Submission No 95

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Ian Quick

Dear members of the Joint Parliamentary Committee on Intelligence and Security.

While I was alarmed to see the reports in the media about the proposal to log everyone's internet access, I was significantly more alarmed when I read the complete terms of reference and discussion paper that have been put out for public comment.

It has clearly been written with little effort to justify many of the proposed significant changes, and has no regard to how decisions on security issues should be made - it reads as typical bureaucratic whitewash with the odd sensible comment.

Specifically, **every** suggested change should be looked at it terms of

1. Exactly what is proposed
   Many of the items raised are not detailed enough to understand exactly what the end result would be.

2. Cost, in a wide sense, including
   a. Individual impact on human rights and privacy.
   b. Loss of amenity (etc) to society as a whole.
   c. Monetary impact.

3. Oversight requirements, including
   a. How effective the *current* arrangement is.
   b. How the proposed oversight is to be implemented, and how effective it will be, including how it could be avoided or misused (ie defeated).

4. Effectiveness, including
   a. What will the proposal accomplish?
   b. What will the side effects be?
   c. How could it be abused?

5. Benefits, including
   a. To the various departments, both cost and effectiveness.
   b. To society as a whole.

All Security is a trade off between 'costs' and 'benefits' – the discussion paper mentions a number of benefits but does not address the many costs or impacts.

As a result, the impression is that all the changes are good and should be done, however this would be true for any suggested changes if only the benefits were listed! ie with exactly the same approach the paper could have suggested mandatory id cards, evening curfews, and requiring permits to travel within Australia – all things that would help the 'security' of the nation and in combating crime.

However, most Australians would say the costs of these measures would be too high a price to pay for the extra 'security' provided.

I have put quotes around 'security' above, as past a certain point too much (or poorly controlled) 'security' by the government results in less security for citizens as a whole – ie 'police states' are about the least secure environment to live in.

If we want to live in a relatively free democratic society – as Australia has largely been to date – increasing the powers of our security agencies should only been done in the light of a clear need and balanced against costs and all of the other issues.

It is certainly clear from the discussion paper that security agencies *want* more power, the question is do they really *need* it and is it worth the price?

Parts of the discussion paper effectively argue against this – as no major terrorist plot has succeeded in Australia since 9/11 and the four attempted ones have been stopped with the *current* powers. The many prosecutions mentioned have occurred with the *current* laws, often there appears to be little justification for extending the agencies powers apart from that it will make it easier on them – which does not necessarily outweigh the costs (in a broad sense) of what they are asking for.

Don't get me wrong, if they *do* need extra powers, have a clearly demonstrated need, clearly identified cost, and sensibly reviewed the issue, it may be additional powers are warranted. However, you simply can't tell on many of the issues raised as there is not enough detail. With others it is difficult to tell if they are reasonable or not as it may depend on specific implementation details – missing from the discussion paper or glossed over, such as many of the oversight requirements.

Many issues raised in the discussion paper clearly need to be addressed, however they need to be investigate in much more detail, with other options explored.

For the rest of my submission I'll look at specific issues that concern me from the proposals. However generally, as above, I find the tone of the proposed changes and the poor discussion paper worrying. Section (3)(a) from the terms of reference was largely ignored throughout the paper ie

> *"contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector*"

My strong recommendation to the Committee is that it considers the public submissions and then creates a new discussion paper that covers each issue far more rigorously – which could be put out for another round of public comment.

I'd also recommend that every committee member reads "Beyond Fear' by Bruce Schneier before making any recommendations on the proposed changes.

I am of course happy to appear before the committee.

Ian Quick
19/8/2012

Part B – Summary of issues from the terms of reference.

Of the 18 proposals, I support 6 of them (6, 7, 8, 10, 13, 16, 18) subject to some implementation details, have not commented on 2 (9,14), and oppose the remaining 10 proposals.

I partly oppose many due to how little thought had gone into the discussion paper, how badly some of the issues were presented and discussed, including an almost total absence of discussion of costs, impacts and oversight.

In many cases there appears to be a valid issue that needs to be discussed and possibly addressed – however the proposed solution does not appear to be the best one from the information provided, taking more than just the 'benefits' into account.

It was also worrying to read a few motherhood statements in the discussion paper along this line ie

> *"At the same time, it is important that legislation governing intelligence agencies continues to include appropriate checks and balances on the exercise of their powers. Ensuring these agencies remain accountable for their actions helps to maintain public confidence in and support for the crucial work of intelligence agencies."*

Which are then promptly ignored in the evaluation of most of the proposals.

In at least one case (proposal 1) the recommendation does the opposite of what the proposal stated, in other cases the ramifications of what is suggested is not even lightly investigated.

It is clear that most of the discussion paper was written with a one sided objective in mind with no attempt to look at many of the issues from an objective – or society wide – point of view, which is extremely disappointing.

Part C – Looking at the proposals from the terms of reference in more detail

> *"1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the Telecommunications (Interception and Access) Act 1979 (the TIA Act). This would include the examination of:*
>
> *a. the legislation's privacy protection objective*
> *b. the proportionality tests for issuing of warrants*
> *c. mandatory record keeping standards*
> *d. oversight arrangements by the Commonwealth and State Ombudsmen"*

While the heading for this proposal seems quite reasonable, the details in the discussion paper seem to be ignoring the word "Strengthening".

Specifically,
(a) the legislation's privacy protection objective
The discussion paper states -

> *"Historically, the TIA Act has protected the privacy of communications by prohibiting interception except as allowed under the Act.*"

This – as it stands – is a good way to protect abuse of privacy. The default is that it **can't** be done, which is much safer than the opposite ie if something **can** be done **unless** forbidden it is rapidly open to abuse and interpretation, and over time will become less and less effective.

It is **not clear** what the discussion paper is suggesting as an alternative, however it states -

"consideration is also being given to introducing a privacy focused objects clause that clearly underpins this important objective of the legislation and which guides interpretation of obligations under the Act."

However, this - ie swapping from a clear proscriptive rule of what can be done to a vague rule of 'objectives' that need to be 'interpreted' - is that this is actually a significant **weakening** of actual privacy outcomes.
This is true for most laws – prescriptive ones work much better than ones that are merely 'objectives' – just look at planning law in Victoria, where everything is up for grabs by arguing in court about what the objectives mean, and if they have been met.

I strongly encourage maintaining proscriptive laws to protect privacy, and if more exceptions need to be added they should be on a case by case basis.

(c) mandatory record keeping standards
The discussion paper does make a good case for change in this area. However, the proposed solution is worrying –

> *"Consideration should be given to introducing new reporting requirements that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes."*

The problem with this is the same as (a) above, **less process oriented** is more open to abuse and interpretation. Instead, the reporting requirements still need to be prescribed, but should probably be expanded to cover a number of scenarios.

It's disappointing that the discussion paper did not address the terms of reference for this issue, as proposal (1) was not about making it easier for the security services – it should have been about strengthening protection!
As a result, I do NOT support proposal 1.

"2. Reforming the lawful access to communications regime. This would include:
a. reducing the number of agencies eligible to access communications information
b. the standardisation of warrant tests and thresholds "

The discussion paper makes a good point on these issues, and its recommendation seems reasonable, ie –

> *"Implementing a standard threshold for both content and stored communications warrants would remove the complexities inherent in the current interpretation of what is a serious offence, recognise the growing number of online offences and provide consistent protection for 'live' and 'stored' content. Consideration is also being given to reducing the number of agencies able to access communications information on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so."*

However, it does **not** state what thresholds it is suggesting, how it is to be simplified, and how agencies would demonstrate need. Without these details it is impossible to tell if this is an acceptable change or not.

As a result, I do NOT support proposal 2.

"3. Streamlining and reducing complexity in the lawful access to communications regime. This would include:

a. simplifying the information sharing provisions that allow agencies to cooperate

b. removing legislative duplication"

The discussion paper states

"The use and disclosure of information obtained from exercising powers under the TIA Act is strictly regulated."

Correct, and it was set up this way for **very good reasons**.

I understand the issues raised in the discussion paper, but the proposed solution should not be accepted, ie

"Simplifying the current information sharing provisions would support cooperative arrangements between agencies and consideration could be given to the ways in which information sharing amongst agencies could be facilitated."

And

"Consideration should be given to introducing new reporting requirements that are less process oriented and more attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes."

Removing the current strict regulations and performing weaker reporting (as above, ie 'process' instead of 'proscriptive', as discussed in other points) is **not** the solution to the issues raised.

I understand why the agencies don't like the current laws, however moving to a more general 'free for all' – which is what is normally achieved from 'simplifying' processes – and less reporting is not the way to go.

Similarly with removing 'duplicate' legislation – in theory it sounds fine, in practice the least restrictive legislation would probably be picked to replace all the 'duplicates' – though there is not enough detail in the discussion paper to tell if this would be the case (it has been in other government processes I've seen).

Far more work needs to be done looking at options for addressing these issues before the current arrangements are to be changed in any way.

As a result, I do NOT support proposal 3.

"4. Modernising the TIA Act's cost sharing framework to:
a. align industry interception assistance with industry regulatory policy
b. clarify ACMA's regulatory and enforcement role"

This appears to be a proposal to make the industry pay more of the costs associated with interception, and to give the ACMA more power to tell the C/CSP's what to do, in a less open way.

This is a classic case of 'externality' ie the person getting the 'benefit' is not paying the 'cost', resulting in the person with the benefit wanting more and more. A real test of what the agencies really **need** for interception capability would be if **they** had to pay for it!

A significant advantage of the current ACMA's power – going to court– is that it is public and open to scrutiny. If, as the discussion paper suggests –

> *"The ACMA's role could be reinforced by expanding the range of regulatory options available and clarifying the standards with which industry must comply."*

it would be possible – though the paper does not say what the 'options' are – that the ACMA could quietly push a C/CSP into doing something it did not want to do. While this may be alleviated by clear standards, **any** option it has should be open to public scrutiny.

As a result, I do NOT support proposal 4.

"5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions
a. to update the definition of 'computer' in section 25A
b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months."

a. to update the definition of 'computer' in section 25A

While clearly this issues needs to be addressed, the suggest approach opens up a number of issues

ie

> *"A possible solution to this issue could be to amend the ASIO Act so that a computer access warrant may be issued in relation to a computer, computers on a particular premises, computers connected to a particular person or a computer network."*

For a specific computer this is clear, but if a warrant is expanded to include all on a 'premises' how wide could this be? Could a single warrant cover all computers at BHP headquarters? All computers at a university? What will be the controls on issuing such warrants be?

A 'computer network' is even more worrying. How is the network defined? Everything the person **could** access anywhere on the internet? Everything on their 'local' (on the premises) network? Where exactly would the warrant boundaries be, given that it could be argued that the bulk of computers on the planet are on the same 'network?

"b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months."

While I understand why not being able to vary warrants must be annoying to the agencies, it was originally done for good reasons and there is nothing in the discussion paper stating what the very good reasons would be for changing it.

The obvious problem caused by allowing the varying of warrants - without the initial full process - is at least 'bait-and-switch' and 'Foot-in-the-door' issues (not even discussed in the paper), and there is no evidence presented that changing the current arrangement of having to go through the full warrant process for changes isn't out weighed by the potential problems if agencies don't have to.

The renewal process has the same problems, ie

> *"In such circumstances, ASIO must apply for a new warrant which necessitates restating the intelligence case and completely reassessing the legislative threshold in instances where there has not been a significant change to either, and where the assessment of the intelligence case remains unchanged. A renewal process would provide appropriate oversight and accountability without requiring excessive administrative resources."*

If all warrants are extended to 6 months as suggested then surely it is reasonable to have to go through the same justification to have them renewed as originally issued? There is nothing in the discussion document saying **what** the renewal process would be and **why** it would provide appropriate oversight, particularly as it would then make warrants effectively **open ended**. Short of convincing details, this proposal should not be agreed to.

As a result, I do NOT support proposal 5.

http://en.wikipedia.org/wiki/Bait-and-switch
http://en.wikipedia.org/wiki/Foot-in-the-door_technique

"6. Modernising ASIO Act employment provisions by:

a. providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'

b. Making the differing descriptions ('officer,' 'employee' and 'staff') denoting persons as an 'employee' consistent

c. Modernising the Director General's powers in relation to employment terms and conditions

d. Removing an outdated employment provision (section 87 of the ASIO Act)

e. Providing additional scope for further secondment arrangements

Intelligence Services Act 2001"

Looks fine to me (though I may have missed something..).

Thus I do support proposal 6.

"7. Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies."

As per proposal 6.

.

Thus I do support proposal 7.

"8. Streamlining and reducing complexity in the lawful access to communications regime – this would include:

a. Creating a single warrant with multiple TI powers"

As stated on one of the proposals above, generally when it is stated that something is going to be 'streamlined' extreme care should be used in examining what is proposed. This is particularly relevant as proposal (1) was effectively ignored by the discussion paper.

However, in this case it appears (on the details available) that the specific proposal (8.a) is reasonable ie

"…by enabling ASIO to apply for a single warrant covering all ASIO Act warrant powers where the relevant legislative thresholds are satisfied."

As long as it is **all** the relevant legislative thresholds, which is implied - but should be stated.

Thus I do support proposal 8, as long as it is clearly 'all' thresholds.

"9. Modernising the Industry assistance framework –

a. Implement detailed requirements for industry interception obligations

b. extend the regulatory regime to ancillary service providers not currently covered by the legislation

c. implement a three tiered industry participation model"

No comment, as I think industry should respond.

> *"10. Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations".*

While it didn't cover all the issues it should have – ie for example what side effects might be, and what the disadvantages or abuses it may make possible – this is one of the more sensibly presented major propositions in the discussion paper.

ie

> *"Should an authorised intelligence operations regime be pursued, it will be critical that it achieves an appropriate balance between operational flexibility and appropriate oversight and accountability. Key features that may contribute to such could include.."*

And then list some specific oversight suggestions (all of which seem sensible) – something absent from the bulk of the discussion paper.

Thus I do support proposal 10, assuming it is implemented correctly with at least the oversight mentioned.

"11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:

a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.

b. Align surveillance device provisions with the Surveillance Devices Act 2007

c. Enable the disruption of a target computer for the purposes of a computer access warrant

d. Enable person searches to be undertaken independently of a premises search

e. Establish classes of persons able to execute warrants"

(a), (b), (d) seem reasonable.

(c) – while at first glance may seem to be OK, is actually opening a can of worms. From the discussion paper –

> *"Subsection 25A(5) currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons. This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be. To address this, section 25A could be amended so that the prohibition does not apply to activity proportionate to what is necessary to execute the warrant".*

What will be proportionate? What and how will oversight be implemented? If incriminating evidence is found on the target computer can it be argued that ASIO put it there or allowed someone else to put it there? For example, if ASIO modifies a computer to allow easier remote access, could it then be argued that some other 3rd party used the easier access to plant files? If ASIO modify a computer as part of a warrant, find no evidence of wrong doing, do they then reinstate it?

I can see that this issue needs to be addressed, but it needs to be looked at far more comprehensively before a decision could be made one way or another on what needs to be done. **Until this is done no changes should occur.**

(e) – there is no doubt that creating classes of people to execute warrants does reduce accountability, as well as slightly increasing the administrative work - not only which people were in which class would have to be kept, but a full history so that respectively it could be seen that a person who did execute a warrant *had the authority at that time* to do so.
Having the actual names of people who can execute a warrant tied to the warrant obviously has more accountability, what is not clear from the discussion paper is if it is worth the trade off of losing this for an increase in ASIO efficiency (as per many parts of the discussion paper, this trade off is not discussed).

As such, more detail should be sought before this proposal, or something else that addresses the issue, is implemented.

As a result I do NOT support proposal 11.

12. Clarifying ASIO's ability to cooperate with the private sector.

I absolutely agree that this should be clarified, **however** far more should be done than what is recommended in the discussion paper ie

> *"It may be desirable to amend subsection 19(1) to avoid any doubt about ASIO's ability to cooperate with the private sector."*

There is no doubt that ASIO should be able to cooperate with the private sector, the big issue is on what basis, with what oversight, what permissions it requires (or should require) on a case by case basis, etc etc.

It seems that one of the world wide trends with security agencies in recent years is to outsource bits of their functionality to the private sector to do an 'end run' around any accountability requirements they are subject to.
This should not be allowed to happen) it Australia, with some signs being worrying - ie the recent report in the mainstream media a week ago, that was removed from all online sites the next day.

As such, proposal 12 should not be done in its current form, it should be subject to its own independent review (in its own right) of what should be implemented.

As a result I do NOT support proposal 12.

> *"13. Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation."*

Unbelievable this wasn't fixed within days of someone noticing the problem.

Thus I do support proposal 13.

> *Telecommunications (Interception and Access) Act 1979*
> *14. Reforming the Lawful Access Regime*
> *a. expanding the basis of interception activities*

There appears to be not enough detail in the discussion paper for me to comment on this item.

As a result I do NOT support proposal 14.

"15. Modernising the Industry assistance framework

a. establish an offence for failure to assist in the decryption of communications

b. institute industry response timelines

c. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts"

a. establish an offence for failure to assist in the decryption of communications

It is ridiculous to make it an offence for failure to assist in the decryption of communications, for both practical and theoretical reasons.

On the practical front, what would an agency do if someone said

1. 'I can't remember the password'
2. 'I've deleted whatever the password was that was used for that period, so can not assist.'
3. 'I didn't know it was encrypted, so have no idea what you are talking about.'
4. 'It's not encrypted, it's just random junk (for whatever reason..)'
5. 'The password I gave you doesn't work? The file/message must be corrupted, I can't help you.'

In addition, many communication protocols regularly used on the internet have session keys used for encryption, which are not recoverable by the end user.

What would the agency do? All the responses above might be legitimate, I have certainly experienced every one of them! How would you distinguish between someone who was truefully saying it and someone who was lying? Surely it would be against the presumption of innocence to fine/jail people who failed to assist unless it could be **proven** that they **could** assist – and how could this be done? How would it be legislated?

On a theoretical basis, shouldn't people broadly have a right against self incrimination, and a right not to answer questions?

While I do believe that there are circumstances in which these rights (and others) should not apply, they should be specifically removed as part of a wider rights removal, with appropriate process and oversight, not part of an 'everyday' warrant. Even then, the practical problems still exist for this specific issue.

"c. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts"

As this is not discussed in detail in the discussion paper, it's hard to tell how the agencies could justify this proposal. However, I'm guessing (in the same way other things in the paper are justified) they would point out the benefits and ignore everything else. The benefit of keeping track of everyone is that when they find someone they are interested in they can go back in time and see what that person has been doing for the last two years. Theoretically great from the agencies perspective - especially as they are not planning to pay for it.

However, this is probably the worst proposal mentioned in the terms of reference -

1. It is monitoring all Australians, not just ones with warrants.

2. It is a massive invasion of everyone's privacy, as the usage database will contain every page they accessed – such as every article they have read on a newspaper site, any online political activity they have done, anything they have done on ebay, what books they have bought on Amazon, which Facebook pages they have gone to, etc etc - and a lot of information that is also often included in the URL.

3. All it takes is one 'small' security slip for this information to be made public, and there will be a significant attempts of people trying to access to it.

   Take Telstra - with over a 40% market share – if their monitoring database was compromised millions of Australians would have their personal information shared across the globe.

   Anybody who thinks this couldn't happen, or that systems can be designed to prevent it, is not living in the real world.

   Large data exposures happen on a weekly basis, ie in just the last few weeks AAPT's records were put online, and in another incidence 500,000 Australian credit card details were stolen.

   What's the Australian government going to say **when** (not if) this happens? Whoops, sorry?

4. It largely won't set out what it is trying to do. If everyone knows all internet traffic is monitored, people with things to hide - or who are just irritated with the government spying on everyone - will simply bypass the monitoring by either hiding what they are browsing or who is doing the browsing.

   ie

   a. Browsing with a public internet service ie internet café, public library.
   b. Using some else's wifi connection (many are not properly secured)
   c. Using someone else's computer, ie a friends or work colleague.
   d. Using Tor or a similar online anonymity tool.
   e. Using any number of open proxy services.
   f. Using a VPN to somewhere outside of Australia and browsing over that.
   g. etc etc..

5. Would potentially costing **hundreds of millions of dollars** to implement and maintain – which would increase everyone's internet costs.

Proposal 15 should be completely removed from consideration.

"Telecommunications Act 1997
16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:

a. by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference
b. by instituting obligations to provide Government with information on significant business and procurement decisions and network designs
c. Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers
d. Creating appropriate enforcement powers and pecuniary penalties Australian Security Intelligence Organisation Act 1979"

This appears to be going way too 'micro managed' far. The government should simply not be involved with this level of detail. (a) is almost impossible to do effectively, (b & c) are effectively a part government take over, and (d) is not relevant given the above…

What the government should do, instead of the suggestions in proposal 16, is something much simpler and far more effective in making telcos (etc) prioritise security – **make them financially liable (including penalties) for any breaches!**

For example, at the moment if someone hacks their network and steals 100,000 credit card details they say 'sorry' and ignore it. Imagine, for example, if there was a $1000 fine for each persons private information that was leaked, and mandatory reporting – in this case the fine would be $100 million, plus whatever was fraudulently withdrawn from peoples credit cards, plus the cost of re issuing new cards, etc.

They would take security much more seriously than they do now!

Although it's outside the scope of this review, the same approach needs to be taken with numerous other sectors.

As a result I do NOT support proposal 16.

"17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:

a. Using third party computers and communications in transit to access a target computer under a computer access warrant.

b. Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant

c. Clarifying that reasonable force may be used at any time during the execution
of a warrant, not just on entry.

d. Introducing an evidentiary certificate regime."

(a) – the discussion paper provides no suggestions on how this could be controlled, apart from saying -

> *"Noting that using a communication in transit or a third party computer may have privacy implications, appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme."*

Exactly what is meant by this proposal, particularly in light of some of the other recommended changes? ie is this suggesting the ASIO could hack person A's computer, to get to B's computer, to get to C's – where C is the only person mentioned in the warrant?
At a minimum every computer should be mentioned in the warrant, and significant oversight should be put in place, with a high hurdle to overcome before a warrant allows this at all – remember were are talking about potentially doing things to peoples computers who are **not** under suspicion to get to some who is. Where would this end?

(b) I agree that clarifying incidental powers is a good idea, however if it is going to 'clarify' to include entering third party premises for surveillance devices (say breaking into my house to put a camera in to watch next door) or other purposes, oversight and other issues need to be discussed as part of the 'clarifying'!

As a result I do not support proposal 17.

Intelligence Services Act 2001

18. Amending the Intelligence Services Act to:

a. Add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter intelligence activities.

b. Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person or persons where the Agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required.

c. Enable ASIS to provide training in self defence and the use of weapons to a person cooperating with ASIS.

This all seems OK, however it is difficult to tell give the poor examination of the issues, and lack of detail, in the discussion paper. I could be missing something obvious.

Thus I do support proposal 18, subject to a lot more details.