

TERMS OF REFERENCE - INQUIRY INTO POTENTIAL REFORMS OF NATIONAL SECURITY LEGISLATION

Having regard to:

- the desirability of comprehensive, consistent and workable laws and practices to protect the security and safety of Australia, its citizens and businesses,
- the need to ensure that intelligence, security and law enforcement agencies are equipped to effectively perform their functions and cooperate effectively in today's and tomorrow's technologically advanced and globalised environment, and
- the fact that national security brings shared responsibilities to the government and the private sector:

1) The Parliamentary Joint Committee on Intelligence and Security is to inquire into potential reforms of National Security Legislation, as set out in the attachment and which include proposals relating to the:

- a) Telecommunications (Interception and Access) Act 1979*
- b) Telecommunications Act 1997*
- c) Australian Security Intelligence Organisation Act 1979*
- d) Intelligence Services Act 2001*

2) The inquiry should consider the effectiveness and implications of the proposals to ensure law enforcement, intelligence and security agencies can meet:

- a) the challenges of new and emerging technologies upon agencies' capabilities
- b) the requirements of a modern intelligence and security agency legislative framework, and to enhance cooperation between agencies, and
- c) the need for enhancements to the security of the telecommunications sector.

3) The Committee should have regard to whether the proposed responses:

- a) 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
- b) apply reasonable obligations upon the telecommunications industry whilst at the same time minimising cost and impact on business operations in the telecommunications sector and the potential for follow on effects to consumers, the economy and international competition, and
- c) will address law enforcement reduction of capabilities from new technologies and business environment, which has a flow-on effect to security agencies.

- 4) The Committee should take account of the interests of the broad range of stakeholders including through a range of public, *in camera* and classified hearings.
- 5) The Committee should provide a written report on each of the three elements of the National Security Legislation referral to the Attorney-General.

The National Security Legislation the subject of the inquiry has three different elements and Objectives. They relate to:

- modernising lawful access to communications and associated communications data
- mitigating the risks posed to Australia's communications networks by certain foreign technology and service suppliers, and
- enhancing the operational capacity of Australian intelligence community agencies.

The proposals across the three different packages are separated into three different groupings:

- A. those the Government wishes to progress
- B. those the Government is considering progressing, and
- C. those on which the Government is expressly seeking the views of the PJCS.

A - Government wishes to progress the following proposals:

Telecommunications (Interception and Access) Act 1979

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

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
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
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

Australian Security Intelligence Organisation Act 1979

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.
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

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

B. Government is considering the following proposals:

Telecommunications (Interception and Access) Act 1979

8. Streamlining and reducing complexity in the lawful access to communications regime – this would include:
 - a. Creating a single warrant with multiple TI powers
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

Australian Security Intelligence Organisation Act 1979

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

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.

C. Government is expressly seeking the views of the Committee on the following matters:

Telecommunications (Interception and Access) Act 1979

14. Reforming the Lawful Access Regime

- a. expanding the basis of interception activities

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

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

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.

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.