The 2019 Terrorist Attacks in Christchurch: A review into NZSIS processes and decision making in the lead up to the 15 March attacks

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 [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 [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 [redacted] at the time of the terrorist attacks on 15 March 2019 (if anything)?
- What **should NZSIS have known** about [redacted] 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 [redacted] 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 [redacted] prior to the attack.

To determine **what NZSIS *did* hold about** [redacted] 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' [redacted] 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 [redacted] 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 [redacted] 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 [redacted] or attack planning.

As a result of these detailed searches, and input from NZSIS's staff, the Review has concluded [redacted] 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 [redacted] 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 gove nment 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 [redacted] 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 [redacted] plans was if NZSIS had gained an intelligence warrant and mounted a covert technical attack on [redacted] 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 [redacted] 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 [redacted], 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 [redacted] 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.

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.