NEW ZEALAND COUNCIL OF TRADE UNIONS
Te Kauae Kaimahi

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

to the

Intelligence and Security Committee

on the

Government Communication Security Bureau and Related Legislation Amendment Bill

P O Box 6645
Wellington
June 2013

1. Summary of recommendations

1.1. The CTU strongly supports calls by Labour and the Greens for an independent inquiry into the operation of the intelligence services as a whole including a review of the impact of information gathering using programmes such as PRISM and BLARNEY to ensure that they appropriately safeguard New Zealand (and New Zealanders' rights) and to rebuild lost trust. Changing legislation to legitimise previous poor practice will do the opposite: amendments to the intelligence agencies' powers should be the last step in a detailed and careful consideration.

1.2. The recent inquiry of the Inspector-General of Intelligence and Security ('the IGIS') into potential breaches of the Government Communications Security Bureau Act 2003 ('the GCSB Act')[1] should be released. While the detail of the investigations may be secret (and may be redacted), the correct interpretation of the Act is an important question of public law and should be disclosed.

1.3. The decision that the Government Communications Security Bureau ('the GCSB') is to be permitted to spy on New Zealanders should be subject to a much more rigorous process than truncated consideration by the Intelligence and Security Committee. The CTU recommends that any law change permitting the GCSB to spy on New Zealand citizens or permanent residents must await the outcome and recommendations of the independent inquiry.

1.4. The CTU recommends that the amendments to expand the grounds for storage and sharing of information under new section 25 to include "preventing or responding to threats to human life in New Zealand or any other country" and "identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country" do not proceed. These grounds are far too broad.

1.5. The CTU supports strongly supports amendments to require the GCSB to:

- Keep a register of interception warrants and access authorisations (clause 18 inserting proposed section 19). It is alarming that this does not occur already.

[1] Regarding the GCSB's spying on 88 New Zealand citizens and permanent residents between the coming into force of the GCSB Act on 1 April 2003 and 26 September 2012.

- Comply with privacy principles relating to the collection, usage, storage and retention of personal information as per the Law Commission's recommendations from the review of the Privacy Act 1990.

1.6. As the Regulatory Impact Statement notes, legislative change is unnecessary in relation to the exercise of the GCSB's powers which may be addressed by the development of guidance. Non-legislative solutions are much more consistent with the rights of freedom of expression and freedom from unreasonable search under the New Zealand Bill of Rights Act 1990.

1.7. Though it is not a matter of legislative change, the CTU recommends moves to ensure that the Office of the IGIS is adequately resourced to proactively and effectively deal with issues. Office staff should include not just a Deputy IGIS but also (modelled on the Australian Office of the IGIS) former intelligence community employees, a legal advisor, review staff and administrators.

1.8. The CTU supports the Bill's proposals to bolster the powers and responsibilities of the IGIS to undertake proactive investigations into systemic compliance issues and the provision of unclassified versions of the IGIS's reports.

1.9. The CTU recommends that changes are made to the Intelligence and Security Committee Act 1996 to ensure that:

- The committee is not chaired by the Minister in charge of the New Zealand Security Intelligence Service. It is a clear conflict of interest.
- The Intelligence and Security Committee is empowered to undertake inquiries of its own motion and to compel evidence from intelligence service employees. Appropriate security safeguards should be put in place to allow this to occur.
- Committee meetings and reports should be open to the public except where there is a compelling reason to the contrary

2. Table of contents

3. Introduction

3.1. This submission is made on behalf of the 37 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With 340,000 members, the CTU is one of the largest democratic organisations in New Zealand.

3.2. 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.

3.3. The CTU has consistently expressed a high degree of concern regarding the increase in powers and intrusiveness of surveillance in New Zealand society including 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 “the making of a contribution to New Zealand’s inter-national well-being or economic well-being”, the increased use of private investigators by companies to watch people it considers are working against its interests, and other developments that could be used against people considered opponents of the government of the day.

3.4. Unionists have long been targets for surveillance and accusations by security forces, despite having a firm basis of legitimacy in domestic and international law. Union activity is deliberately concerned with economic wellbeing, as is much political activity in the community.

3.5. Our concerns are rendered acute by the revelations of ubiquitous monitoring of electronic and telephonic communications by the United States of America's National Security Agency ('NSA') under programmes codenamed PRISM and BLARNEY.[2]

3.6. The Prime Minister has stated "We do exchange - and it's well known - information with our partners [including the NSA]."[3] His reassurances that information sharing is not used to circumvent New Zealand law ring somewhat hollow however as it is unclear what interpretation of the New Zealand law the GCSB relies upon. The Prime Minister has been unforthcoming on the question of whether New Zealand uses similar systems to PRISM.

3.7. We are concerned that, in light of the GCSB's failings and failure of oversight identified in the Review of Compliance at the Government Communications Security Bureau ('the Kitteridge Report') the Government's response has been to legislate away the parts of the Act which the GCSB has breached.

3.8. We agree with the Kitteridge Report that:[4]

> GCSB [is at the] high-risk end of the compliance spectrum. Its powerful capabilities and intrusive statutory powers may only be utilised for certain purposes. The necessarily secret nature of its capabilities and activities prevents the sort of transparency that would usually apply to a public sector organisation. It is therefore imperative that the public be able to trust that those exercising the powers are doing so only in the way authorised by Parliament. A robust compliance regime, including visibly demanding external reporting and oversight, should provide considerable assurance to the public.

3.9. While the Government Communication and Security Bureau and Related Legislation Amendment Bill ('the Bill') goes part way towards addressing compliance issues we believe this is not enough and that it addresses some issues in the wrong way.

---

[2] See for further detail: http://www.guardian.co.uk/world/nsa

[3] David Fisher and Matthew Theunissen 'Key: No GCSB legal loophole' NZ Herald 11 June 2013 http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10889696

[4] 'Review of Compliance at the Government Communication Security Bureau', Rebecca Kitteridge March 2013 at [38]. Retrieved from http://www.gcsb.govt.nz/newsroom/reports-publications/Review%20of%20Compliance_%20final%2022%20March%202013.pdf

3.10. The New Zealand Public Service Association (the PSA), which is an affiliate of the CTU, represents a number of the staff of the GCSB. There is a constructive relationship with the Chief Executive and the PSA expects that it will be fully engaged and consulted on any aspects of the proposals in the Bill that impact on PSA members in the GCSB and their jobs and workloads.

4. Scope of the law regarding New Zealand citizens and residents

4.1. The CTU is extremely concerned that the proposed amendments widen the GCSB's ambit to undertake surveillance of New Zealand citizens and permanent residents.

4.2. The first justification is that the law is unclear. In her introductory speech to the Bill's first reading the Minister of Justice, Hon Judith Collins, stated that:[5]

> A particular issue has arisen around the bureau's role in supplying crucial support to other entities, including the New Zealand Defence Force, the New Zealand Security Intelligence Service, and the New Zealand Police. It has been a longstanding practice of the Government Communications Security Bureau…to provide assistance to other entities. However, as I stated earlier, there are difficulties of legal interpretation in the existing Government Communications Security Bureau Act, including in relation to this assistance. The Government has decided that there is too much uncertainty to continue this very important activity under the existing law. The vast bulk of this type of activity remains on hold until legislation is passed by this Parliament to provide greater clarity about whether the bureau can provide assistance to others. Currently the Act says that assistance may be provided but only on matters relevant to the pursuit of the bureau's own objective, or the safety of a person, or the prevention or detection of serious crime. That limits or at least makes uncertain when the bureau is able to share its expertise across the intelligence community and the wider public sector. We want to provide greater clarity and ensure the bureau can help other agencies fulfil their lawful duties, particularly in the areas of security and law enforcement.

4.3. Much of the assessment of the legality of the GCSB's actions remains secret, such as the report of Paul Neazor, the Inspector-General of Intelligence and Security ('the IGIS'), into 88 instances of possible illegality in the GCSB's surveillance of New Zealand citizens.

4.4. While Mr Neazor has not released or commented on his report, the Director of the GCSB, Ian Fletcher, has issued a media statement on the unreleased report. Mr

[5] (8 May 2013) 689 NZPD 9657

Fletcher notes "The Inspector-General is of the view that there were arguably no breaches and the law is unclear."[6]

4.5. As Matthew Hooton (and others) have noted "a conclusion that reads 'arguably there were no breaches of the law' can be re-written as 'arguably there were breaches of the law' without any change in meaning."[7] This analysis is strengthened by the requirement in section 6 of the New Zealand Bill of Rights Act 1990 that "wherever an enactment can be given a meaning that is consistent with the rights and freedoms contained in this Bill of Rights [including rights of freedom of association and security against unreasonable search and seizure], that meaning shall be preferred to any other meaning."

4.6. Mr Neazor's conclusions ought to be subject to public scrutiny and discussion even if confidential information is redacted to protect sensitive on-going investigations. It is important to address public suspicion that he has been "captured" by the agencies it is his unique role to scrutinise, and releasing this report is an important step in this direction. The CTU recommends that the Intelligence and Security Committee takes whatever actions open to it or its individual members for this to occur.

4.7. Notwithstanding Minister Collins' comments or Mr Neazor's view (which we cannot assess) we believe that the law is clear in relation to the interception of communications of New Zealand citizens and permanent residents. We agree with Nicky Hager that:[8]

> This is not a technical legal issue about unclear legislation. The GCSB has had a clear, long-term pact with the public. It claimed the right to spy on countries and join in wars without telling us anything about it, but it gave an assurance that it would not spy on New Zealanders. This reassurance has been repeated year after year and is written into legislation.
>
> I am embarrassed to say that I heard the unequivocal assurances and read the clear prohibition in the GCSB legislation, and I believed that they did not spy on New Zealanders. But it turns out they have been regularly spying on New Zealanders from before 2003 and since. They have seriously let down the public.

[6] Ian Fletcher, 21 May 2013 'IGIS finds no GCSB breaches but law not clear' http://www.gcsb.govt.nz/newsroom/reports-publications/PR%20IGIS%20review%20May%202013.pdf
[7] Matthew Hooton 'Labour, Greens right on GCSB report' *National Business Review* 23 May 2013 http://www.nbr.co.nz/report
[8] Nicky Hager 'Who is really responsible for the GCSB shenanigans?' retrieved from http://pundit.co.nz/content/who-is-really-responsible-for-the-gcsb-shenanigans

4.8. We note also the repeated assurances made during the passage of the original GCSB Act that New Zealanders would not be spied upon. In her speech at the first reading, Helen Clark stated categorically:[9]

> In the absence of a legislative framework for GCSB, for example, some have wrongly inferred that the Bureau's signals intelligence operations target the communications of New Zealand citizens; that the GCSB exists only as an extension of much larger overseas signals intelligence agencies; and that the Bureau's operations are beyond the scope of Parliamentary scrutiny.
>
> For the record, I reiterate again today that the GCSB does not set out to intercept the communications of New Zealand citizens or permanent residents. Furthermore, reports of the Inspector-General of Intelligence and Security have made it clear that any allegations to the contrary are without foundation. The Inspector-General has reported his judgement that the operations of the GCSB have no adverse or improper impact on the privacy or personal security of New Zealanders.

4.9. The second justification used for the expansion of the GCSB's power is the cost of duplication. The associated Regulatory Impact Statement[10] ('the RIS') states that:

> 21. In addition to the issues above, the GCSB plays a crucial role in the support of other government agencies, in particular the New Zealand Defence Force and the NZSIS. The GCSB also supports the New Zealand Police in the detection and investigation of serious crime. The GCSB's unique capabilities are an invaluable resource for those agencies to draw upon.
>
> 22. The GCSB Act review considered that in a small jurisdiction such as New Zealand we cannot afford to duplicate expensive and sophisticated assets, and there are limited numbers of people that can work with such assets. Consistent with the Better Public Services programme, the capabilities such as those developed or acquired by the GCSB, where appropriate and subject to necessary safeguards, should be available to assist in meeting key Government priorities. This too should be addressed in the update of the GCSB Act.

4.10. While the CTU is sympathetic to cost pressures in Government and the desire to do more with less, we are extremely concerned that, as the Bill currently stands, the necessary safeguards are insufficient and have been substantially weakened.

4.11. We agree with Vikram Kumar that:[11]

---

[9] Helen Clark 'First reading of the GCSB Bill' (8 May 2001) http://www.beehive.govt.nz/release/first-reading-gcsb-bill

[10] 'Government Communications Security Bureau Act Review' Regulatory Impact Statement 22 March 2013

[11] Vikram Kumar's draft submission retrieved from http://internetganesha.files.wordpress.com/2013/06/submission-gcsb-bill.pdf

> No analysis has been provided of the costs vs. benefits (both tangible and intangible) of alternative options, in particular of an agency such as the New Zealand Security Intelligence Service (SIS) developing the capabilities it needs itself, or that the National Cyber Security Centre (NCSC) cannot be strengthened or re-purposed to achieve this goal.
>
> Extending this logic and the Better Public Services programme, in the name of efficiency, expertise concentration, systems, sources, and resource rationalisation, the SIS and GCSB should be merged into a single agency. The logic that drives the Government to keep these two agencies separate is the very reason that the specialised capabilities of the GCSB should not be used to further the work of the SIS and other agencies… The unrestrained flow of GCSB's data to the NSA… is another consideration.

4.12. The decision that the GCSB ought to be permitted to spy on New Zealanders should be subject to a much more rigorous process than truncated consideration by the Intelligence and Security Committee. We call for an independent inquiry into our intelligence services below. The CTU recommends that any proposal allowing the GCSB to spy on New Zealand citizens or permanent residents must await the outcome and recommendations of the independent inquiry.

5. Information retention and sharing with other agencies

5.1. The CTU is concerned that the proposed provisions allowing the GCSB to retain and share information with "any other person that the Director thinks fit to receive the information"[12] are far too wide.

5.2. As Grant Robertson notes:[13]

> When I obtained the documents from the court about the Kim Dotcom case, one of the things that struck me about the documents that came from the Government Communications Security Bureau as part of those court documents was the classifications on top of each page of those documents. Having worked in the Ministry of Foreign Affairs and Trade, I am used to the various titles and names, but there were some that I did not recognise, and on further investigation they were classifications that indicated that this material was going to be shared with international agencies. We have been told publicly by various people with the bureau that this material would not be shared, but that information—those designations on those documents—indicates that it is routine for Government Communications Security Bureau information to be shared internationally. What assurances do New Zealanders have that under this legislation, if the bureau is working with those other agencies, that information will not be shared overseas?

[12] Proposed section 25(3)(d))
[13] (8 May 2013) 689 NZPD 9657

5.3. The current authorisation for information sharing with New Zealand and international agencies is given by section 25 of the GCSB Act:

> **25 Prevention or detection of serious crime**
>
> Despite section 23 [destruction of irrelevant records obtained by interception], the Director, for the purpose of preventing or detecting serious crime in New Zealand or in any other country, may retain any information that comes into the possession of the Bureau and may communicate that information to employees of the New Zealand Police or to any other persons, and in any manner, that the Director thinks fit.

5.4. The proposed new section 25 is considerable wider:

> **25 When incidentally obtained intelligence may be retained and communicated to other persons**
>
> (1) Despite section 23, the Director may—
>
> (a) retain incidentally obtained intelligence that comes into the possession of the Bureau for 1 or more of the purposes specified in subsection (2); and
>
> (b) communicate that intelligence to the persons specified in subsection (3).
>
> (2) The purposes are—
>
> (a) preventing or detecting serious crime in New Zealand or any other country:
>
> (b) preventing or responding to threats to human life in New Zealand or any other country:
>
> (c) identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country.
>
> (3) The persons are—
>
> (a) any employee of the New Zealand Police:
>
> (b) any member of the New Zealand Defence Force:
>
> (c) the Director of Security under the New Zealand Security Intelligence Service Act 1969:
>
> (d) any other person that the Director thinks fit to receive the information.

5.5. Serious crime is defined in section 4 of the GCSB Act as any indictable offence in New Zealand[14] though this definition will be amended on 1 July 2013 to specify offences punishable by two or more years imprisonment (the indictable / summary distinction is being removed).[15]

[14] To constitute serious crime, offences in overseas countries must be offences that would be indictable if occurring in New Zealand

[15] It may be appropriate to ask whether this is the correct threshold to use. Offences punishable by 2 years maximum imprisonment include (*inter alia*): misconduct in relation to human remains (section 150 Crimes Act 1961); bigamy or feigned marriage / civil union where the other spouse knew that the marriage / civil union would be void (sections 206 and 207 of the Crimes Act 1961); conspiring to prevent collection of rates or taxes (section 309 of the Crimes Act 1961); and (perhaps ironically) use of interception devices (section 216B of the Crimes Act 1961)

5.6. We are concern by the widening of the grounds for retention and sharing of information. No real justification has been given for the widening to include "preventing or responding to threats to human life" and "identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country."

5.7. It is unclear what additional situations "preventing or responding to threats to human life" might cover that are not also serious crimes.

5.8. Much more concerning is the extension of the provision to "the national security of New Zealand or any other country." Unlike 'serious crime,' 'national security' is not defined in legislation.[16] The DPMC's document 'New Zealand's National Security System' sets outs a non-exhaustive definition of national security as used by New Zealand's intelligence agencies as follows:

> **What is National Security?**
>
> National security is the condition which permits the citizens of a state to go about their daily business confidently free from fear and able to make the most of opportunities to advance their way of life. It encompasses the preparedness, protection and preservation of people, and of property and information, both tangible and intangible.
>
> Seven key objectives underpin a comprehensive concept of national security:
>
> 1. Preserving sovereignty and territorial integrity
> *Protecting the physical security of citizens, and exercising control over territory consistent with national sovereignty*
>
> 2. Protecting lines of communication
> *These are both physical and virtual and allow New Zealand to communicate, trade and engage globally.*
> 3. Strengthening international order to promote security
> *Contributing to the development of a rules-based international system, and engaging in targeted interventions offshore to protect New Zealand's interests.*
>
> 4. Sustaining economic prosperity
> *Maintaining and advancing the economic well-being of individuals, families, businesses and communities.*
>
> 5. Maintaining democratic institutions and national values

[16] 'Security' is defined broadly in section 2 of the New Zealand Security Intelligence Service Act 1969 but following ordinary rules of statutory interpretation, it would appear that 'national security' is intended to be different (or parallel drafting would have been employed). If the Committee intends otherwise then the term 'security' should be used

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

6. Ensuring public safety

Providing for, and mitigating risks to, the safety of citizens and communities (all hazards and threats, whether natural or man-made).

7. Protecting the natural environment

Contributing to the preservation and stewardship of New Zealand's natural and physical environment.

National security policies were traditionally focused on protecting the State against military threats or political violence. While responding to any such threats remains a fundamental responsibility of government, modern concepts of national security manage civil contingencies and societal risks alongside these traditional priorities.

This broadening of the concept of national security in recent years has been driven by a number of factors. Globalisation and trans-boundary challenges such as pandemics, climate change, cyber-attack, terrorism and proliferation of weapons of mass destruction, mean that the risks faced by modern societies extend well beyond national borders. A more detailed description of the context of New Zealand's security is provided in Annex A.

The integrated and networked character of national and international infrastructures, such as electricity, gas and water grids, telecommunications networks, air, rail and shipping services, and the extent to which daily life depends on their efficient functioning, has created new points of vulnerability.

5.9. This expanded definition is wide enough to capture nearly any activity or discussion with a political motive: 'preventing activities aimed at undermining values that underpin New Zealand society' for example. 'National security' is a term with far too wide an ambit. It would give the GCSB carte blanche to monitor and share New Zealanders' information as it wishes. No case has been made for this expansion.

5.10. The CTU recommends that the amendments to expand the grounds for storage and sharing of information under new section 25 to include "preventing or responding to threats to human life in New Zealand or any other country" and "identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country" do not proceed.

6. Information management

6.1. The CTU supports strongly supports amendments to require the GCSB to:

- Keep a register of interception warrants and access authorisations (clause 18 inserting proposed section 19). It is alarming that this does not occur already.
- Comply with privacy principles relating to the collection, usage, storage and retention of personal information as per the Law Commission's recommendations from the review of the Privacy Act 1990.

7. New Zealand Bill of Rights Act 1990 analysis

7.1. The associated Regulatory Impact Statement 'Government Communications Security Bureau Act Review' dated 22 March 2013 ('the RIS') has been released. We note however that the paper has been redacted. The scale of these redactions has not been made clear (for example through use of black lines) and it is possible that some issues have been canvassed then redacted. We must judge the RIS on what we can see however.

7.2. As released to the public, the RIS is an extremely poor piece of work. Treasury's Regulatory Impact Statement Handbook ('the RIS Handbook') states that "Generally speaking, the level of analysis undertaken (detail and depth) should be commensurate with the magnitude of the problem and the size of the potential impacts of the options being considered."[17] Given the significance of the changes proposed and the encroachment on New Zealander's rights the RIS is inadequate.

7.3. Issues of RIS quality are also particularly acute where much of the supporting information that informs parliamentary decision making is secret or classified or where a Bill is referred for consideration by a committee within a truncated timeframe. We rely upon the State services to do their analysis thoroughly as our ability to challenge their ideas is severely limited.

7.4. In considering options for change, the RIS states in relation to non-legislative options:

[17] Section 2.2, Regulatory Impact Statement Handbook available at http://www.treasury.govt.nz/publications/guidance/regulatory/impactanalysis

25. As noted above the GCSB Act is a piece of legislation that sets out and provides safeguards for the use of intrusive state powers. The GCSB cannot address any new threats beyond those it is permitted to address in its legislation.

26. The difficulties associated with the interpretation of the GCSB Act could be addressed by developing detailed guidance material, but it would be of limited benefit and consume considerable time and expenditure on legal advice to develop. This would not substantially address the need to improve management and external oversight of the GCSB.

7.5. As discussed above, we support the proposed measures to improve management and external oversight though we believe they do not go far enough.

7.6. If 'difficulties' with the GCSB Act as it stands could be remedied through non-legislative measures we believe that this option is more appropriate than legislative amendment. It should be noted that legislative amendment consumes considerable time and expenditure that likely dwarfs that in developing guidelines.

7.7. Most importantly, non-legislative amendments best square with the Government's obligations under the New Zealand Bill of Rights Act 1990. Section 21 of that Act states:

21 Unreasonable search and seizure
Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.

7.8. Crown Law's analysis for compliance with the New Zealand Bill of Rights Act 1990 notes that the proposals may have a 'chilling effect' on freedom of expression.[18]

7.9. Section 5 of the same Act states:

5 Justified limitations
Subject to section 4, the rights and freedoms contained in this Bill of Rights may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

7.10. The Government is bound to adopt the measures which create the least risk of unreasonable search or restriction of freedom of expression. For the reasons above (particularly relating to retention and sharing of information) we disagree with Crown Law's assessment that the measures are justified. The expansion of powers in the Bill does not meet this test.

[18] Section 14, New Zealand Bill of Rights Act 1990. Crown Law's analysis is here: http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/government-communications-security-bureau-and-related-legislation-amendment

8. The Office of the IGIS

8.1. The CTU approves of the changes to the Inspector-General of Intelligence and Security Act 1996 as recommended by the Kitteridge report.[19] We believe that more than a legislative solution is required however. We note the Kitteridge Report's comments on the Australian office of the IGIS:[20]

> The overwhelming impression one gets about the Office of the IGIS in Australia is that it is very muscular. All parties to whom I spoke described it consistently as robust and assertive. Agencies reported to me that they were proactive and cooperative in their dealings with the IGIS's office. It was obvious that the agencies all saw how important the oversight was for the maintenance of public trust, and that they saw the need for proactive openness and transparency with the IGIS's Office as a vital investment to maintain that public trust.

8.2. Though it is not a matter of legislative change, the CTU recommends moves to ensure that the Office of the IGIS is adequately resourced to proactively and effectively deal with issues. Office staff should include not just a Deputy IGIS but also (modelled on the Australian Office of the IGIS) former intelligence community employees, a legal advisor, review staff and administrators. This is an important step to rebuild trust given the low public confidence in the intelligence agencies generally.

8.3. As far as possible given the subject matter, justice should not only be done but be seen to be done. We support measures in the Bill bolstering the powers and responsibilities of the IGIS to undertake proactive investigations into systemic compliance issues and the provision of unclassified versions of the IGIS's reports.

9. Parliamentary oversight

9.1. The Intelligence and Security Committee, as it is currently constituted by the Intelligence and Security Committee Act 1996, provides inadequate parliamentary oversight of the New Zealand intelligence community.

9.2. We note Russel Norman's comments:[21]

> In other jurisdictions there is democratic oversight. When I have spoken to people who have been involved in the intelligence community over the years, what they have said is: "The thing we've always feared in a United States framework was that the congressional committee would pull us up and we would be forced to give testimony to the congressional intelligence committee about what we'd done, and if we'd broken the law we'd be put in jail."

[19] Kitteridge Report, [83]-[94]
[20] Kitteridge Report, [92]
[21] (8 May 2013) 689 NZPD 9657

> There is no parliamentary capacity in the New Zealand system for the Intelligence and Security Committee to force any of the agencies to give testimony. They do not have to say a word to us. We have no ability to force them to tell us what they are doing. I am a member of the Intelligence and Security Committee. We have no capacity to force the intelligence agencies to tell us whether they are acting lawfully or not. We have no capacity to force an intelligence officer to appear in front of the committee and tell us what they are doing. We have no capacity to inquire into it.
>
> If you think about it, the Intelligence and Security Committee is going to have to consider this legislation. It would be a bit like if the Social Services Committee had to consider legislation about Work and Income but it was not allowed to ask any questions about how Work and Income operates; it was not allowed to ask how the unemployment benefit is administered, or any of the other benefit systems; and it had to decide whether the legislation was good legislation or bad legislation, without knowing or being allowed to ask a single thing about how Work and Income operates.

9.3. And the comments of Phil Goff: [22]

> You also need changes to be made to the Intelligence and Security Committee. I served on that committee for 3 years. It is a farce. It does not do the job, because John Key does not let it do the job. It hardly ever meets, it does not get briefed properly, and it does not give anywhere near adequate reports to this House. It is an absolute conflict of interest that the Minister in charge of the Security Intelligence Service should be the chair of the committee having oversight into the Intelligence and Security Committee. He is the person who should be held to account. This bill says: "Oh, put the Deputy Prime Minister in or the Attorney-General." That is not good enough. Maybe we should look at the Regulations Review Committee and, like that committee, have an Opposition member chairing the committee.

9.4. The CTU recommends that changes are made to the Intelligence and Security Committee Act 1996 to ensure that:

- The committee is not chaired by the Minister in charge of the New Zealand Security Intelligence Service. It is a clear conflict of interest.
- The Intelligence and Security Committee is empowered to undertake inquiries of its own motion and to compel evidence from intelligence service employees. Appropriate security safeguards should be put in place to allow this to occur.
- Committee meetings and reports should be open to the public except where there is a compelling reason to the contrary.

[22] (8 May 2013) 689 NZPD 9657

10. Independent inquiry

10.1. We note the results of the recent One News-Colmar Brunton poll showing that 32% of New Zealander do not trust the GCSB and the Security Intelligence Service.[23] This trust is likely to have been further eroded by the recent revelations regarding the NSA's PRISM and BLARNEY programmes and the uncertainty about the New Zealand intelligence agencies' access to, involvement in, benefit from these programmes or similar ones.

10.2. The matter is further complicated by the fact that the NSA has relatively unrestricted access to a great depth of information about foreign (i.e. non-US) people including New Zealanders. This increases the concern that the information may at times be used in ways that are contrary to New Zealand's and New Zealanders' interests. The degree of dependency that New Zealand intelligence agencies have on our overseas counterparts including the NSA raises the question whether the New Zealand agencies would properly investigate and if necessary act to counter such use of information and actions that stem from it.

10.3. Given the high trust model under which these agencies operate this level of mistrust is disastrous and symptomatic of the high profile failures of management and governance highlighted in the Kitteridge Report (at least in relation to the GCSB).

10.4. The CTU strongly supports calls by Labour and the Greens for an independent inquiry into the operation of the intelligence services as a whole including a review of information gathering using programmes such as PRISM and BLARNEY.

10.5. We note the significant value of the regular independent inquiries into the Australian intelligence services.[24]

10.6. Changing legislation to legitimise previous poor practice will do the opposite: amendments to the intelligence agencies' powers should be the last step in a detailed and careful consideration.

[23] 23 April 2013, http://tvnz.co.nz/politics-news/many-kiwis-distrustful-spying-agencies-poll-5415597
[24] Flood Report (2004) http://www.dpmc.gov.au/publications/intelligence_inquiry/ and Cornall-Black (2011) http://www.dpmc.gov.au/publications/iric/index.cfm

11. Conclusion

11.1. For the intelligence agencies to retain public trust they must respect the freedom and privacy of people carrying out legitimate activities, and to the greatest extent possible be seen to be doing so. As a matter of necessity they must operate under a cloak of secrecy and they wield great power. There must therefore be particularly effective and independent scrutiny of their activities.

11.2. It appears to us (and to the public in general) that their power has not been used responsibly or fairly, and that sufficient effective and independent scrutiny does not exist. This has significantly reduced public trust. Changes in the Bill to legitimise these previous abuses and extend the ability of the GCSB to repeat them will further erode this trust.

11.3. We believe that the changes we propose will begin to rebuild public confidence in the GCSB (and the other intelligence services). We urge the Committee to consider them seriously.