Australian Government

Office of the Australian Information Commissioner

Inquiry into the DLA Piper Report on allegations of sexual and other abuse within Defence

Submission to Senate Foreign Affairs, Defence and Trade References Committee

22 November 2012

Timothy Pilgrim
Privacy Commissioner

Contents

Executive summary **1**

Key Messages **1**

A. Information held in the Fairness & Resolution Database 1

B. Ensuring ADF personnel are fully informed 2

C. ADF personnel service records and Archives' open access period 2

Introduction **2**

Background **3**

Structure of this Submission **3**

A. Information held in the Fairness & Resolution Database **4**

The application of the Privacy Act to information held in the Fairness & Resolution Database 4

The Defence Instructions (General) and the Privacy Act 6

Finding 29 of the Report – ensuring personal information is accurate, up to date and complete 6

B. Ensuring ADF personnel are fully informed **7**

IPP 2 notice obligations 7

The use of personal information to provide advice to complainants on the outcome of their complaint 7

C. ADF personnel service records and Archives' open access period **8**

Executive summary

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Senate Committee on Foreign Affairs, Defence and Trade References on the Inquiry into the report by DLA Piper on the Review of allegations of sexual and other abuse in Defence and the Government's response to that report.

The OAIC recognises that it is important for Defence to have at its disposal information that will allow it to assess, investigate and respond to allegations of abuse in an effective and timely manner. In addition, the OAIC acknowledges that this information can play a critical role in enabling Defence to identify and manage systemic issues of abuse.

The OAIC is mindful that information relating to allegations of abuse within Defence often includes the personal information of Australian Defence Force (ADF) personnel. The OAIC is concerned to ensure that such personal information is handled in a way that protects the privacy interests of the individuals concerned. However, the OAIC's view is that this can be achieved without inhibiting Defence's ability to effectively respond to specific allegations of abuse and to identify and manage any systemic issues that may arise.

Key Messages

A. Information held in the Fairness & Resolution Database

i The OAIC notes that the Information Privacy Principles (IPPs) do not prohibit the collection and use of personal information about individuals involved in an allegation of abuse within Defence, provided that the information is handled in accordance with the principles outlined in the *Privacy Act 1988* (see paragraphs 10-15).

ii Given the sensitive nature of personal information of this type, the OAIC suggests that the proposed Phase 2 of the Review should give specific consideration to:

- what, if any, collection, use or disclosure of personal information is necessary
- establishing clear instructions and/or policies outlining the purpose for which personal information can be collected and subsequently used or disclosed
- whether personal information recorded in the Fairness and Resolution Unacceptable Behaviour Database (FRD) is handled and protected appropriately
- whether personal information held in the FRD is accurate, up to date, complete and not misleading, and is fit for the purpose for which it was collected (see paragraphs 16-17).

iii The OAIC recommends that Defence consider undertaking a Privacy Impact Assessment in relation to the FRD (see paragraphs 18-19).

iv The OAIC is unclear whether the Defence Instructions (General) carry the force of law and suggests that Phase 2 give consideration to this matter (see paragraphs 20-22).

v Given the serious consequences that might flow from the use or disclosure of information contained in the FRD, the OAIC suggests that Defence should be satisfied as to the quality of the information contained in the FRD (see paragraphs 23-25).

vi The OAIC suggests that, to the extent that the information contained in the FRD is not accurate, up to date or complete, it might not be relevant for the purpose for which it was collected (see paragraph 26).

B. Ensuring ADF personnel are fully informed

vii The OAIC notes the importance of ensuring that ADF personnel are fully informed about how their personal information relating to complaints of abuse within Defence will be handled (see paragraph 27).

viii The OAIC notes the relevance of making an individual aware of how their personal information may be disclosed when considering whether a disclosure is permitted under IPP 11.1(a) (see paragraphs 28-31).

C. ADF personnel service records and Archives' open access period

ix The OAIC reiterates the importance of ensuring that ADF personnel are fully informed about how the personal information contained in their service record may be handled (see paragraphs 32-35).

Introduction

1. The Office of the Australian Information Commissioner (OAIC) was established by the *Australian Information Commissioner Act 2010* (AIC Act) and commenced operation on 1 November 2010. The former Office of the Privacy Commissioner (OPC) was integrated into the OAIC on 1 November 2010.
2. The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner.
3. The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information (FOI) in one agency, to advance the development of consistent workable information policy across all Australian government agencies.
4. The Commissioners of the OAIC share two broad functions:
    - the FOI functions, set out in s 8 of the AIC Act — providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982*, and
    - the privacy functions, set out in s 9 of the AIC Act — protecting the privacy of individuals in accordance with the *Privacy Act 1988* (Privacy Act) and other legislation.

5. The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

Background

6. On 10 October 2012 the Government asked the Senate Committee on Foreign Affairs, Defence and Trade References (the Committee) to consider a report by DLA Piper on the Review of allegations of sexual and other abuse in Defence (the Report)[1] and the Government's response to that report (the Inquiry). The overarching purpose of the Inquiry is to develop recommendations for improving the way in which Defence and the Government manage and respond to allegations of abuse within Defence.
7. DLA Piper was engaged by Defence to review allegations of sexual and other forms of abuse in Defence and to make recommendations for further action. The Report is the final Report of Phase 1 of the DLA Piper Review (the Review). The Report is primarily concerned with assessing, handling and responding to specific allegations of abuse and with the identification of systemic issues in Defence's management of abuse.
8. The Committee's terms of reference include one that is particularly relevant to the OAIC's activities:
    - *the effectiveness and timeliness of the government's processes for assessing, investigating and responding to allegations of sexual or other forms of abuse, including:*
        - iii) *whether data and information collection and dissemination, in relation to sexual and other forms of abuse in Defence, is adequately maintained and appropriately acted upon and, if not, any alternative mechanisms that could be established.*
9. The Report identifies a number of areas where current practices in the handling of personal information are impacting on Defence's ability to assess, investigate and respond to allegations of sexual or other forms of abuse within Defence. In particular, the Report addresses the question of whether current information handling practices are restricting Defence's ability to manage systemic issues of abuse.

Structure of this Submission

The OAIC's comments on the issues identified in the Report are made under the following headings:

A. Information held in the Fairness & Resolution Database

[1] Rumble, G *et al.* 2011, *Report of the Review of allegations of sexual and other abuse in Defence: Facing the problems of the past, Volume 1: General findings and recommendations* (2012) available at <http://www.defence.gov.au/pathwaytochange/docs/DLAPiper/index.htm> (the Report).

B. Ensuring ADF personnel are fully informed

C. ADF personnel service records and Archives' open access period

A. Information held in the Fairness & Resolution Database

The application of the Privacy Act to information held in the Fairness & Resolution Database

10. The OAIC understands that the Australian Defence Organisation is comprised of three Commonwealth agencies – the Australian Defence Force (ADF), the Department of Defence and the Australian Defence Materiel Organisation. The OAIC notes that, as agencies within the meaning of the Privacy Act, these entities (collectively referred to as Defence) are required to comply with the Information Privacy Principles (IPPs) when handling personal information.

11. The OAIC understands that current practice within Defence requires information about complaints of abuse and the name and personal details of respondents who have had formal action taken against them in relation to such complaints to be recorded in a central database – the Fairness and Resolution Unacceptable Behaviour Database (FRD) – that is managed by the Fairness and Resolution Branch of Defence.[2]

12. The OAIC notes that the purpose of the database is to assist in the identification of repeat behaviour. However, the information recorded in the FRD may also be taken into account for the purposes of career management and posting decisions.[3]

13. The Report points out that current practice within Defence is never to record the names of complainants in the FRD, even where formal action has been taken against a respondent in relation to a complaint. In addition, the name and personal details of a respondent are not recorded where no formal action has been taken against them. It appears, from the Report, that these restrictions are generally attributed to privacy considerations and, more specifically, to obligations that arise under the Privacy Act.[4]

14. The OAIC acknowledges the concern identified in the Report, that the information contained in the FRD is therefore not as comprehensive as it could be. Further, by not providing Defence management with all the relevant information, Defence is hampered in its ability to identify systemic issues of abuse (particularly in relation to serial low level perpetrators).[5]

15. The Privacy Act does not prescribe the types of information that may be collected by organisations and agencies. Rather, the Privacy Act outlines principles about the way in which personal information should be handled. This provides both agencies and

[2] See the Report, p 131; Defence Instructions (General) (DI(G)) PERS 35-3, Para 46.
[3] See DI(G) PERS 35-3, Para 47.
[4] See the Report, pp xxxiv and 132. The report notes that DI(G) PERS 35-3 explicitly recognises that Defence personnel responsible for handling complaints must comply with the Privacy Principles contained in the *Privacy Act 1988* (Privacy Act); see DI(G) PERS 35-3, Para 38.
[5] See discussion in the Report, pp xxxiv, 129-133.

organisations with the flexibility to tailor their information handling practices to suit their own needs. Accordingly, the IPPs do not prohibit the collection and use of personal information about individual complainants or respondents, provided that the information is handled in accordance with the principles in the Privacy Act. For example, an agency may only collect information that is necessary for a lawful purpose of the agency.

16. Given the sensitive nature of this type of personal information, the OAIC emphasises the importance of ensuring that Defence complies with the IPPs when handling personal information of this type and, in particular, that:
    - careful consideration is given to what, if any, collection, use or disclosure of personal information is necessary in relation to a complaint of abuse within Defence
    - there are clear instructions and/or policies in place within Defence, relating to the handling of complaints, that clearly outline the purposes for which personal information can be collected, and for which it may subsequently be used or disclosed
    - there are safeguards in place to ensure that personal information recorded in the FRD is handled and protected appropriately
    - personal information held in the FRD is accurate, up to date, complete and not misleading, and is fit for the purpose for which it was collected (for a more detailed discussion of this point see paragraphs 23-26 below).
17. The OAIC notes Issue 8 identified in the Report – namely that the proposed Phase 2 of the Review should include a discussion with the Fairness and Resolution Branch of Defence about the information that is currently available on the FRD with a view to expanding the information recorded there and increasing its availability and value to managers. The OAIC suggests that as part of any such discussions, specific consideration should be given to the issues identified at paragraph 16 above.
18. In view of the sensitive nature of the information held in the FRD, the OAIC is mindful of the significant detriment that ADF personnel could suffer if this information was used or disclosed inappropriately.[6] The OAIC also notes that if the information recorded in the FRD is expanded this risk is increased.
19. Accordingly, the OAIC recommends that Defence consider undertaking a Privacy Impact Assessment (PIA) in relation to the FRD to identify any privacy risks and ascertain what mitigation strategies may be applied. Matters that may be considered as part of a PIA include:
    - what personal information may be required to enable the FRD to operate effectively

[6] See the Report, p 134.

- whether or not this represents an unreasonable level of intrusion given the outcomes Defence is seeking to achieve through the operation of the FRD
- what safeguards need to apply to personal information contained in the FRD to mitigate any privacy risks identified by the PIA.[7]

The Defence Instructions (General) and the Privacy Act

20. Under section 9A of the *Defence Act 1903* the Chief of Defence and the Secretary of the Department of Defence are authorised to issue Defence Instructions (General) (DI(G)s) in relation to the administration of the ADF.
21. The OAIC notes that DI(G) PERS 35-3 states that Defence has an obligation to collect information in relation to management and reporting of unacceptable behaviour incidents and report it to the chain of command or line management and the Fairness and Resolution Branch. The Fairness and Resolution Branch records the information from complaints reported by commanders and managers on the FRD in accordance with DI(G) PERS 35-4.
22. The OAIC is unclear whether the DI(G)s carry the force of law and suggests that Phase 2 give consideration to this matter, with a view to providing greater certainty about Defence's obligations in relation to the handling of personal information in the FRD.

Finding 29 of the Report – ensuring personal information is accurate, up to date and complete

23. The OAIC notes Finding 29 of the Report – that the FRD has not been kept up to date and has, therefore, not provided up to date information for Commanding Officers and others in the ADF with the responsibility of managing the welfare of ADF members.
24. The OAIC is mindful of the serious consequences that might arise from the use or disclosure of information in the FRD for ADF personnel.[8] In these circumstances, the OAIC suggests that Defence should be satisfied as to the quality of the information in the FRD. Moreover, Defence has obligations under IPPs 7 and 8 to take reasonable steps to ensure that the personal information in the FRD is accurate, up to date and complete.
25. The OAIC suggests that before consideration is given to expanding the information recorded in the FRD (see paragraph 17 above) Defence should be satisfied that the mechanisms and processes it has in place for ensuring that such information is accurate, up to date and complete meet its obligations under the IPPs.
26. In addition, the OAIC notes that IPP 9 prohibits an agency from using personal information that it holds, except for a purpose to which that information is relevant.

[7] Office of the Australian Information Commissioner 2010, *Privacy Impact Assessment Guide*, available at <http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html>.
[8] See the Report, p 134.

The OAIC suggests that, to the extent that the information contained in the FRD is not up to date, it might not be relevant for the purpose for which it was collected, especially where there has been no finding of unacceptable behaviour.

B. Ensuring ADF personnel are fully informed

IPP 2 notice obligations

27. The OAIC emphasises the importance of ensuring that ADF personnel are fully informed about how their personal information relating to complaints of abuse within Defence will be handled. This is consistent with the obligations imposed on agencies by IPP 2 when soliciting personal information, namely, to ensure that individuals are generally aware of:
    - the purpose for which Defence is collecting the information
    - if the collection of the information is authorised or required by law, the fact that it is so authorised or required (including under the DI(G)s, if relevant)
    - any entity to whom personal information of this type is usually disclosed.

The use of personal information to provide advice to complainants on the outcome of their complaint

28. The OAIC notes that a number of individuals who reported incidents of abuse within Defence indicated to the Review that they were not informed about the outcome of their complaint. The Report stated that this was because Defence believes that providing this information to a complainant could breach the Privacy Act.[9]
29. IPP 11.1 prohibits an agency from disclosing personal information unless the disclosure falls within one of the five listed exceptions.[10] The OAIC considers that IPP 11.1 is likely to apply in the context of providing a complainant with information relating to the outcome of their complaint.
30. One of the exceptions is where the individual concerned is reasonably likely to be aware or has been made aware under IPP 2 (see discussion at paragraph 27 above) that personal information of that kind is usually disclosed to a particular entity.
31. The OAIC suggests that Defence may find it useful to consider the approach set out in Australian Public Service Commission *Circular 2008/3: Providing information on Code of Conduct investigation outcomes to complainants* (Circular 2008/3), developed in consultation with the OPC. Circular 2008/03 provides guidance about what information Australian Public Service agencies can or should give complainants about the outcome of their complaints. In particular, Circular 2008/3 states that:

[9] See the Report, p 145.

[10] For a discussion of the meaning of 'disclosure' see Office of the Privacy Commissioner 1996, *Plain English Guidelines to Information Privacy Principles 8-11*, available at <http://www.privacy.gov.au/materials/types/guidelines>, p 12.

- an agency should notify an employee involved in an alleged incident of abuse in writing that their personal information may be collected for the purpose of conducting the investigation and that the information might be disclosed to the person making the complaint
- if the agency has notified the individual that their personal information may be collected for the purpose of conducting the investigation or inquiry, and that it was possible that the information might be disclosed, it is likely that the disclosure will be permitted under IPP 11(1)(a).[11]

C. ADF personnel service records and Archives' open access period

32. The OAIC notes that the current practice within Defence is to make an entry on PMKeyS, Defence's personnel management database,[12] to indicate where action has been taken against a member for unacceptable behaviour if the complaint is established and considered sufficiently serious to warrant formal sanction.[13]
33. The OAIC notes that under section 31 of the *Archives Act 1983* (Archives Act) the National Archives of Australia (NAA) is required to make available for public access ADF service records that it holds where they are within the open access period, unless the information is exempt for one of the reasons set out in section 33(1) of the Archives Act, including that the information relates to the personal affairs of an individual. The Privacy Act does not apply to documents that are within the open access period.
34. The OAIC is mindful that where service records contain information, such as records of performance management and disciplinary action, ADF personnel and ex-ADF personnel may expect that this information will not be made public.
35. The OAIC suggests that Defence consider whether information held on PMKeyS would be likely to be released under the Archives Act and ensure that ADF personnel are fully informed about this, in accordance with the notification requirements of IPP 2.

[11] Australian Public Service Commission 2008, *Circular 2008/3: Providing information on Code of Conduct Investigation outcomes to complainants*, available at <http://www.apsc.gov.au/publications-and-media/current-circulars-and-advices/2008/circular-20083>.
[12] Australian National Audit Office 2005 *Audit Report No.8 2005–06: Management of the Personnel Management Key Solution (PMKeyS) Implementation Project*, available at <http://www.anao.gov.au/Publications/Audit-Reports/2005-2006/Management-of-the-Personnel-Management-Key-Solution-(PMKeyS)-Implementation-Project>, p 11.
[13] See the Report, p 129.