REPORT OF THE IGIS INQUIRY INTO THE ALLEGED IMPROPER INVESTIGATION OF THE MINISTER FOR DEFENCE BY THE DEFENCE SIGNALS DIRECTORATE

June 2009

REPORT OF THE IGIS INQUIRY INTO THE ALLEGED IMPROPER INVESTIGATION OF THE MINISTER FOR DEFENCE BY THE DEFENCE SIGNALS DIRECTORATE

Introduction

On 27 March 2009 I initiated, of my own motion, an inquiry into allegations which had appeared in the media that an individual or individuals employed by the Defence Signals Directorate (DSD) may have improperly accessed information technology used by the Minister for Defence, the Hon. Joel Fitzgibbon MP as part of a covert investigation into the Minister's activities and associations. As an own motion inquiry I also had the capacity to examine any related matters which fell within my jurisdiction.

2. I need to be clear that my jurisdiction is limited to the activities of the three Defence agencies specified in my enabling legislation, namely the Defence Imagery and Geospatial Organisation (DIGO), the Defence Intelligence Organisation (DIO), and DSD. My jurisdiction does not include other elements of the Department of Defence or any person(s) outside the Department of Defence who might have had legitimate access to the Minister's IT equipment or data.

3. My various lines of investigation into this matter have now been completed and this is the report of the inquiry, prepared in accordance with the requirements of section 22 of the Inspector-General of Intelligence and Security Act 1986 (IGIS Act).

4. The report covers the following matters:

- the allegations made (pp. 2-5)
- a brief explanation of DSD's role (pp. 5-6)
- the legal basis for this inquiry (pp. 6-7)
- the relationship of this inquiry to one conducted by the Department of Defence (p. 7)
- the various lines of investigation I pursued (pp. 8-14), and
- my conclusions and formal findings (pp. 14-15).

5. My key general conclusion was that I found no evidence or indication which might raise suspicion that the allegations concerning DSD personnel are correct.

Allegations made

6. On the morning of 26 March 2009, newspaper articles were published which alleged that the Minister for Defence, the Hon. Joel Fitzgibbon MP, had been the

subject of an investigation by persons within the Department of Defence. A number of allegations about the Minister were made.[1]

7. These articles, and further articles published in the ensuing days, included the following claims about Department of Defence personnel:

- Officials in the Department of Defence had conducted a "covert" investigation into the relationship between the Minister for Defence and an Australian businesswoman of Chinese heritage, Ms Helen Liu.

- The basis for this covert investigation was concern on the part of the persons who initiated it, that the relationship between the Minister for Defence and Ms Liu posed a potential security risk.

- As part of the covert investigation a DSD officer "accessed Mr Fitzgibbon's office IT system and is understood to have found Ms Liu's banking details".

- The persons who conducted this covert inquiry had informed senior Defence figures of their concerns and the outcome of their investigations, but these matters were taken no further (although this was contradicted in a later article on 7 May 2009[2]).

- This covert investigation had been initiated "well before" a dispute about the payment of allowances to Special Air Service soldiers emerged as an issue which was the subject of public debate (i.e. circa October 2008).

- Individuals within the Department of Defence had leaked the results of their covert investigations to the media.

8. The articles noted that their sources or confirmation for a significant part of the material about the Minister included court records, company records, the register of members' pecuniary interests, as well as comments provided by business associates of Ms Liu and political associates of Mr Fitzgibbon. One commentator noted that:

> *"The material about Fitzgibbon was apparently supplied initially via an anonymous letter to an investigative reporter …"*[3]
>
> *"… much of the material supplied to the journalists who broke the story had nothing to do with Ms Liu and was not related to security at all"*.[4]

---

[1] *The Sydney Morning Herald*, 26 March 2009, p.1, 'Defence leaks dirt file on own minister';
The Canberra Times, p.1, 26 March 2009, p.1, 'How Defence officials spied on Fitzgibbon', and
The Age, 26 March 2009, p.1, 'Defence probe into minister'.

[2] *The Age*, 7 May 2009, p.1, 'Helen Liu had spy link: officials', A person alleged to have been part of the covert investigation was quoted as saying: *"It didn't go anywhere … I don't think it went up the chain of command at all."*

[3] *The Daily Telegraph*, 28 March 2009, p.34, 'Fitzgibbon's devil is in forgotten details'.

[4] ibid.

9. Soon after the first articles appeared the Minister for Defence said that he had failed to declare trips he had made in 2002 and 2005 to the People's Republic of China which had been paid for by Ms Liu, or her associated commercial interests. Mr Fitzgibbon apologised for not having declared this travel.[5]

10. An article published on 28 March 2009 included further allegations about the Minister and commented on the possible source of another aspect of the allegations made:

> *"Personal details emerging from the unauthorised inquiry include Mr Fitzgibbon's sub-letting of a Canberra residence from Ms Liu, his possession of her bank account details and his receipt of gifts from her, including a Hugo Boss suit which he later returned …*
>
> *Details concerning the gift are likely to have come from either close observation of the minister's personal affairs, surveillance of Ms Liu or a disclosure by a member of his staff.*
>
> *… the secret probe also raised potential conflict of interest questions about lobbying by Mark Fitzgibbon the Minister's brother and chief executive of NIB Health Fund and executives from US health services giant Humana.*
>
> *It has been alleged by Defence officials that the minister's brother and the US executives used Mr Fitzgibbon's office as a base for their lobbying of Government ministers and senior officials."*[6]

The article also contains a statement by a spokesman for the Minister which rejects any conflict-of-interest claims.

11. The Attorney-General, the Hon. Robert McClelland MP, released a media statement on the morning of 27 March 2009, which said that:

> *"… the Acting Director-General of Security has advised me that ASIO has no information relating to Ms Helen Liu which would give rise to any security concern regarding her activities or associations."*[7]

12. It seems that allegations along the lines of those published were contained in an anonymous letter or letters circulated to some journalists in the period preceding 26 March 2009. I spoke with two of the journalists concerned and they advised that they were not in a position to provide a copy of the anonymous letter they had received.

---

[5] *The Australian*, 27 March 2009, p.1 'Fitzgibbon admits woman friend paid for China trips'.
[6] *The Canberra Times*, 28 March 2009, p.1, 'Fitzgibbon's brother hit in covert file'.
[7] http://www.attorneygeneral.gov.au/www/ministers/RobertMc.nsf/Page/Media_Releases (accessed on 26 May 2009).

13. I was able to access emails which the journalists had sent to the office of the Minister for Defence prior to 26 March 2009, asking a series of questions which I have assumed reflect the content (or much thereof) in the anonymous letter or letters.

14. Most of the topics covered in the emails are those that appeared in the newspaper articles. Those points which did not appear in the media seem to have had little basis in fact.

15. Given the seriousness of the allegations that suggested that a covert investigation of the Minister had been undertaken by persons in the "intelligence and security area of Defence", supported by a DSD officer who had purportedly accessed the Minister's office IT system, I decided that it was necessary for me to initiate an inquiry under the IGIS Act which would focus on DSD.

Role of Defence Signals Directorate

16. The Defence Signals Directorate is Australia's national authority for signals intelligence, and for information security.

17. DSD's legislated mandate is as follows:

> *"(a) to obtain intelligence about the capabilities, intentions or activities of people or organisations outside of Australia in the form of electromagnetic energy, whether guided or unguided or both, or in the form of electrical, magnetic or acoustic energy, for the purposes of meeting the requirements of the Government, and in particular the requirements of the Defence Force, for such intelligence, and*
>
> *(b) to communicate, in accordance with the Government's requirements, such intelligence, and*
>
> *(c) to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; and*
>
> *(d) to provide assistance to the Defence Force in support of military operations and to cooperate with the Defence Force on intelligence matters; and*
>
> *(e) to provide assistance to Commonwealth and State authorities in relation to:*
>
> *(i) cryptography and communications and computer technologies; and.*
> *(ii) other specialised technologies acquired in connection with the performance of its other functions; and*
> *(iii) the performance by those authorities of search and rescue functions."*[8]

[8] Section 7 of the *Intelligence Services Act 2001 (Cwth),* Act No. 152 of 2001 (ISA).

18. If DSD believes it is necessary in performing its function to intentionally collect intelligence information on Australian persons, a specific authorisation must be obtained from the Minister for Defence.[9]

19. If a matter concerns a threat to security, the agreement of the Attorney-General is also required.[10]

20. Collection of intelligence or information by DSD without lawful authority would be a clear breach of the ISA. There are also criminal offences in Part 10.7 of the Criminal Code 1995 (Cwth) relating to unauthorised access to restricted data held in a Commonwealth computer.

Legal basis for IGIS inquiry

21. The IGIS Act establishes the role and functions of the Inspector-General of Intelligence and Security, details the limits of the Inspector-General's jurisdiction, and provides a framework within which the Inspector-General can conduct inspection activities and inquiries.

22. The IGIS Act currently provides that the Inspector-General has jurisdiction to review the activities of the six intelligence and security agencies which collectively comprise the Australian Intelligence Community (AIC), namely the:

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

23. The Inspector-General's range of functions with respect to DIGO and DSD are specified under section 8(2) of the IGIS Act, and with respect to DIO under section 8(3) of the IGIS Act.

24. These provisions include a capacity for the Inspector-General to initiate, of his or her own motion, an inquiry into the legality, compliance with ministerial directions, propriety and respect for human rights of the activities of DIGO, DIO and DSD.

[9] See sections 8 and 9 of the *Intelligence Services Act 2001 (Cwth).*
[10] See section 9(1A)(b) of the *Intelligence Services Act 2001 (Cwth).*

25. Section 17(1) of the IGIS Act requires that an inquiry of this kind shall be conducted in private, and in such manner as the Inspector-General sees fit. The purpose of this provision is not to hide the fact of an inquiry but to enable the Inspector-General to pursue investigative activities and consider classified and/or highly sensitive material which it would not be in the national interest to be publicly ventilated.

26. Section 18 of the IGIS Act provides the Inspector-General with a suite of strong coercive investigative powers and associated immunities and protections, which are akin to those that would be available to a royal commission.

Relationship to Defence Inquiry

27. As already noted, my jurisdiction as IGIS is currently limited by the IGIS Act to the activities of the six AIC agencies.

28. The intelligence and security areas of the Department of Defence naturally include the three intelligence agencies which fall within my remit, but could also conceivably include the Defence Security Authority (DSA), Australian Defence Force intelligence units, and other elements of the Department which deal with security issues.

29. On 26 March 2009, the Secretary of the Department of Defence, Mr Nick Warner, had initiated an inquiry into these allegations, which was conducted by DSA.

32. I liaised with Mr Warner on 27 March 2009, to ensure that he was aware of my intention to initiate my own inquiry, with a particular focus on DSD.

30. I met with Mr Warner, Mr Stephen Merchant (a Deputy Secretary in the Department of Defence with functional oversight of the three Defence intelligence agencies as well as DSA), and the Director of DSD on 30 March 2009. The purpose of this meeting was to map out the general direction of our respective inquiries, to ensure that they would be complementary (although separate) activities.

31. In the above meeting I indicated that the primary focus of my investigation would be on DSD, and that I would be happy for DSA to pursue matters as they saw fit within DIO and DIGO.

32. The only qualification I placed on this arrangement was that I should be promptly informed of any developments of relevance relating to DIGO or DIO, and I reserved the right to pursue further or other investigations into those agencies if I considered this to be necessary or appropriate. This was agreed and the two inquiries proceeded on this basis.

Lines of investigation

33. I decided that a central element of my investigations needed to be expert IT forensic examination to identify whether or not there had been any unauthorised access to the Minister's computing facilities. Such an examination would not be limited to whether unauthorised access had been attempted from within DSD itself, but whether anyone from any location had attempted unauthorised access.

34. I also saw such forensic examination as an opportunity to ascertain whether the computing facilities used by the Minister for Defence contained any information which might have formed the basis for any of the various allegations made.

35. While the essential allegation I was concerned with was whether DSD had accessed the Minister's computing facilities without authority, I decided that it was important to also examine whether there might have been any other means by which DSD personnel were part of, or contributed to, any covert investigation of the Minister. The hypotheses relevant to this included whether:

(a) DSD had had access to the Minister's records as part of its information security role (and from which there might have been improper disclosures).

(b) DSD had unlawfully intercepted any electronic communications of the Minister for Defence.

(c) DSD had any item of information obtained from its legitimate signals information activities, which had also appeared in the newspaper articles.

(d) Other methods of investigation of the Minister had been attempted (e.g. unauthorised physical intrusion into his parliamentary offices, or signs of investigation by Defence personnel such as searches on Department of Defence or other relevant databases).

36. The following sections of this report briefly explain what was done for each of these lines of investigation and what the results were.

IT forensic analysis

37. I met with the Commissioner of the Australian Federal Police AFP, Mr Mick Keelty APM, on 30 March 2009, and requested assistance for the IT forensic work.

38. Commissioner Keelty immediately agreed, and assigned a senior computer forensic examiner to this task for as long as I required, who would be subject to direction and tasking from me.

39. I am very appreciative of the Commissioner's willingness to make such expertise so readily and promptly available to my inquiry.

40. I must also express my great appreciation for the professional and thorough way the forensic examiner readily tackled the work I commissioned.

41. I spoke with the Minister for Defence and in the course of doing that obtained written consent from him, which among other things, authorised persons acting on my behalf to conduct checks of the Minister's Parliamentary Services computer equipment and email accounts. The Minister provided this consent immediately it was asked of him and without demur.

42. A copy of the Minister's consent was provided to the Department of Parliamentary Services (DPS), who in turn informed the Presiding Officers of the actions being taken.

43. I must also acknowledge the assistance provided by DPS staff in facilitating access to the relevant equipment and data, and in explaining the applicable security arrangements.

44. The primary task I asked the AFP computer forensic examiner to undertake was to examine the information technology used by the Minister, and advise me whether there was any indication of unauthorised access to this equipment from any location.

45. As a secondary task, a list of search terms was developed for which the examiner should search in the Minister's records. The purpose of the activity was to determine if there were any records contained in or otherwise linked to the information technology equipment used by the Minister, particularly of a personal nature, which could have formed the basis for the stories which had appeared in the media.

46. The computer forensic examiner provided me with two very comprehensive reports.

47. It is not appropriate for me to provide details of these reports in an unclassified document for both privacy and security reasons. I can, however, provide the conclusion reached by the examiner. This was that there was no evidence to indicate that any unauthorised persons had accessed or attempted to access the computing items or data contained therein. Nor was any malicious or unauthorised software (or associated data artefacts) identified that would have facilitated such access.

48. There was one piece of equipment from the Chief Information Officer Group in Defence used by the Minister which had been re-imaged when replaced by the Department (as one would expect from a security point of view), leaving no remanent data from its original use. However, the extent to which this could have been used to yield access to some of the Minister's personal data would have been very limited.

The Minister advised me that he did not hold any personal data on his Defence issued equipment.

49. It was also evident from the search of the Minister's Parliament House electronic records that they contained very little of the personal information contained in the newspaper articles.

Whether information security access

50. As noted earlier, another hypothesis I considered was the possibility that DSD staff may have legitimately accessed the Minister's IT facilities (in discharging DSD's information security function), and that this was a means by which personal information about the Minister could have been accessed and then used or disclosed improperly.

51. My staff reviewed records that are held in DSD, which would show any instance where its staff had legitimate cause to examine, or otherwise access, information technology equipment or systems used by the Minister. This review activity revealed nothing of consequence or concern.

52. In the course of these review activities, it was noted that the Minister and a member of his staff had each been given USB memory sticks at an overseas conference. The memory sticks contained basic information about the conference but could theoretically be used to store any electronic document.

53. Being security conscious, the Minister provided these small gifts to DSD for safekeeping.

54. As these memory sticks were in the possession of DSD, I asked for each of them to be examined in the presence of my staff, so that we might independently ascertain whether they contained any personal information relating to the Minister, or which might have formed the basis of any of the news reports contained in the media.

55. I am satisfied that no such information was contained on the USB memory sticks.

Whether interception of communications

56. Another hypothesis explored was whether DSD might have deliberately intercepted the Minister's communications.

57. In a similar vein, the question arose in my mind as to whether any of the information in the media stories had been part of interception activities on legitimate targets.

58. So as to test these hypotheses my staff undertook or oversighted a number of independent searches on various DSD databases using search terms which I had determined, for evidence of anything untoward, or inappropriate, or which could have formed the basis for media reporting and speculation.

59. These searches revealed nothing to support the allegations.

Whether suspicious database searches

60. I thought it would also be worthwhile to explore whether staff might have attempted searches in relation to "Helen Liu" in reporting/intelligence databases available to them (For ease of reference, this activity might accurately be described as a 'search of searches').

61. The purpose of this exercise was to ascertain whether any person had input a search term which might suggest an inappropriate, or at least unexplained, interest in someone connected with the Minister.

62. In this regard I relied on checks conducted by DIO as to whether anyone (including intelligence staff from elsewhere in the Department of Defence) had attempted such a search on its databases. A similar check was also done by DSD of its databases, at my request.

63. I also contacted an agency outside of Defence, to ascertain whether anybody from any of the agencies of interest to me had initiated searches on a relevant database.

64. The ultimate result of this 'search of searches' exercise was that there was no evidence of any person attempting a search which might have been of interest to my inquiry, in the relevant period.

Whether physical intrusion

65. I considered the possibility that information about the Minister might have been obtained by unauthorised access to the Minister's Parliament House office or his electorate office, rather than through unauthorised interception or hacking activities.

66. There was, however, no indication of unauthorised physical intrusion at either location.

Whether suspicious communications

67. In addition to conducting the above investigative activities, I thought it would also be appropriate to undertake a number of telephone records checks on several telephone numbers of interest to my inquiry.

68. The purpose of these telephone records checks was to identify if persons using the telephones in which I had an interest had been in contact with work related telephones allocated to personnel in any of the three Defence intelligence agencies within my remit.

69. As the billing records for most of the phones in question are held by the Chief Information Officer Group within the Department of Defence, I sought their assistance in obtaining and analysing relevant records in the previous 12 months.

70. I separately tasked DSD to undertake a similar review activity with respect to official phones for which it, rather than CIOG, held relevant billing records.

71. These searches revealed no information which needed to be followed up.

Declarations by senior DSD staff

72. My staff and I developed a list of 34 persons who hold senior leadership and specialist positions within the Defence Signals Directorate, whom I believed might be in a position to provide me with information which would advance my inquiry.

73. I wrote to each of the 34 persons so identified, on 31 March 2009, asking each to complete and sign a statutory declaration, responding to six questions.

74. None of the responses raised anything that might support the allegations in the media or which warranted further follow up by me.

75. In addition to the 34 statutory declarations I solicited, one DSD officer volunteered to complete a statutory declaration of their own volition, on the basis that they had a family connection to a person of possible interest outside of the Department of Defence. The person making this declaration disavowed any knowledge of any issues associated with the allegations which had appeared in the media.

Open letter

76. In an attempt to generate additional lead information I prepared an open letter to be issued to all Department of Defence staff (i.e. civilian and military personnel).[11]

77. The above letter, which had the support of the Secretary of the Department of Defence and the Chief of the Defence Force, was issued to all Defence staff on 31 March 2009.

78. In the above letter, I asked that anyone who had any information which might be relevant to my inquiry to contact my office. I also provided appropriate assurances that any information provided to me would be handled discretely and securely.

[11] IGIS letter 2009/169 dated 31 March 2009.

79. The open letter generated one phone call to my office. The information which was conveyed was not germane to the matters under investigation.

Notices issued under section 18 of the IGIS Act

80. At the outset of my inquiry I had decided that I would seek statements from more junior staff or former staff in relevant areas of DSD, but that I would do so after the IT forensic work was well advanced.

81. When this point was reached I issued formal notices under section 18 of the IGIS Act to 151 individuals, requiring them to provide me with written responses to four questions which were pertinent to my inquiry.

82. Section 18(1) of the IGIS Act provides me with express powers to obtain information and documents from any person who I believe is capable of giving information, or producing documents, relevant to a matter into which I am inquiring under the IGIS Act.

83. I explained in the letter which I sent to each person on the above list that I had chosen to seek this information by means of a section 18 notice rather than a statutory declaration, because doing so gives special protection to anybody who provides information to me, when it is required to be produced in this manner.

84. The only exception to the protection which I described would be if a prosecution were to be launched against an individual who, in responding to a section 18 notice, sought to deliberately mislead the Inspector-General, contrary to their obligation to be truthful.

85. All 151 recipients responded to the notice.

86. None of the information in the responses contained any suggestion which might support the published allegations or which required follow-up by me.

87. In the course of my inquiry I had considered obtaining statements from the various Departmental Liaison Officers who spent time working in the Minister's office in the relevant period.

88. I did not pursue this option myself, as DSA had already obtained statements from these individuals and this had revealed nothing of particular interest or concern.

89. Based on other thoughts which I had developed in the course of my inquiry, I determined that it was appropriate for me to seek information from six individuals who were involved in conducting security briefings and debriefings, for persons employed in the Minister's office.

90. I therefore issued six additional notices made under section 18 of the IGIS Act, on 21-22 May 2009. In these notices I asked each respondent to answer a single question, which was relevant to my inquiry.

91. There was nothing in the responses to these six section 18 notices which caused me to extend my investigation.

92. Should there have been justification to do so, I had intended to formally interview any persons of interest arising from any of the above exercises. Given the responses I received there was no basis for me to pursue this course.

Conclusion

93. The IT forensic examination conducted as part of my inquiry did not identify any unauthorised access or attempts at unauthorised access (including by DSD personnel) to the Minister's computing items or data contained therein.

94. In the light of this result, it is worth reflecting on the nature of the information involved in this matter.

95. As noted in paragraph 8, a good deal of the information which has been published is accessible in the public domain, or is otherwise known to a number of people who work in, or who have worked in, Parliament House, or indeed elsewhere.

96. There are a few items – essentially those referred to in paragraph 10 – which would have been known to a relatively small number of people. The small number of people in that group are not limited to people employed by the Department of Defence.

97. Most of the information in this category (i.e. known to a relatively small number of people) is not available in the Minister's electronic records, and would have been known by other means such as physical observation. There is one item which must have come from viewing the Minister's records, but a number of people outside of the Department of Defence had legitimate access to this record. The significance of this is that the allegations against the Minister could have been formulated without there having been unauthorised access to the Minister's computing facilities.

98. Examination of other means by which DSD personnel might have been involved in, or contributed to, a covert investigation of the Minister, did not yield any indication that such activities had occurred. Some of this examination also covered whether DIGO or DIO staff may have done so, but there was no indication of that having happened.

Findings

99. My formal findings are therefore as follows:

1. There is no evidence or indication which might raise suspicion that there has been an official or legally sanctioned investigation by the Defence Signals Directorate of the Minister for Defence.

2. There is no evidence or indication which might raise suspicion that any Defence Signals Directorate officer(s) attempted or were part of an unofficial investigation.

3. The Defence Signals Directorate has not accessed any of the personal information which has been disclosed in the media, as part of its information security role or other legitimate activities.

4. Nothing was seen in the course of this inquiry which suggests that the conclusions drawn in the general Defence inquiry[12] are incorrect in respect of those other parts of Defence which fall within my legislative jurisdiction, namely the Defence Intelligence Organisation or the Defence Imagery and Geospatial Organisation.

Recommendations

100. Given the nature of the findings set out above, there is no basis for me to make any recommendations.

Ian Carnell
Inspector-General
of Intelligence and Security

June 2009

[12] Defence media release MSPA 178/09 dated 29 May 2009, 'Defence Review Finds No Investigation of Minister'. An unclassified version of the DSA report is available on the Defence website at: http://www.defence.gov.au/header/publications.htm (accessed on 1 June 2009).