of 'missteps'. It will also likely lead to significant resource savings across a range of functions and reduce 'second guessing' about what is, and what is not, required.

315. Given nearly two years has passed since the introduction of the ISA 2017 legislation and associated policies, the **Review recommends NZSIS test with the Minister, Commissioner of Intelligence Warrants and the IGIS NZSIS's view of warrant thresholds; the situations where NZSIS believes the use of these more intrusive powers is warranted; and the level of detail required by those who authorise and provide oversight to the process in order to inform their judgements and decisions.** In preparing any such submission, the Review believes it would be important to include case studies as these will be useful in informing staff regarding the requirements of decision makers.

316. From mid-2018 NZSIS has also increased its discovery work. This is important given the changes in the security environment which make it increasingly difficult to identify matters of security concern, as was demonstrated by the 15 March 2019 terrorist attacks. For the same reasons as detailed above, the Review would further **recommend that NZSIS test its understanding of investigation thresholds with the Minister.** This will assist NZSIS in ensuring it is operating up to the 'line' the government expects and managing risk to New Zealand as effectively as possible within that setting.

Ministerial Policy Statements and Joint Policy Statements

317. There is a widely agreed view, both inside and outside NZSIS, that these policy documents were produced quickly and, with what has been learned since their introduction, there are several areas which could be improved. From a Review perspective, the policies most commonly commented on were those relating to information sharing with foreign

partners (including requirements for HRRAs) and the use of publicly available Information. As noted elsewhere in this document, it is the Review's contention that the management of the HRR process can be significantly improved within the current policy framework. There is probably a greater argument in respect of reviewing the MPS governing NZSIS's use of open source information, especially online. In any case, given the Royal Commission is due to report in December 2019 and the MPSs are scheduled to be reconsidered in 2020, it is **the Review's recommendation that NZSIS work within the current MPS framework with a view to pursuing the required amendments during the 2020 review.**

NZSIS Partnership Arrangements

318. Like in many aspects of its operations, NZSIS has made significant progress in the building of essential partnerships. What were in the past, perhaps at best, limited transactional arrangements with NZ Police are now significantly more open and demonstrate good levels of collegiality and trust across all levels of management. The challenge for NZSIS will be to take these relationships to the next level and to engage a wider cross-section of government, business and the broader community. Several of the recommendations made earlier in this section are relevant to this area, in particular those relating to lead generation.

Increased engagement with government, business and the wider public

319. As noted earlier in this section the Review considers there to be significant benefit for NZSIS to engage in a structured programme to enhance government and public understanding of NZSIS's priorities and requirements. Intelligence requirements and reporting should be shared at the lowest feasible level (such as through tearlines). In terms of dissemination, NZSIS should consider assuming greater responsibility for the dissemination of information to those without classified communications, and bolstering NZSIS's impact by ensuring those sharing the information have a sufficient depth of knowledge to have meaningful follow-up discussions. There should be clear points of contact for agencies, with personnel at tier 3 senior management level and above having ownership of key relationships.

320. The likely scale and resourcing implications of building connections into an ever-widening national security community mean it will not be able to happen overnight and there will need to be an unambiguous narrative, directly involving Government, as to why this is important to the nation's security. There are, however, a range of initiatives NZSIS might develop in the shorter term while considering what a longer term strategy might entail and seeking Government support for that strategy. In the short term **the Review recommends that NZSIS:**

- **ensure partners in the 'wider' New Zealand national security community have a clear understanding of NZSIS's role and its requirements and the materials (and other assistance) which will help those partners better educate their staff about NZSIS.** ~~s6a: operational detail~~
[REDACTED];
- **produce and disseminate intelligence reporting and NZSIS's information requirements at the lowest feasible classification (particularly in respect of counter-terrorism);**
- **produce unclassified material which describes likely indicators of security relevant activity, wherever possible, which can be provided as appropriate to a wider range of those who work with the community. This will primarily relate to those engaged in enforcement actions but will have wider applicability;**
- **put systems in place to use NZSIS systems to send and store classified materials government officials need to see where partners do not have access to classified national security communication systems** ~~s6a: operational detail~~
[REDACTED]
- **build feedback loops into systems where other parts of government provide information to NZSIS. This will help shape what they provide and encourage further involvement.**

321. Finally, the Review recommends NZSIS should consider balancing its security briefings with training on how 'need to know' works. This will allow greater confidence in staff sharing information and requirements in order to have greatest impact while preserving security.

Appendix

1.	s6a [Redacted]
2.	(U) Terms of Reference for a Royal Commission on the attack in the Christchurch Mosques on 15 March 2019
3.	(R) Terms of Reference for NZSIS Christchurch attack review, 8 April 2019
4.	(C) Arotake – NZSIS internal review (Email) 11 April 2019
5.	(R) AROTAKE: Request for endorsement of proposed search protocol (tranche 1), 3 May 2019
6.	(S) Appendix A – Information Repositories (AROTAKE)
7.	(S) Appendix B - Discovery Search Terms (AROTAKE)
8.	(U) Intelligence and Security Act 2017
9.	(S) Discovery Search Results AROTAKE
10.	s6a [Redacted]
11.	s6a [Redacted]
12.	s6a [Redacted]
13.	s6a [Redacted]
14.	(TS/NZEO) Performance Improvement Framework – Review of the agencies in the core NZIC March 2014
15.	s6a [Redacted]
16.	(TS//NZEO) New Zealand national security and intelligence priorities supporting organizing framework approved Dec 2018 [ERS-18-SUB-0026]
17.	s6a [Redacted]
18.	(S//NZEO) Project AGUERO: Review of the New Zealand Intelligence Community’s Security Intelligence Operating Model, September 2015
19.	(S//NZEO) Project STERLING: The NZSIS 10-Year Operational Strategy, June 2016

20.	s6a	[Redacted]
21.	s6a	[Redacted]
22.	s6a	[Redacted]
	s6a	[Redacted]
23.	s6a	[Redacted]
24.	s6a	[Redacted]
25.	s6a	[Redacted]
26.	s6a	CTAG Threat Assessment: The New Zealand terrorism threat environment (082/18/TA), dated 16 January 2018
27.	(U)	Age of the Wolf: A Study of the Rise of Lone Wolf and Leaderless Resistance Terrorism, 15 February 2015
28.	s6a	[Redacted]
29.	(S) s6a	Implementation: Refreshing corporate and change governance: Decision Paper, December 2017
30.	(S)	Principles for Monitoring the NZSIS Workforce Plan – as at 31 August 2018, 31 August 2018
31.	(TS//NZE0)	Highlights of SCRR Growth: Building Trust and Confidence through the First Four Years of Scenario Three to 2020, April 2019
32.	s6a	[Redacted]
33.	(C)	Auckland SLT Discussion 25 October 2018
34.	(U)	Intelligence and Security Committee Act 1996
35.	(U)	Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand – Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM – 29 February 2016
36.	(U)	Privacy Act 1993
37.	(U)	Ministerial Policy Statement – Cooperation of NZ intelligence and security agencies (GCSB and NZSIS) with overseas public authorities
38.	(C//FVEY)	Joint policy statement: JPS-006 Human Rights Risk Management Policy

39.	(S//NZEO) New Zealand Intelligence Service Annual Report 2018
40.	s6a [Redacted] s6a [Redacted] s6a [Redacted]
41.	(S//NZEO) s6a [Redacted] Review: Proposal for Change, 31 May 2017
42.	(S//NZEO) Project STERLING Strategic Goal Implementation Plan, March 2018
43.	(S// FVEY) Counter Terrorism Unit Strategy 16 July 2018
44.	(S//FVEY) Discovery Questions, June 2018
45.	(S//FVEY) Discovery (PowerPoint) September 2018
46.	s6a [Redacted]
47.	s6a [Redacted]
48.	(S) NZSIS Investigations interim guidance, 13 June 2018
49.	s6a [Redacted]
50.	(S//ORCON//FVEY) New Zealand Terrorism Update: September-November 2018, 4 December 2018
51.	(S//NZEO) Information and Intelligence Requirements: Extreme Right Wing (XRW) Activity in New Zealand, 9 July 2018
52.	s6a [Redacted]

~~TOP SECRET COMINT~~
~~NEW ZEALAND EYES ONLY~~

DMS60-8-1105

	s6a	
53.		
54.		

~~NEW ZEALAND EYES ONLY~~
~~TOP SECRET COMINT~~

55.	s6a	[REDACTED]
56.	s6a	[REDACTED]
57.	(R) XRW Exercise	
58.	(S//NZEO) CT Table Top Exercise (Notes), 3 January 2019	
	(S//NZEO) CT Tabletop Exercise Oct 2018 (PowerPoint)	
59.	s6a	[REDACTED]
60.	s6a	[REDACTED]
61.	s6a	[REDACTED]
62.	s6a	[REDACTED]
63.	s6a	[REDACTED]
64.	(S) AROTAKE: Mock Investigation Leads	