NEW ZEALAND COUNCIL OF TRADE UNIONS
Te Kauae Kaimahi

Submission of the New Zealand Council of Trade Unions Te Kauae Kaimahi

to the

Independent Review of Intelligence and Security

P O Box 6645
Wellington
14 August 2015

1. Introduction

1.1. This submission is made on behalf of the 36 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With 325,000 members, the CTU is one of the largest democratic organisations in New Zealand.

1.2. The CTU acknowledges Te Tiriti o Waitangi as the founding document of Aotearoa New Zealand and formally acknowledges this through Te Rūnanga o Ngā Kaimahi Māori o Aotearoa (Te Rūnanga) the Māori arm of Te Kauae Kaimahi (CTU) which represents approximately 60,000 Māori workers.

1.3. Thank you for the opportunity to make this submission. We would like to be contacted by the independent reviewers to discuss this submission. In the first place, please contact Dr Bill Rosenberg, Policy Director/Economist, billr@nzctu.org.nz, or landline (04) 8023815.

2. Context

2.1. The CTU has over many years consistently expressed a high degree of concern regarding the increase in powers and intrusiveness of surveillance in New Zealand society including both the SIS and GCSB and their increased powers and wide definitions regarding "terrorism", the widening of authority to install and use surveillance equipment such as through the Search and Surveillance Bill, the widening of the definition of "security" to include "New Zealand's international well-being or economic well-being"[1], the increased use of private investigators by companies to watch people the SIS considers are working against its interests, the increased powers to make use of informants, aspects of the extension of powers regarding electronic surveillance, and other developments that could be used against people considered opponents of the Government of the day.

[1] For example the definition of 'security' in s.2 of the New Zealand Security Intelligence Service Act 1969 includes:

> **security** means— … (c) the protection of New Zealand from activities within or relating to New Zealand that— … (iii) impact adversely on New Zealand's international well-being or economic well-being

2.2. Unionists have long been targets for surveillance and accusations by security forces, despite having a firm basis of legitimacy in domestic and international law. We can provide examples of abuse of security powers and unjustified negative consequences for unionists and other people exercising their rights as citizens in New Zealand over several decades. Those consequences come from the State and from those with a degree of power over them such as employers.

2.3. The expansion of the remit of SIS and the GSCB[2] to include protection of "economic well-being" meant that any actions or viewpoints with potential economic consequences could be subject to SIS or GCSB activities (the latter through its cybersecurity remit). Most union activity is deliberately concerned with economic wellbeing, as is much political activity in the community. The reach of the agencies is therefore too broad and this heightens the need for improved transparency, accountability and oversight.

2.4. The definition of National Security[3] used by the Department of the Prime Minister and Cabinet (DPMC) in its coordinating role for all of government is even more wide reaching and includes:

1. Preserving sovereignty and territorial integrity

Protecting the physical security of citizens, and exercising control over territory consistent with national sovereignty.

3. Strengthening international order to promote security

Contributing to the development of a rules-based international system…

4. Sustaining economic prosperity

Maintaining and advancing the economic well-being of individuals, families, businesses and communities.

[2] For example s 7(3) of the Government Communications Security Bureau Act 2003 states that one of the three objectives of the Bureau is to contribute to "the economic wellbeing of New Zealand." Similarly the definition of "security" in s 2 of the New Zealand Security Intelligence Service Act 1969 defines security, in part, as the protection from actions that "impact adversely on New Zealand's international well-being or economic well-being".

[3] "New Zealand's National Security System", May 2011, p.3, http://www.dpmc.govt.nz/sites/all/files/publications/national-security-system.pdf, accessed 14 August 2015.

5. Maintaining democratic institutions and national values

Preventing activities aimed at undermining or overturning government institutions, principles and values that underpin New Zealand society.

2.5. Recent revelations include the surveillance of 88 New Zealanders by the GCSB with dubious legality, the events surrounding Kim Dotcom (again of questionable legality and having little to do with New Zealand's security and much to do with pursuit of alleged economic rights by US copyright holders), and the provision of misleading material by the SIS Director to political operatives in the Prime Minister's office which was clearly of use and used against his political opponents. These events aggravate concerns that extraordinary powers are at high risk of being used improperly or for mainly economic reasons, that the systems intended to protect against abuse are insufficient and the services lack sufficient public scrutiny.

2.6. In addition, the Snowden revelations added substance and evidence to previous concerns regarding New Zealand agencies' relationship with foreign agencies such as the National Security Agency (NSA) in the US. New Zealand agencies are collaborating with foreign agencies which can collect and use data to disadvantage New Zealand individuals or to monitor or disrupt legal activities which the foreign government considers against its interest. Data gathered by the NSA – some provided by New Zealand agencies – could be used in ways that are illegal in New Zealand but provide information to local agencies enabling them to evade legal responsibilities.

2.7. An exemplar of many of these concerns is the growing, now widespread, opposition to the Transpacific Partnership Agreement (TPPA) negotiations and similar treaties regarding international commerce. The interests at stake are in large part economic ones and it is an entirely valid civic debate with themes similar to many common political discussions and election campaigns. The economic aspect provides a pretext for New Zealand intelligence agencies to surveil and otherwise take an interest in the opponents of the TPPA in the guise of "the protection of New Zealand's international well-being or economic well-being" when the whole debate

is about whether the TPPA adds to or subtracts from New Zealand's well-being. This is far from the normal view of protecting security: it is deeply political.

2.8. The debate over the TPPA is also substantially about sovereignty and democracy with many concerned that it would significantly detract from the practice and principle of these values. It is also fundamentally about the establishment of a "rules- based international system". The DPMC's definition of National Security therefore encompasses many parts of this debate. It is unlikely this definition of security will lead to the intelligence and security agencies being used to rein in Government actions despite widespread concerns that those actions imperil national sovereignty, prosperity, economic well-being and democratic values and misuses "rules-based international systems". Instead it leads to concern that legitimate debate is exposed to surveillance and democratic processes are undermined.

2.9. There is also concern that the New Zealand agencies are used to monitor the communications of small island states engaged in negotiations with New Zealand such as the long drawn out, unequal and sometimes bitter PACER-Plus negotiations, giving New Zealand even greater advantage. Documents released by Snowden showed New Zealand spying on Fiji and the Solomon Islands for example. The allegations that Minister Tim Groser's ambition to become Director-General of the World Trade Organisation was assisted by New Zealand surveillance of his rivals falls into a similar bucket. Ethical concerns are not limited to freedom of speech, political freedom, privacy and confidentiality.

2.10. There are fundamental questions as to whether and to what extent we need agencies for security and intelligence, or whether some or all of their activities would be better performed by (for example) the Police who are open to much more public and judicial scrutiny.

2.11. We are therefore concerned that the terms of reference of this inquiry are not broad enough to consider many of the most important problems with New Zealand's intelligence and security system.

2.12. We have not answered the multiple choice questions at the beginning of your submission form because it is impossible to do so accurately in such a simplistic way. We are concerned that reliance will be placed on the answers to those questions. They assume definitions (such as of "terrorism", "New Zealand's economic interests", and "adverse foreign influences") over which there is no agreement.

2.13. However in general terms we are as uncomfortable about corporate access to personal information and their potential use of it as we are about state access and use. New Zealanders' interests are being compromised by the lack of regulation of (for example) sale of metadata and personal information.

2.14. We also draw your attention to our submission on the Government Communication Security Bureau and Related Legislation Amendment Bill 2013 which contains a number of recommendations relevant to this inquiry. It is available at http://union.org.nz/policy/gcsb-ctu-submission.

3. Responses to questions about topics in the terms of reference

3.1. Here, we respond to some of the questions from 13 onwards in your submission form. Questions 14, 17 and 18 overlap so we answer them under question 14 but that should be read in conjunction with our reply to question 13.

13. Do you think the functions and powers the GCSB and NZSIS have under their governing legislation strike the right balance between allowing the agencies to effectively protect New Zealand's interests and ensuring people's rights are respected? Please describe what you see as the strengths and weaknesses with the current system in terms of striking this balance, and how you would suggest any weaknesses could be addressed.

3.2. No.

3.3. The definition of "security" is far too broad, encompassing, as noted above, New Zealand's "economic well-being" which opens virtually all political and union activity to surveillance. This should be removed from the definition. The status of the even broader DPMC's definition of National Security, which presumably has practical

effect in determining the activities and priorities of the agencies, should also be clarified.

3.4. The definition of "terrorism" could be interpreted by an authoritarian government or a politically prejudiced security agency (both of which have occurred in New Zealand's history) to encompass political activities or industrial action in New Zealand or abroad which even if unpopular is far from what is commonly accepted as terrorist behaviour. For example s5 of the Terrorism Suppression Act 2002 which defines a "Terrorist act" includes an act intended to cause major economic loss for the purpose of advancing an ideological or political cause with the intention to unduly compel or to force a government to do or abstain from doing any act. There are many ambiguous terms used here, and these kinds of accusations are not infrequently made against workers taking strike action or citizens taking disruptive forms of protest. There is an attempt to address such concerns in s5(5) of the Terrorism Suppression Act 2002, but it is confusing and difficult to understand. It is not clear why terrorism should be distinguished from any other serious crime which our statutes deal with. The motivation is what defines it and that can be taken into account in sentencing rather than in broader powers which risk compromising civil liberties.

3.5. These mean that surveillance, threat of which or whose discovery can be intimidating to many people, can be carried out against citizens whose activities present no threat to New Zealand's security in a commonly accepted sense.

3.6. Powers to use informants pay insufficient regard to the potential for abuse of the informants' powers and the effect on employment relationships. Operatives who are not fully trained and do not have full accountability to the head of the agency should not be used.

3.7. Public information about use of surveillance powers and warrants is far from sufficient for the public to know whether powers are being properly used or abused. More detail should be published more frequently. The blanket secrecy around agencies' funding should be removed from the Public Finance Act and reporting

should be public with withholding of specific information only where justified on reasonable grounds.

3.8. There is no longer protection against the GCSB surveilling or conducting mass surveillance over New Zealand residents. There should be a clear line drawn to prevent this surveillance.

3.9. The agencies' relationships with international counterparts including sharing of personal information provides opportunities for abuse and damage to New Zealand's international reputation. There is potential for these relationships to be used to avoid restrictions on the New Zealand agencies' activities and powers with regard to New Zealand residents, and to aid foreign agencies in doing the same with regard to their own nationals. Legislation should protect New Zealand residents against surveillance by foreign powers. It should make clear that the agencies cannot use their international relationships to avoid restrictions on their activities and powers, nor to abet unlawful behaviour by other agencies. There should be public reporting on international relationships and what kinds of activities they entail.

14. Do you think the legislation contains adequate checks and balances on how the agencies exercise their powers and functions?

17. Do you think the current oversight arrangements are sufficient to ensure that the GCSB and NZSIS operate within the law and act appropriately?

18. Do you think the current oversight arrangements give members of the public confidence that the activities of the GCSB and NZSIS are adequately scrutinised?

3.10. No. The checks and balances and statutory oversight of the GCSB and NZSIS are insufficient.

3.11. While the office of the Inspector-General of Intelligence and Security has been strengthened, recent revelations about the agencies leaves strong concerns that they are still able to act in improper ways without sufficient and pro-active oversight. The Inspector-General is still not empowered to stop the agencies from

continuing with inappropriate or unlawful activities. While more rigorous investigations by the Inspector-General and her greater willingness to make public critical reports are a step forward, the investigations have been prompted by evidence that has come into the public arena. We do not yet have confidence that the kinds of behaviour criticised or whose lawfulness was brought into doubt by these reports would have been discovered or clamped down on, let alone prevented, if they had not been made public. There needs to be more frequent and detailed public reporting of the office's activities and findings. Scrutiny by the Intelligence and Security Committee (but see below) should be open to the public.

3.12. The political oversight is still severely compromised. The Intelligence and Security Committee is not a Select Committee and does in general not meet or act openly. It is controlled by the Prime Minister and so is no substantial check on him or her. It has no interest in (or can be prevented from) investigating problems in the intelligence and security system if the Prime Minister is happy with the way the system is working or doesn't wish to be embarrassed by revelations that might result.

3.13. The Committee should be a full Select Committee with membership not in Cabinet and not including the Prime Minister and with power to conduct reviews, question the Prime Minister, any responsible Minister and heads of the agencies. It should have independent expertise available to it on security and technical matters. The Committee's proceedings should by default be open to the public and records of its proceedings and its reports should be made public with minimal redactions.

3.14. In short, there is no effective public oversight of the Prime Minister's role in intelligence and security. The fact that there is now a separate Minister with responsibility for these agencies only diminishes this concern slightly: the Minister is likely to be unwilling to challenge the Prime Minister and to expose politically embarrassing activities of the agencies.

3.15. The reporting from the agencies is minimal and provides no ability for the public to judge them. The public is consequently reliant on the Prime Minister and the

Intelligence and Security Committee to carry out this role, but it may not be in their interests to do so. There should be much fuller and frequent reporting.

15. Do you think the legislation has kept up with changes in technology and the nature of national security risks? If you answered no, please explain why and whether there any amendments you would suggest to respond to these changes.

3.16. We are concerned that mass surveillance has been made practical by technology but there is insufficient protection against mass surveillance occurring either by the New Zealand agencies or from agencies abroad (such as through provision of data by New Zealand agencies or by monitoring international communications, including through stations on New Zealand soil).

3.17. We are equally concerned at the growing potential for the private sector to collect and use information gathered electronically. This is particularly true of information and communication technology suppliers such as Microsoft, Apple, Google, Facebook and ISPs, but also retailers increasingly collecting information through loyalty schemes and other means. While most current use may be benign, the potential for surveillance for commercial purposes, which could then be acquired by state agencies, is high.

3.18. Storage of the information is also an issue. Where it is stored overseas it may be subject to surveillance and use by security and intelligence agencies in those countries, and there may be fewer protections for the data of non-nationals than for nationals. This is true in the US.

Countering Foreign Terrorist Fighters Legislation

20. Do you think some or all of the current provisions should continue in their present form beyond 31 March 2017?

3.19. The Bill was introduced and passed with unnecessary speed, allowing only two days for submissions. Such a process increases public suspicion at the motives for the legislation, and leads to poor legislation. It is disrespectful of the public and the democratic processes.

3.20. The changes allowed the SIS to carry out visual surveillance on private properties under warrant, and to conduct surveillance activities for up to 24 hours without a warrant in situations of emergency or urgency where activities related to terrorism are alleged.

3.21. Given that no evidence has been produced about the use or misuse of these powers, their successes and failures, it is impossible for the public to judge other than from first principles. Neither have we have seen evidence that threat levels in New Zealand are so high that this legislation, which breaches basic human rights, was necessary.

3.22. Reports from the Inspector-General and the Privacy Commissioner on the use of the powers in this legislation should be requested and published, and then further opportunity given for public submissions. The report should cover the situation regarding "Foreign Terrorist Fighters" in New Zealand including numbers suspected of leaving to become "terrorist fighters", the numbers surveilled and the numbers prevented from leaving New Zealand, the numbers of warrantless uses of the legislation and numbers of warrants issued for these purposes, the nature of the use of Customs data, the number of times it was used, whether or not it was effective in deterring the activities as intended, any concerns of its use or abuse, and whether the information could have been obtained by other means.

3.23. We do not believe that obtaining a warrant is an impossible barrier to urgent action. Provisions could be put in place for such emergencies to ensure that the Commissioner for Security Warrants and the Minister are readily available through secure electronic means.

3.24. While the limitation of its use to alleged terrorist activities is better than no limitation as originally proposed, it still suffers from the problems with the definition of "terrorism" and the possibility that suspicions of such activities were wrong. This comes on top of concerns that the agencies have a record of improperly using their powers (such as in the cases noted above).

3.25. On current evidence, we do not believe the current provisions for warrantless surveillance and special powers to search Customs data should continue.

Definition of "private communication" in the GCSB Act 2003

22. What type of information do you think should be covered by the definition of "private communication" (and therefore protected under section 14)? For example, should only the content of communications be protected, or metadata (eg, the date and time of an email) as well?

3.26. The Act defines "private communication" as follows (s4):

private communication—

(a) means a communication between 2 or more parties made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but

(b) does not include a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so

3.27. We agree with the concerns of submitters when the GCSB Act was amended in 2013. According to the Commentary to the Government Communications Security Bureau and Related Legislation Amendment Bill 2013 which amended the Act, "Currently the GCSB does not consider metadata to be a 'communication'". Therefore metadata interception and collection does not require a warrant. Metadata, however, is according to some experts at least as valuable and possibly more valuable that the content of communications when large volumes of data are being intercepted. Information on who is communicating with whom, how often, from where to where and at what times can be highly intrusive and useful to the agencies.

3.28. We also agree with submitters who expressed concern that the "reasonableness to expect interception" test can create a vicious circle of increased surveillance: the more surveillance there is (or it is perceived or reputed there is), the greater the "expectations of interception" which in turn permits increased surveillance.

3.29. It is crucially important for privacy and confidentiality reasons to prevent mass surveillance and warrantless surveillance. This requires protection of the whole message being communicated including metadata. It also requires protection of communications between New Zealand residents and residents of other countries.

4. Conclusion

4.1. This inquiry cannot be adequate because of its limited terms of reference.

4.2. We have longstanding concerns about the potential for misuse of security agency powers and these concerns are increased by evidence of the actions and attitudes of the agencies over many years, including recent events.

4.3. There is insufficient oversight of, and too little information available about, the activity of the agencies and it may well be that many of their functions could be better carried out by the Police with greater accountability. We have made recommendations on these matters.

4.4. On specific questions, the powers given by the Countering Foreign Terrorist Fighters Legislation should not continue, private communications should be defined to include metadata, and there should be greater protection of private communications against interception.