Letting in the Light – Increasing Transparency in the New Zealand Intelligence Community
Speaking Notes for Transparency International NZ AGM

Ms Rebecca Kitteridge, Director-General of Security

New Zealand Security Intelligence Service

Monday 30 October 2017, Wellington

Tēna koutou, tēna koutou, tēna koutou katoa.

I am really grateful to Transparency International New Zealand for inviting me to speak today. I am a real believer in the importance of the work of Transparency International. In addition to its work with the private sector, it shines a light on the workings of governments around the world in support of open government, democracy, and integrity in decision making.

Those are values in which I have strongly believed all my life. They are values that my parents instilled in me, and they have been areas of specific focus for me in my professional life – particularly when I worked in the Cabinet Office as constitutional adviser, Deputy Secretary, and as Cabinet Secretary. In those roles my work involved advising on the operation of democracy, considering ethics and propriety in relation to the conduct of executive government, supporting open and accountable government under the Official Information Act, and ensuring sound decision-making processes.

So how did a nice girl like me end up working in a secret organisation like the New Zealand Security Intelligence Service? How did a champion of open government turn into a secret squirrel, and why did she want to?

The answer is that I have always wanted to make the best contribution I can to New Zealand through public service. The NZSIS seemed to need a person with my kind of background, to help it out of a time of trouble and to create greater openness and public trust. The way it actually happened was like this. I became interested in the Service in about 2010. Iain Rennie, then State Services Commissioner, suggested that I might want to think about it as a next step.

I remember thinking "What do they actually DO at NZSIS?" I knew about vetting for security clearances, but apart from that I knew almost nothing about them – only what I had read in the media, which over many years had been relentlessly negative. As Cabinet Secretary I had a clear understanding of other government agencies, but this one was opaque. On the rare occasions when I dealt with staff at the Service (for example, when consulting them on aspects of the Cabinet Manual), the people I spoke to wouldn't even give their last names. I was intrigued.

So I was already interested in the New Zealand Intelligence Community when I was asked to carry out a review of compliance at the Government Security Communications Bureau. (You may remember that the compliance review was prompted by the events surround the raid on Mr Kim Dotcom.) I knew even less about GCSB and had absolutely no idea what to expect. I imagined that the staff of GCSB would be suspicious of me when I arrived to start the review, but they could not have been more open and welcoming. I realised the truth of the statement that these agencies have "high external walls but low internal barriers." Once you have your TOP SECRET SPECIAL clearance, then people will freely share with you what you need to know.

It was a real privilege to work in GCSB at such a time of organisational distress. I saw people who were proud of their work, who were passionate New Zealanders, and who were motivated to do what Parliament had mandated them to do in the way that Parliament had intended. They knew that they were in difficulty and they were horrified about it. They were not at all defensive about working with me to identify the root causes.

During that time I got my first real view of the work of New Zealand's intelligence community, and how the intelligence cycle works. I was very impressed with the calibre of the staff and how clever they are at their work. Not that I would claim to understand the technical side of what they do at the Bureau – maths has never been my strong point. But I developed a very high regard for the signals intelligence professionals and the others who work at GCSB. By the time the review was completed I was really interested in the role of Director of the NZSIS. Interestingly, even though the Service had co-located with the Bureau in Pipitea House, I still had very little idea about what its people did. I did not "need to know" about the NZSIS for the purposes of the GCSB compliance review, and so I was not told.

When the NZSIS Director role was advertised, I applied and started preparing in earnest. I knew that the Service was an agency that specialised in human intelligence, or "HUMINT." I didn't have many sources of information about the work of the Service. There was of course popular fiction. The works of John Le Carré, James Bond films, and programmes like Homeland gave me some pretty weird ideas about what might be going on at the NZSIS.

So, being a lawyer, I turned to what promised to be a more reliable source of information: the New Zealand Security Intelligence Act 1969. And that told me almost nothing. It described the functions of the NZSIS in general terms – to collect intelligence, to provide protective security advice, and so on – but most of the focus of the legislation is on intelligence warrants. If you just relied on the 1969 Act to form a view of the scope of the intelligence collection activity of the Service, you would think that all we do is intercept private communications under the authority of a warrant.

In reality the Service has always conducted a range of human intelligence collection activities, including physical surveillance in public places, and obtaining information from human sources.

I learned about these other activities after I got the job as Director. And what I realised was that these activities were not included in the legislation because they were not unlawful. The Service started out its life when the Police Special Branch was turned into a stand-alone agency, and at that time it had no legislative basis whatsoever. As with other security agencies in similar countries, officers of the Service simply undertook a range of activities in carrying out their work in the interests of national security.

The 1969 Act represented a great step forward when it provided a legislative basis for activities such as intercepting telephone calls and installing listening devices. But the 1969 Act did not in any way refer to any activities undertaken by the Service that were lawful, such as physical surveillance. When passed in 1993, The Privacy Act would have created problems for a number of our activities (like obtaining information from banks and telecommunications companies) except that we obtained a broad exemption to much of the Act. But none of the activities that we were undertaking under that exemption were referred to in the 1969 Act.

From a strictly legal point of view, this was fine. There is a strong line of argument among jurists that legislation should only be used when required to authorise activity, and should not purport to regulate activity that is already lawful.

Under this argument legislation should not authorise physical surveillance, for example, because it is already lawful to follow and watch a person in a public space.

The problem with this argument in relation to the Service over time was that the social contract was changing. By “social contract” I mean on the one hand the licence given by the public to intelligence agencies to operate, and on the other hand the level of information the public expects to know about intelligence activities in return. There are several reasons why the social contract has been shifting.

First, the changes in the threatscape around the world – particularly in relation to terrorism – have meant that security agencies have needed greater powers to detect the activities of terrorists.

Second, changes in technology have given security and intelligence agencies more opportunities and more challenges, with greater privacy implications for New Zealand citizens.

Third, as transparency in government has increased, the public's expectations have changed. People expect to know what the agencies of the state are doing. The public pays for these agencies and there is an expectation that the public will have a say in our activities and how they are conducted.

The outcome of the public debate that has occurred in New Zealand and in other liberal democracies is that there is a new point of balance between the public's right to know and the agencies' need to keep operational activity and capabilities secret. And that is very healthy.

Being more open about what we do reduces the risk that staff will want to expose operational activity that they feel the public should know about. Ultimately it strengthens public trust. There will always be a point at which we need to keep operational information and capabilities secret. Our targets and adversaries are watching and listening closely to learn how to evade or penetrate us. But more information about us is being made public without seriously compromising our ability to carry out our work.

The government recognised the need to recalibrate the social contract when it decided in 2015 to conduct a comprehensive review of the legislation governing the two intelligence agencies and our oversight bodies.

The review was conducted by Dame Patsy Reddy (now the Governor-General) and Sir Michael Cullen (former Deputy Prime Minister under the previous Labour Administration). In 2016 they released the Report of the First Independent Review of Intelligence and Security in New Zealand.

The Report, and the legislation that was based upon it – the Intelligence and Security Act 2017 – intentionally created a level of transparency and openness about our work that had previously not existed. In fact, the reviewers stated in the report's introduction that they saw the review as an opportunity to raise public awareness about the intelligence and security agencies' work.

The Report was unclassified and was made publicly available. It gave people access to information about what we do, why we do it and how we do it, which in many cases had not previously been described publicly. For example, the Report talked about the NZSIS's human intelligence activities – also referred to as HUMINT. That was the first time that HUMINT had been referred to publicly.

If you haven't read the report, I recommend taking some time to read through it. It is a great example of the balance that can be struck in describing activity without compromising it. The Intelligence Community contributed to the review and the subsequent legislative public consultation process by providing a number of case studies. Those case studies were a mix of actual cases and

hypotheticals, which helped to give people a clear understanding of the context in which we might need certain powers or functions, and how we might conduct ourselves. They were unclassified and were published on the Department of Prime Minister and Cabinet website.

The case studies really shone a light on specific aspects of our work for the first time. For the first time, we gave examples of our counter-espionage work. Espionage is the act of obtaining confidential information by covert means. Espionage is traditionally associated with states stealing secrets from other governments, but the Report revealed that espionage is now also being conducted against New Zealand businesses.

We described a case concerning some undeclared foreign intelligence officers working in New Zealand, who had displayed an enduring interest in a prominent New Zealand private sector entity. The entity had been the subject of both traditional human and cyber espionage by the foreign intelligence service.

NZSIS had engaged the New Zealand entity to provide a defensive briefing and had discussed with them the espionage threat posed by foreign intelligence services. GCSB had also provided advice and support.

That is just one of many case studies included in the Report. The Report therefore represented a significant flinging open of the doors of the agencies, and the Intelligence and Security Bill maintained that approach. The Bill was referred to the Foreign Affairs, Defence and Trade Committee of Parliament (rather than the secret Intelligence and Security Committee) and followed a normal select committee process, including the consideration of public submissions. On 28 March this year, the Intelligence and Security Act was passed with the first provisions coming into force on 1 April. The remainder of the provisions came into force on 28 September.

Some important principles have been carried forward from our earlier legislation (although in some cases these provisions apply for the first time to the GCSB):

- For example, section 16 continues to state that the agencies are not law enforcement agencies.
- Section 17 continues to provide that the agencies must act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; independently and impartially; with integrity and professionalism; and in a manner that facilitates effective democratic oversight.
- Section 18 provides that the agencies must be free from improper influence and be politically neutral.

- Section 19 states that the activities of the agencies must not limit the right of freedom of expression in New Zealand.
- Section 20 continues the obligation on the Directors-General of the agencies to keep the Leader of the Opposition regularly informed about matters relating to the functions of the agencies.

The Act sets out our objectives and functions in a more transparent way. The Service and the Bureau have largely the same national security objectives and functions. We contribute to the protection of New Zealand's national security, its international relations and well-being, and its economic well-being.

We achieve these objectives by collecting, analysing and communicating intelligence to those who need to know it. We provide protective security services, advice and assistance. We cooperate with other public authorities (such as Police, and NZDF) to facilitate their functions.

While NZSIS's and GCSB's objectives and functions are largely the same, the Act makes clear that we deploy different and complementary capabilities in relation to those objectives and functions. In the case of the Service, we deploy human intelligence capabilities, and in the case of the Bureau, signals intelligence and cybersecurity capabilities.

The ISA provides a much clearer authorising framework. The Act states more clearly what we do under a warrant, including any human intelligence activity that would otherwise be unlawful.

The Act makes it easier for people to understand the two different types of warrants we use, and the approvals that are required.

Type 1 warrants relate to New Zealand citizens or permanent residents. In most cases, Type 1 warrants will only be issued if they will enable an intelligence and security agency to investigate harms such as terrorism, violent extremism, espionage being directed against New Zealand, sabotage, proliferation of weapons of mass destruction, or transnational crime.

To obtain a type one warrant, there is a 'triple lock' process. The warrant is issued by the Minister and a Commissioner of Intelligence Warrants. It is then reviewed by the Inspector General. Type 2 warrants relate to foreign citizens. A type two warrant is issued by the Minister alone, and is also reviewed by the Inspector-General after it is issued.

You may recall my earlier comment about why statutory authorisation should not be provided for activity that is already lawful. The reviewers came up with a really clever mechanism for regulating

our activities, including some of our lawful activities. That mechanism is the Ministerial Policy Statement – or MPS.

The ISA provides that the Minister must issue MPSs across a range of operational activities. An MPS sets out the Minister's expectations and guidance for the agencies as to how certain lawful activities, necessary for us to perform our functions under the Act, should be carried out.

We must apply the guidance and principles articulated in the MPS when we plan and carry out the activities to which each MPS relates. That in turn provides the framework for good internal decision making and assists the Office of the Inspector-General with its oversight function.

The MPSs were drafted for the Minister by the Department of the Prime Minister and Cabinet, after consultation with NZSIS and GCSB. DPMC also consulted the InspectorGeneral of Intelligence and Security, the Privacy Commissioner, and other relevant agencies such as Ministry of Foreign Affairs and Trade, the Ministry of Justice, and the New Zealand Police.

Eleven MPSs are now in effect. Very briefly, they provide guidance as to the conduct of the following activities:

- Conducting surveillance in a public place
- Conducting surveillance activities in accordance with an exemption from the Land Transport (Road User) Rule 2004
- Requesting information from other agencies, both in the public and private sectors
- Requesting information lawfully from agencies or individuals when we do not have a warrant and we are therefore asking people to share information voluntarily
- Obtaining and using publicly available information (for example, open source information that is available on the internet)
- Creating and maintaining a legal entity such as a company without revealing its connection to NZSIS
- Our staff acquiring and maintaining assumed identities to give them cover so that they can undertake their work
- Our staff making false or misleading representations about being employed with an intelligence and security agency (which is also about our staff maintaining cover)
- How information obtained by GCSB and NZSIS is managed, including the retention and destruction of that information
- How the New Zealand intelligence and security agencies cooperate with overseas public authorities (in particular, to ensure that we meet our human rights obligations under New Zealand law)
- How GCSB provides information assurance and cybersecurity support to an organisation, with the consent of that organisation.

These MPSs cover some very significant ground. They are unclassified documents, which are publicly available through our website, the GCSB website and the New Zealand Intelligence Community website. As well as the Ministerial Policy Statements, there a number of other operational activities that are either new to us or that are articulated and made public for the first time.

The first is Direct Access Agreements. Direct Access Agreements allow an intelligence agency to access information from other agencies directly, so they are very important. The ISA provides that Ministers may agree to allow direct access, but they must sign a Direct Access Agreement, setting out in detail the constraints and procedural requirements governing the access.

Two Agreements have been entered into so far, relating to Customs and Immigration New Zealand databases. The Agreements are available on our website and the website of the relevant agency.

The Act also introduces a new regime for intelligence agencies to obtain business records from telecommunication and financial service providers. Previously, those companies provided information to us on a voluntary basis. They understood that we needed the information for the purposes of investigating threats to national security, and that they could provide the information properly under an exemption to the Privacy Act. Nonetheless the voluntary approach was becoming more and more difficult to sustain. The companies concerned were trying to balance the competing interests of national security and customer privacy. The Act recognises this difficulty by enabling an intelligence agency to compel a telecommunication or financial service provider to release certain records, with the approval of the Minister and a Commissioner of Intelligence Warrants. This provision formalises the basis on which information is provided and makes the process much more transparent.

For the first time, our legislation provides for NZSIS to use cover and assumed identities to carry out our work. Although people have probably been aware that the NZSIS would use cover identities, this essential practice had no legislative basis until now. The ISA made amendments to the Protected Disclosures Act 2000 as it relates to the disclosure of classified information and information about activities of an intelligence agency. This is commonly referred to as “whistle-blowing.”

The amendments mean that for disclosures of classified information, or information relating to the activities of an intelligence and security agency, organisations are required to put in place a number of internal procedures.

The provisions make clear that the Inspector-General of Intelligence and Security is the "appropriate authority" for protected disclosures relating to the intelligence agencies. The provisions also ensure

that disclosures are made to people who have the appropriate security clearance and who are authorised to have access to that information. The ISA also continues the existing protections for employees who bring any matter to the attention of the Inspector-General.

These provisions are extremely important to the agencies, as well as the public. They mean that if a staff member has concerns about any aspect of an intelligence agency's work, there is a route to raise the concerns that is independent, effective, safe to the staff member, and that protects national security equities. We regularly remind our staff that they can make protected disclosures to the Inspector-General.

This brings me to oversight. The new Act continues to provide strong oversight of both intelligence agencies.

Most information about our work, by necessity, is classified. We do not reveal a lot of what we do publicly in the same way as most other public sector agencies. In these circumstances, effective oversight of our activities is essential to provide New Zealanders and the government with confidence that we are conducting ourselves lawfully. There are three types of oversight of the agencies.

The Office of the Inspector-General of Intelligence and Security (or the "Office of the IGIS" as it is sometimes known) is the key oversight body of the New Zealand intelligence agencies. The IGIS inspects key documents, and reviews the activities of the agencies. The office also investigates public complaints about the activities of the intelligence agencies. The IGIS has full, direct access to our information and records, both operational and corporate. The intelligence agencies provide information and resources to support IGIS investigations and queries. The agencies meet regularly with staff from the Office of the IGIS to discuss issues.

The Inspector-General's unclassified versions of reports on our work are published on her website for anyone to read. The second oversight body is the Intelligence and Security Committee, which provides parliamentary oversight of the intelligence agencies. The Committee examines issues like organisational efficiency and efficacy, budget, expenditure and policy. The Committee is made up of members of Parliament representing both the Government and the Opposition.

Thirdly, like all public service agencies, the NZSIS is subject to the Official Information Act and Privacy Act.

When NZSIS receives requests for information we try to be as open as possible without compromising security. Due to security and privacy concerns, however, we cannot always be forthcoming with information. When we cannot release information, we try to provide as much information as possible and clearly explain why we have given a particular response.

Under the previous Act NZSIS was exempt from nearly all of the Information Privacy Principles under the Privacy Act. We are now subject to more Privacy Act provisions than we have been previously. We are still exempt from some provisions, for national security reasons, but the exemptions are much more limited.

We continue to have the ability to give a "neither confirm nor deny" response. That response is sometimes necessary from a national security point of view. NZSIS has, in the past, been the subject of orchestrated requests from people of security concern who are trying to find out more about NZSIS-specific areas of investigation. NZSIS does not always know who is making a bona fide request and who is not.

The Office of the Ombudsman and the Office of the Privacy Commissioner provide important oversight of the work we do. If a member of the public is not satisfied with the NZSIS's response, they may seek a review with the Ombudsman or the Privacy Commissioner.

The last thing I will mention about the new legislation – but by no means the least – is that under the ISA, the NZSIS has become a public service department.

We had been behaving like one as much as possible already (for example, my appointment process was managed by the State Services Commissioner, who also reviewed my performance), but now, like Pinnochio becoming a "real boy," NZSIS is a "real public service department." The Public Service Code of Conduct applies to us now. My staff can belong to a union, and they can pursue employment grievances through the Employment Court. I'm sure you can see that the journey that we have been on, as it relates to transparency and openness, has been very significant indeed.

The media and the public now have access to a lot of information about us and our work, through documents like the Independent Review, the legislation, and the websites of the agencies and the Inspector-General. GCSB's Director-General Andrew Hampton and I are committed to continuing to speak publicly and to make ourselves available, as appropriate, to the media. Our intention is to be as open and accountable as possible.

My successor will have a much easier time working out what kind of organisation he or she is

applying to lead. It will be evident to him or her that an episode of Homeland is not a very true reflection of the Service's work, and that James Bond would be unlikely to get a job with us.

Having more accurate information in the public domain will help the people of New Zealand to have an informed voice in the ongoing discourse about the place and work of intelligence and security agencies. I truly believe that that can only be positive for the intelligence community and the public.

I want to thank you again for inviting me here to speak with you.

The NZSIS has not always had a very visible public presence. While the NZSIS handles secret information, we need not be a completely secret organisation.

Thanks for having me.