# SUBMISSION OF THE CIVIL LIBERTIES COUNCILS ACROSS AUSTRALIA TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY INQUIRY INTO THE NATIONAL SECURITY LEGISLATION AMENDMENT BILL (NO 1) 2014

The councils for civil liberties across Australia (New South Wales Council for Civil Liberties, Liberty Victoria, Queensland Council for Civil Liberties, South Australia Council for Civil Liberties, Australian Council for Civil Liberties, Civil Liberties Australia) welcome the opportunity to put forward their submission on aspects of the National Security Legislation Amendment Bill (No.1) 2014 (The Bill). We welcome the Government's referral of The Bill to the PJCIS. We are grateful for the extension of time from 13 to 20 days to prepare this submission. We appreciate that the Committee has to maintain a schedule which delivers on the Government's commitment to proceed with the legislation in early September.

Nonetheless, we wish to register the impossibility for volunteer organisations such as ours to provide a detailed analysis of the 124 pages of provisions within such a time frame. Indeed, it is not possible for us to give as detailed a response as we would like on the matters that generate the greatest concern within our organisation and on which we offer comment in this submission.

A more reasonable time frame for a considered response on these proposals –given the very significant implications of some - would be in the order of at least 6 to 8 weeks.

We have therefore, of necessity, confined our comments to those provisions which cause us the greatest concern.

- Computer Access Warrants Regime
    - Definition of 'computer' and 'target computer'
    - Power to disrupt target and third party computer
    - Access to third party computers and communications
- Special Intelligence Operations
- New offences S35P
- New cooperative arrangements between ASIO and ASIS

## 1. GENERAL COMMENTS

The CCLs accept that ASIO and other intelligence and security organisations must have the powers and resources necessary for the protection of national security including protection against the very real threat of terrorist activity in Australia- consistent with democratic values. We support the modernisation and appropriate streamlining of national security legislation including the ASIO Act 1979 to ensure that the agencies are not hindered by outdated legislation in the face of massive and fast moving technological change particularly in the communications arena. However, where the proposed changes expand existing ASIO powers and/or weaken balancing safeguards and protections our endorsement is dependent upon persuasive evidence justifying such changes and clear demonstration that rights and liberties are not being unwarrantedly or disproportionately encroached upon.

**In our view, such persuasive evidence has not been provided to justify some of the new or enhanced security powers being proposed in this Bill.**

### 1.1. Human Rights implications

The Bill implements most of the recommendations from Chapter Four of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) June 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. These changes include significant extensions to the powers of the Australian Security Intelligence Organisation (**ASIO**) to gather intelligence and collaborate with other organisations.

Important liberties and human rights are often at stake when enhanced security and counter-terrorism laws are under consideration. The Explanatory Memorandum identifies eight human rights that are engaged by the Bill's provisions and in relation to which Australia has international law obligations. [1] The CCLs are particularly concerned with the impact of the Bill's provisions on two of these:

- the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)
- the right to freedom of expression in Article 19 of the ICCPR

In the absence of an Australian Bill of Rights or Human Rights Charter, it is incumbent on the Government to provide robust justification for any encroachments on these recognised human rights and liberties. The failure of the Government – and specifically the Department of the

[1] Explanatory Memorandum to the National Security Legislation Amendment Bill (No 1) 2014 (EM 2014) Page 6

Attorney-General– to provide credible justification for obvious encroachments in the 2012 review of the Potential Reforms of National Security Legislation was a common criticism- and was criticised strongly by civil liberties and human rights groups.[2]

It is therefore particularly disappointing and totally unacceptable that this Bill is being progressed with minimal improvement. Under the ICCPR, each of the rights can be limited, but only in particular circumstances and to the extent necessary. The amendments in the Bill need to be advanced on the basis of rigorous evidence and after weighing the benefits of the proposal against the human rights impacts.

The justifications that are advanced in the Explanatory Memorandum and the Department of the Attorney-General's Submission to this Inquiry to establish that the various encroachments on rights are permissible and compatible with our obligations are, in the main, superficial and tokenistic. The assessment rarely goes beyond rhetorical assertion in relation to necessity, reasonableness and proportionality.[3] (The PJCIS 2012 report does in places provide more substantial contextual information to support its assessments of the proportionality of some encroachments.)

We will address this failure in the discussion of relevant provisions. It is particularly evident in multiple encroachments- some of which are very serious- on the right to privacy.

The right to privacy is fundamental to human dignity and autonomy. It enables individuals to live their lives without experiencing the restraining effect of government scrutiny. A meaningful guarantee of privacy is necessary for the exercise of civil liberties such as freedom of expression and freedom of association. The right to privacy is also important at a broader societal level to ensure that the potential for scrutiny does not stifle intellectual freedom and debate.

The potential for unnecessary and disproportionate invasion of large numbers of non-suspect persons' privacy is a central concern of the CCLs with key provisions in this Bill. This concern is exacerbated by a corresponding lack of attention to appropriate safeguards and protections. Inadequate consideration has been given limiting the impact on individuals' privacy and other rights and to ensuring effective accountability in the exercise of enhanced powers.

## 2. COMMENTS IN RELATION TO SPECIFIC PROVISIONS

### 2.1. Schedule 2 Powers of the Organisation: computer access warrants regime

The linked issues of ASIO's powers granted by a computer access warrant and the general definition of 'computer' and the specific 'target computer' are matters of significant concern to the CCLs.

[2] For example NSWCCL Submission to PJCIS Inquiry Into Potential Reforms Of The National Security Legislation 21 August 2012 (NSWCCL submission 2012) P6.
[3] A diagrammatic summary of a standard approach to the assessment of proportionality of reforms provided to the PJCIS during the 2012 inquiry is at Attachment A

The CCLs accept that there is a need to ensure that ASIO is not hindered from doing its job by dated and inappropriately constricted definitions of a computer and we have no objection to streamlining the warrant application process to remove inefficiencies- if there are no other implications. As it stands, the combined impact of the proposed amendments to S22 (Interpretations) and S25 (Search warrants) and S25A (Computer access warrant) is a disturbing and unjustified overreach with profound implications for the privacy of large numbers non-suspect persons.
Currently the 'Minister is only to issue the warrant if he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a particular computer (the ***target computer***) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the ***security matter*** ) that is important in relation to security.' S25A(2)

### 2.2. Definition of 'computer' and 'target computer'

The current definition of 'computer' in the Act is: 'a computer, a computer system or part of a computer system.' S22.

The proposed expansion of this definition to include computer networks was a highly contentious issue in the context of the 2012 inquiry by the PJCIS. Commentators and many of the submissions at the time pointed out the expansive ambit of a 'network' of computers ranging from a home network to a university or business network to the global network of the internet. NSWCCL noted the impossibility of understanding what was intended by such an unclear and open-ended definition.[4]

The PJCIS report quoted from a number of submissions - including from the Australian Privacy Foundation and Inspector General of Intelligence and Security - cautioning against such an open-ended definition. Nonetheless, it recommended that the definition be amended to include 'multiple computers operating in a network'. R20.

Not surprisingly therefore the proposed amendment in the Bill dramatically expands the current definition to: 'all or part of: (a) one or more computers; or (b) one or more computer systems; or (c) one or more computer networks; or (d) any combination of the above.' (Item 4)

We accept that 'the capability of ASIO should not be degraded by the definition of computer in the ASIO Act being obsolete'.[5] However, neither the PJCIS recommendation nor the Bill's proposed definition is acceptable. They both permit the ultimate expansive definition of all computers connected to the internet -and anything in between including local area networks, peer- to-peer networks, public Wi-Fi hotspots and corporate extranets.

Any casual perusal of current definitions of 'computer network' establishes that it incorporates anything up to, and including, the whole of the internet. For example: 'When you have two or more

[4] NSWCCL Submission 2012
[5] PJCIS Report of the Inquiry into Potential Reforms of Australia's National Security Legislation May 2013 (PJCIS Report 2013) p88

computers connected to each other you have a network……The internet could be described as a global network of networks'[6]. Or: 'You see, the Internet is a large network of inter-connected computers" [7]

The PJCIS recommendation 20 had a second dimension which may have been intended to place some stronger boundaries around the definition of a computer network. It recommended that the warrant provisions authorising access to a target computer 'may extend to all computers at a nominated location and all computers **directly associated** with a nominated person in relation to a security matter of interest'. [8] (CCL's emphasis)

The proposed amendment in the Bill includes a looser definition of the target computer: ' a computer associated with, used by or **likely to be used by**, a person (whose identity may or may not be known).' S25A(3). (CCL's emphasis) This remains open-ended. If the internet is a 'network' most suspects would be likely to be using it.

It is obviously not intended to give ASIO access to all computers on the internet, or, hopefully, within a university or large business on the basis of a single warrant. Nonetheless, the proposed definition is clearly open to this interpretation.

It is somewhat surprising, given the high level of concern expressed around this issue during the previous review process, that the drafting has not been able to develop a less ambiguous and less expansive definition of 'computer' and 'target computer' to equip ASIO with the capability of accessing computers where reasonable grounds exist to suggest they hold data 'that is important in relation to security'.

As currently drafted, it allows for extraordinary and disproportionate invasion of the privacy of unknown numbers of non-suspect persons.

A tighter and clearer definition of a computer network must be developed or alternative terminology developed to set unambiguous boundaries as to the computer, computers or groups of computers covered by the access warrant, including limits on how wide a location can be specified.

Access should not be permitted to any computer or computers unless reasonable grounds can be established for believing they hold data of importance in relation to security and that the target person had use of or access to these computers.

[6] Online Tech-Terms.com
[7] Example sentence for definition of 'a computer network", oxforddictionaries.com
[8] PJCIS Report 2013, P89

In addition, there should be a stronger burden of proof required for access to multiple computers beyond those on a household or local network. A two tier warrant system would deliver a better safeguard.

A redrafted definition and warrant provision should be subject to further public and expert consideration before being progressed in Parliament.

### 2.3. Power to disrupt target and third party computer

The Bill amends section 25A so that the level of permissible disruption of the target and third party computer is significantly increased.

Currently ASIO cannot add, delete or alter data on a target computer, interfere with the 'lawful use 'of the target computer or cause any loss or damage to others lawfully using the computer. The amendment weakens this restriction to '**materially'** interfere with etc and cause **'material** loss or damage' to other persons lawfully using the computer. This limitation is further weakened by the exception provision: 'unless it is otherwise necessary to execute the warrant'.

The justification for this amendment is that the current restrictions 'can prevent ASIO from effectively executing a search warrant or a computer access warrant as they prevent a warrant from authorising even minor interferences or disruptions. They also create uncertainty if it is not possible to determine whether an act may cause a disruption.' [9]

The CCLs accept that it is appropriate to amend this tight restriction so an access warrant can be issued permitting minor interference and disruption to the target computer.

The CCLs are, however, concerned that the Bill will permit ASIO to disrupt a target and third party computer or computer networks as long as the interference and loss or damage is not 'material' with all access warrants- and cause 'material' loss or damage if it is necessary to access the computer.

If this is the intended outcome of the amendment, this open ended ('material') level of disruption has not been justified and for third party computers is disproportionate.

Apart from the impact on privacy, the CCLS note the warnings of IT experts as to the high level of risk in relation to unintended and serious consequences in permitting this kind of disruptive activity by ASIO.

The Bill should specify a less imprecise and open ended limitation to protect the level of permissible disruption –especially to third party computers.

[9] Attorney-General's Department Submission to The Parliamentary Joint Committee On Intelligence And Security Inquiry Into The National Security Legislation Amendment Bill (No 1) 2014 (AG Submission 2014) p2

The CCLs also suggest consideration be given to limiting the type of data that may be collected or interfered with as a safeguard against arbitrary interference with privacy. Other accountability measures which should be considered include:

- Limiting the power to specified categories of third parties (currently the Bill allows access to 'any other computer or communication in transit');
- Creating a duty to notify third parties of the use at an appropriate time; and
- Creating a duty to rectify any interference made with a third party computer.

### 2.4. Access to third party computers and communications

The Bill will allow ASIO to use any third party computers or communications 'in transit' to access a suspect's computer and if necessary to add, copy, delete or alter other data in the computer or communication. These amendments have the potential for far-reaching privacy consequences for innocent people. They will increase the incidental power of a warrant to interfere with the privacy and civil liberties of persons not named in the warrant.

While the CCLs accept that there may be contexts in which it is necessary to access third party computers in transit to the target computer the safeguards are not adequate. Under the bill, ASIO will be able to access third party computers or communications whenever it is 'reasonable in all the circumstances to do so', having regard to other methods of obtaining access to the target computer which are likely to be as effective.[10]

This is a vague, low threshold for a significant intrusion into the privacy of a non-suspect person's computer. The AG Department submission argues that these safeguards are appropriate because the IGIS has oversight of the use of these provisions and ASIO must follow the Attorney-General's Guidelines which require ASIO to use as little intrusion as possible.[11]

As drafted, this will not require ASIO to first exhaust other methods of accessing the target computer although the PJCIS recommendation (R22) indicates this should be a condition-in that it recommends safeguards should be consistent with the existing provisions under the Telecommunications (Interception and Access) Act 1979. The explanation provided for not abiding by the PJCIS recommendation is that exhaustion of all other methods was looked at, but was 'considered too limiting'.[12] This is not sufficiently informative to constitute a serious justification for non-inclusion of a significant safeguard.

The CCLs would like to emphasise that operational convenience is not a sufficient reason to infringe on human rights. The use of a third party computer or communication in transit should not just be

[10] National Security Legislation Amendment Bill (No.1) 2014, Schedule 2, Item 23 inserting new paragraph 25A(4)(ab) of the ASIO Act.
[11] AG Submission 2014, p5
[12] ibid

reasonable, but necessary and proportionate. As pre-requisite for exercise of powers of access to a third party computer those exercising the power ought to be able to demonstrate that such access would result in substantial operational and security benefits and that all other methods of accessing the target computer have been exhausted.

### 2.5. Scope of incidental power to enter third party premises

The CCLs consider entry into a third party's premises involves a significant invasion of individual privacy and should not be treated as an 'incidental' issue. It is a significant exercise of power in its own right and must be subject to appropriate safeguards.

The Bill will permit access to *any* premises for the purposes of executing a warrant.[13] Access to third party premises should be limited to premises specified in a warrant. Requiring ASIO to identify which third party premises they will need to access provides an important safeguard.

The CCLs consider that the use of third party premises should be limited to situations where:

- There is a high likelihood of an offence being committed by the suspect;
- Use of a third party premises is necessary to access a target premises; and
- Interference with the third party premises would be minimised as much as possible.
- Creating a duty to notify third parties of the access at an appropriate time; and
- Creating a duty to rectify any interference made with the third party premises.

### 2.6. **Special Intelligence Operations**

The Bill proposes a new statutory framework for the conduct by ASIO of special intelligence operations (SIOs) based on the controlled operations regime in Part IAB of the *Crimes Act 1914* (Crimes Act) in relation to activities of the Australian Federal Police. The regime will provide ASIO officers and affiliates with immunity from criminal and civil liability when operating in an authorised SIO.

This is a very significant amendment to the safeguards relating to ASIO's operations and brings with it considerable risk. In our view such a significant change requires strong justification from the Government.

The Explanatory Memorandum states that 'some significant investigations either do not commence or are ceased due to the risk that an ASIO employee or ASIO affiliate…. could be exposed to criminal or civil liability.' [14] As there is no information as to how many

[13] National Security Legislation Amendment Bill (No.1) 2014, Schedule 2, Item 10 inserting new paragraph 25(4)(aa) of the ASIO Act.

[14] EM p14 Par54

'significant' investigations have not commenced or have ceased for this reason it is not possible for us to assess how powerful a justification this is.

There is also the implication that, as such immunity exists for the AFP in controlled operations, it is obviously unproblematic to extend it to ASIO officers. Thus the Attorney-General argued that it is appropriate to extend 'corresponding protections' available to AFP to participants in 'covert intelligence operations.'[15]

On the face of it, this argument is plausible. We accept that ASIO officers need to work covertly and that there will be some contexts in which intelligence gathering and terrorism investigations may require the commission of unlawful acts. However, there are deeper and more important issues at stake with this proposal and the CCLs on reflection, consider the proposed SIO regime unnecessary, dangerous and inappropriate for a domestic intelligence agency.

It is not appropriate to presume that powers appropriate for the AFP as a law enforcement agency are automatically appropriate for ASIO. Law enforcement agencies operate more visibly, are subject to accountability through the criminal trial process and sit in a different administrative position from ASIO. The latter is – of necessity - a far more secret organisation.

It is not necessary, because ASIO has strong collaborative arrangements with the AFP who are able to conduct these covert operations for them exercising their powers and immunities under the controlled operations regime. We presume this would be possible in most contexts. In any context where AFP collaboration may not be possible, ASIO officers can operate covertly and avoid unlawful acts- or if unlawful acts are necessary, they can seek the discretionary power of the Director of Public Prosecutions (DPP) to not prosecute. It is difficult to envisage a context in which the DPP would not exercise this discretion if ASIO officers had reasonable justification for their unlawful actions. While there may be a slight risk factor for ASIO in relying on this protection from prosecution, this may not be a bad thing. It imposes an independent safeguard that covert, unlawful actions are appropriate and essential for the intelligence task.

We note that similar intelligence agencies in the United Kingdom, New Zealand and Canada do not have immunity from criminal and civil liability.

[15] Commonwealth Parliament *Parliamentary Debates* 16th July 2014. 2R speech ,Senator Brandis

The CCLs are deeply uneasy with the proposed SIO regime for ASIO and do not support its implementation.

We do note however, that the PJCIS report in 2013 does recommend the creation of an SIO regime…' ' (R 28).

The CCLs urge the PJCIS to reconsider this recommendation.

If the SIO regime is implemented, it is of critical importance that strong safeguards apply. The PJCIs was explicit that its support for SIOs was : 'subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the Crimes Act 1914.'(R28)

While there are safeguards embedded in the Bill, they are not as strong as those that apply to the AFP controlled operations regime. In our view, the safeguards for an immunity regime encompassing covert operations of a domestic intelligence agency should be at least as strong as those applying to the APF.

Most significantly, the APF controlled operations regime activates an external independent check if the duration of the operation is to be extended beyond the initial 3 months authorised period. While the Commissioner or Deputy Commissioner can authorise the initial period, renewal after 3months requires authorisation by the Administrative Appeals Tribunal.

The CCLs urges that a similar independent, and external to ASIO body, exercises renewal authorisations for SIOs after the first three months.

The AFP controlled operations authorisations must be renewed after 3 months and have a maximum duration of 24 months. The SIO authorisations are for up to 12 months and can be renewed internally indefinitely. The intervention of an independent body to authorise SIO extensions is very important to place effective checks on their duration.

As with other extraordinary new ASIO powers, the CCLs consider this provision should be subject to review and a sunset clause after three years.

### 2.7. New offences S35P

The Bill introduces two new offences relating to unauthorised disclosure of information relating to an SIO.[16] Under the current wording, the unauthorised disclosure offences would apply to

[16] National Security Legislation Amendment Bill (No.1) 2014, Schedule 3, Item 3 inserting new Division 4 into the ASIO Act. The new offences will be in new Section 35P.

disclosures by ***any person*** including persons who are *recipients* of an unauthorised disclosure. They will carry maximum penalties of five years' imprisonment, and ten years for an aggravated offence.

The first offence is exceptionally broad and is of major concern.

CCLs understand the need for secrecy in relation to certain intelligence gathering operations. However, the Bill fails to draw an important distinction between disclosures which undermine the effectiveness of particular operations and endanger the lives of those involved in them, on the one hand, and on the other, public interest disclosures, for example those regarding any aspect of ASIO activity generally which might legitimately be considered a cause for concern.

The Bill provides for very limited defences largely relating to legal obligations to disclose or to the performance of ASIO functions. As a result, these provisions could, for example, be used to prosecute journalists who report in the public interest on information they receive about SIOs. The person may not be aware that the information relates to an authorised SIO. They can be convicted on the basis of recklessness if the person is aware of a substantial possibility that the information is in any way connected to an SIO. The penalty is five years.

This offence is particularly concerning because of the very broad range of activities that fall within the scope of SIOs. Under the amended ASIO Act , an 'SIO' will mean an operation for which SIO authority has been granted by the Director-General of Security or the Deputy Director-General, 'is carried out for a purpose relevant to the performance of one or more special intelligence functions' and 'may involve an ASIO employee or an ASIO affiliate in special intelligence conduct'.[17]

This extremely broad definition may catch activities that, if disclosed, could reveal serious government wrongdoing without posing a security threat.

It is the view of the CCLs that no agency of the state should be shielded from public scrutiny in this way. We are concerned that in addition to preventing publication of information which is harmful to Australia's national security interests, the new offences could be used to prevent or deter publication or disclosure of important information regarding the use and misuse of official power that is essential to the proper functioning of a democratic state.

The CCLs oppose the creation of this offence.

It will have- and appears intended to have- a major deterrent effect on legitimate whistle-blowers, on the freedom of the media to report on abuses of power by ASIO and on debate relating to intelligence and counter terrorism issues. More broadly, and when considered in conjunction with the increased penalties and new offences applying to unauthorised disclosures by ASIO employees

[17] National Security Legislation Amendment Bill (No.1) 2014, Schedule 3, Item 1 amending Section 4 of the ASIO Act.

and contractors proposed in schedule 6, these provisions will have a chilling effect on the operation of democracy in this country.

**Cooperation between ASIO and ASIS**

**Piecemeal approach to counter-terrorism and national security reforms**

## 3. SUMMARY OF CCLS' POSITIONS AND RECOMMENDATIONS

3.1. Persuasive evidence has not been provided to justify some of the new or enhanced security powers being proposed in this Bill.

### 3.2. Compatibility with human rights

The justifications that are advanced in the Explanatory Memorandum and the Department of the Attorney-General's Submission to this Inquiry to establish that the various encroachments on human rights are permissible and compatible with our obligations are, in the main, superficial and tokenistic.

### 3.3. Definitions computer and target computer

As currently drafted, the definitions of a computer and of a target computer too ridiculously expansive and will allow for extraordinary and disproportionate invasion of the privacy of unknown numbers of non-suspect persons.

A tighter and clearer definition of a computer network must be developed or alternative terminology developed to set unambiguous boundaries as to the computer, computers or groups of computers covered by the access warrant, including limits on how wide a location can be specified.

Access should not be permitted to any computer or computers unless reasonable grounds can be established for believing they hold data of importance in relation to security and that the target person had use of or access to these computers.

In addition, there should be a stronger burden of proof required for access to multiple computers beyond those on a household or local network. A two tier warrant system would deliver a better safeguard.

A redrafted definition and warrant provision should be subject to further public and expert consideration before being progressed in Parliament.

### 3.4. Power to disrupt target and third party computer

The Bill should specify a less imprecise and open ended limitation to protect the level of permissible disruption –especially to third party computers.

Consideration be given to limiting the type of data that may be collected or interfered with as a safeguard against arbitrary interference with privacy. Other accountability measures which should be considered include:

- Limiting the power to specified categories of third parties (currently the Bill allows access to 'any other computer or communication in transit');
- Creating a duty to notify third parties of the use at an appropriate time; and
- Creating a duty to rectify any interference made with a third party computer.

3.5. Access to third party computers

As pre-requisite for exercise of powers of access to a third party computer those exercising the power ought to be able to demonstrate that such access would result in substantial operational and security benefits and that all other methods of accessing the target computer have been exhausted.

**3.6. Special Intelligence Regime**

The CCLs are deeply uneasy with the proposed SIO regime for ASIO and do not support its implementation.

The CCLs urge that an independent and external to ASIO body, exercises renewal authorisations for SIOs after the first three months as is the case with the AFP controlled operations regime .

As with other extraordinary new ASIO powers, the CCLs consider this provision should be subject to review and a sunset clause after three years.

**3.7. New SIO offences S35P**

The new non-aggravated offence is exceptionally broad both in its application to 'any person' and the very wide scope of ASIO activities that are captured and therefore raises major civil liberties and human rights concerns.

In addition to preventing publication of information which is harmful to Australia's national security interests, the new offences could be used to prevent or deter publication or disclosure of important information regarding the use and misuse of official power that is essential to the proper functioning of a democratic state. No agency of the state should be shielded from public scrutiny in this way.

The CCLs oppose the creation of this offence.

## 4. Concluding comments

It had been our intention to provide comments relating to the proposed new cooperative arrangements between ASIO and ASIS but the time has not permitted this. We will submit some supplementary comments registering our strong concerns about this proposal.

We also intended making some strong observations on the Governments approach of introducing important security and counter-terrorism legislation in piecemeal tranches. As we were preparing our responses to this significant package of proposals, the Government had begun a media blitz announcing what appears to be two more tranches of very significant and controversial counter-terrorism proposals. This is a confusing and unhelpful approach. The national security and counter-terrorism legislation is large and complex and much amended body of law. It is obviously a far more effective to bring all the proposed amendments forward at the same time. This allows the community and the parliament to gain a more coherent understanding of the cumulative impact of all proposed changes.

As it now appears that all foreshadowed changes will be coming forward over the next parliamentary session, there is no good reason for not proceeding in this more orderly and measured way.

The CCLs have one further recommendation.

The current National Security Legislation Amendment Bill (No1) 2014 not proceed at this time but be considered in the context of foreshadowed further amendments relating to meta data-retention and other new counter-terrorism laws.

The CCLs have collaborated on this submission because of the obvious national importance of changes to the powers of ASIO and the potential for major impacts on civil liberties and rights.

We hope our submission is of assistance to the PJCIS and the Government. We are very willing to take up the invitation to elaborate on this submission and offer brief supplementary comments at the planned public hearings next week.

This submission was written by Dr Lesley Lynch NSWCCL and members of Liberty Victoria's *Young iberty for Law Reform* and is endorsed by the councils for civil liberties across Australia.

Significant contributions were made by Dr Martin Bibby, NSWCCL. *Liberty Victoria would like to acknowledge Gerson Hernandez, Sarah Mercer, Gram Morris, Natasha Nguyen and Dale Straughen, members of Liberty's Young Liberty for Law Reform initiative, for their research and assistance in preparing this submission.*

**Contact in relation to this submission**
**Dr Lesley Lynch**
**Secretary NSW Council for Civil Liberties**

**Attach 1 Proportionality test diagram: LibertyVictoria**

**Attachment 1: Overview of Proportionality Test**

The proportionality test is a tool for assessing the extent to which laws or proposed laws limit human rights and the extent to which that limitation is proportionate to the aims sought to be achieved. The proportionality test may assist the Committee in determining whether the National Security Reforms achieve an appropriate balance between the needs of law enforcement and national security on the one hand, and the protection of the human right to privacy and other human rights, on the other hand.

The diagram below shows the process involved in applying the proportionality test.