

**IGIS SUBMISSION TO THE
SENATE LEGAL AND CONSTITUTIONAL COMMITTEE
INQUIRY INTO
THE TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL 2006**

INTRODUCTION

1. The purpose of this Bill is to amend the *Telecommunications (Interception) Act 1979* (TI Act) to implement many of the recommendations of the Blunn Report.
2. Two of the proposed amendments will have implications for the activities of the Australian Security Intelligence organisation (ASIO), which is oversighted and reviewed by the office of the Inspector-General of Intelligence and Security (IGIS). One of these amendments involves the capacity to intercept communications of a person known to communicate with a person of interest, and the second is the capacity to intercept telecommunication services on the basis of the telecommunication device rather than an identified telecommunication service number.
3. This submission provides an outline of the role of the IGIS, an overview of the amendments which are most relevant to ASIO, and the inspection program carried out by the IGIS and his office, to ensure legislative compliance.

GENERAL ROLE OF IGIS

4. The position of IGIS was established by the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). The role and functions of the IGIS in respect of ASIO are specified in sections 8 and 9A of the IGIS Act.
5. Section 8 of the IGIS Act details the circumstances in which the Inspector-General can conduct formal inquiries into ASIO's activities, while section 9A provides a general right for the IGIS to inspect any of ASIO's activities which the Inspector-General considers appropriate, for the purpose of giving effect to the objects of the IGIS Act.
6. The objects of the IGIS Act are expressed in section 4 to include legality, propriety and consistency with human rights of the activities of the Australian intelligence and security agencies, and also the effectiveness and appropriateness of agency procedures in regard to legality, propriety and consistency with human rights.

IMPACT OF BILL ON ASIO

7. The proposed amendments in Schedule 2, Items 1 to 10, will permit ASIO to seek telecommunication interception warrants in relation to B-Party services in circumstances when all other practical methods of identifying the telecommunication services of a person of interest have been exhausted, or it is not possible to intercept the services used by the person of interest.
8. B-Party interception warrants would only be available to ASIO for 90 days, instead of the 6 month period regularly applicable to telephone intercept warrants. Moreover, they would be available only in circumstances where the issuing authority is satisfied that the person being intercepted will likely be contacted on that telecommunication service by the person of interest.
9. Schedule 3, Items 1 to 24 will amend the named person telecommunications interception warrant provisions to enable ASIO to intercept communications to and from communications equipment such as mobile handsets and computer terminals.

10. Before issuing such an Equipment-based warrant, the issuing authority must be satisfied, among other things, that ASIO has no practicable method of identifying the telecommunication services used or likely to be used by the person of interest, or that the interception of those services would not be possible.

IGIS INSPECTION REGIME

11. The office of the IGIS conducts monthly inspections of all request by ASIO for telecommunication interception (including named person) warrants under the TI Act. In addition to this, the office of the IGIS also inspects all requests for questioning and detention, entry and search, listening device, computer access and computer access warrants sought under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).

- In scrutinising ASIO's requests for warrants, the office of the IGIS particularly checks that:
- the intelligence or security case is soundly based
- appropriate internal approvals have been obtained
- individuals who may execute the warrant or communicate the information obtained from the warrant have been nominated in writing by the Director-General of Security
- any appropriate certifications or approvals external to ASIO have been obtained
- reports to the Attorney-General of the outcome of executed warrants are factual and have been provided in a timely manner, and
- the activity concerned occurred only during the approved period.

13. Both B-Party interception and Equipment-based interception will be subjected to this inspection regime.

14. The nature of B-Party interception warrants inherently involves a potential for greater privacy intrusion for persons who may not be involved in activities of legitimate concern under the ASIO Act. As a result, particular attention will be given to the additional legislative tests for this type of warrant, as well as checking that the duration of 90 days is adhered to.

15. Similarly, particular attention will be paid to the case put forward for named person warrants to be equipment-based ie, that there is no other practicable method of identifying the telecommunications services used or likely to be used b the person of interest, or that the interception of those services would not be possible.

SUMMARY

16. The proposed amendments to the TI Act in relation to B-Party interception and Equipment-based interception by ASIO will be the subject of the same rigorous inspection regime that all warrant requested by ASIO undergo.