



INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

2007/376

File Ref: 2006/49

Ms Jackie Morris
Committee Secretary
Senate Legal and Constitutional Affairs Committee
Parliament House
CANBERRA ACT 2600

Dear Ms Morris

Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007

Thank you for your communication of 21 June 2007 inviting a written submission to the Committee's inquiry into the Telecommunication (Interception and Access) Amendment Bill 2007 (the Bill).

2. By way of background I should briefly outline the role of the Inspector-General of Intelligence and Security (IGIS).

3. The position of IGIS was created by the *Inspector-General of Intelligence and Security Act 1986*. The IGIS is an independent statutory position which reviews the six agencies referred to as the Australian Intelligence Community (AIC), namely:

- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Defence Intelligence Organisation (DIO)
- Defence Imagery and Geospatial Organisation (DIGO)
- Defence Signals Directorate (DSD)
- Office of National Assessments (ONA).

4. The purpose of this review is to hold the AIC agencies accountable in respect of compliance with Australian law and with ministerial directions, the propriety of their

activities and respect for human rights.

5. The IGIS can conduct formal inquiries using powers similar to those of a Royal Commission. Such inquiries can be triggered by a complaint, or of the Inspector-General's own motion, or on the request of a relevant minister.

6. Importantly, my office also conducts a range of inspection activities which involve visiting agencies and inspecting records. Inspections are aimed at identifying, where possible, issues at an early stage.

7. The inspection program also recognises that intelligence activities are covert and the subjects of intelligence interest will often simply not be in a position to make a complaint about the conduct of an AIC agency. Moreover, in a period when collection agencies are being given additional powers and capabilities, there is a need for reassurance that these are being used professionally and properly and for the purposes for which they were given.

Prospective telecommunications data

8. One of the proposals in the Bill is that very senior officers of ASIO will be able to issue authorisations requiring carriers or carriage service providers to provide prospective telecommunications data for the duration of the authorisation (up to 90 days) – see proposed section 176 in Part 1 of Schedule 1 of the Bill.

9. The Explanatory Memorandum to the Bill notes that there is a higher privacy impact from the disclosure of information on a prospective basis, and the Bill requires such authorisations to be issued at a more senior level than authorisations for historical telecommunications data.

10. While this requirement for more senior approval is appropriate, I believe it is also a process which should be examined as a part of my office's inspection program. This would involve periodic visits by my staff during which they would review all of the authorisations granted in the preceding period to ensure that there was sufficient justification and that requirements imposed by the Communications Access Coordinator under the proposed section 183 were met.

11. In a general way this would reflect the process undertaken by my office in relation to warrants sought by ASIO pursuant to Divisions 2 and 3 of Part III of the *Australian Security Intelligence Organisation Act 1979*.

Development or testing

12. The Bill also proposes (Item 16 of Part 1 of Schedule 2) that the heads of Commonwealth security authorities be able to obtain authorisations from the Attorney-

General to undertake interception for the purpose of developing and testing interception capabilities.

13. Safeguards include that information or records obtained under such an authorisation be destroyed as soon as practicable once they are no longer required in relation to the development or testing (proposed section 31C) and that a report be provided to the Attorney-General within three months of the authorisation ceasing (proposed section 31D).

14. The term "security authority" will be defined by means of inserting into section 5(1) the following:

security authority means an authority of the Commonwealth that has functions primarily relating to:

- (a) security; or
- (b) collection of foreign intelligence; or
- (c) the defence of Australia; or
- (d) the conduct of the Commonwealth's international affairs.

15. It is not clear to me why element (d) of the proposed definition is necessary, at least in respect of the development and testing of interception capability.

16. In respect of those agencies which are within my jurisdiction my intention would be, if these amendments are enacted, to include review of authorisation requests and of reports made as to outcomes and the destruction of records, in my office's inspection program.

Network protection

17. Items 11 and 12 in Part 1 of Schedule 2 of the Bill are said to allow network administrators in certain agencies to protect network infrastructure without the risk of being in breach of the Act.

18. Relevant agencies in this regard are "a Commonwealth agency", or "a security authority" or "an eligible authority of a State". The first of these categories is defined in section 5 of the *Telecommunications (Interception and Access) Act 1979* as meaning three agencies only – the Australian Federal Police, the Australian Commission for Law Enforcement Integrity and the Australian Crime Commission.

19. While one can well understand the need for adequate protection of the agencies which directly protect obvious national security interests (i.e. Australia's defence, security, international relations or law enforcement), the question also arises as to whether there is other network infrastructure the protection of which is also of particular importance to Australia's interests.

20. Work on critical infrastructure protection often highlights the interconnectedness of dependencies as well as the vital importance of a range of activities to the general security of the Australian community.

21. I confess that I do not have the expertise or immediate knowledge to answer the question I have posed, but I suggest that it is one which needs to at least be addressed.

22. I hope these comments are of assistance to the Committee in its inquiry.

Yours sincerely

Ian Carnell
Inspector-General of
Intelligence and Security

11 July 2007