Australian Government

Department of Health

Submission to the Australian Information Commissioner
Disclosure of public servants' names and contact details under the FOI Act

Thank you for the opportunity to provide a submission on your discussion paper on Freedom of Information (FOI) and the disclosure of public servants' names and contact details.

The Department of Health (the department) has had the benefit of reviewing the submissions of the Australian Public Service Commissioner and agrees with the views expressed there. The department's submission does not repeat matters raised in that submission but rather focuses on additional aspects of the questions raised in the discussion paper.

Question One: *Does your agency have concerns about releasing the names and contact details of staff in response to FOI requests? If so, what are your concerns? Has your agency experienced any specific work health and safety issues as a result of a person's name or contact details being released in response to an FOI request?*

Department of Health response: Yes.

The department acknowledges there is a public interest in the right of access to documents held by Government and the value in providing information in order to promote better informed decision making and enable greater scrutiny, discussion, comment and review of Government activities.

Each FOI request made to the department is considered by an FOI delegate on a case-by-case basis, applying the *Freedom of Information Act 1982* and having regard to the Information Commissioner's guidelines.

At times, the application of an FOI exemption may mean the whole of a particular document is exempt and separate consideration of the names and contact details of public servants that may appear in the document is not necessary. At other times, it is necessary for the FOI decision maker to consider the names and contact details of public servants, and the following FOI exemptions may apply: s47E(c) (substantial adverse effect on the management and assessment of personnel), s.47E(d) (substantial adverse effect on agency operations), and s47F (personal privacy).

In practice, the names and contact details of staff are usually deleted as irrelevant to the FOI request (s.22). It is often not necessary to consider whether an FOI exemption applies as we raise the issue with the applicant (as part of the email acknowledging receipt of the FOI request) and they are not generally interested in this information.

However, we do have concerns the provision of names and contact details in documents released on FOI, particularly when placed on the internet, could be used to obtain unauthorised access to information or to cause financial or reputational damage to individuals or organisations, particularly when combined with other already available information.

The fraud and security risk due to release of names and contact details of staff affects:

- the department;
- individual staff in their personal capacity; and
- individuals and entities whose data is held by the department.

The discussion paper indicates that deletion could, instead, occur at a later stage, prior to release on the department's internet FOI disclosure log. The department does not adopt this approach as deletion of public servants names and contact details after FOI release to the applicant, and prior to placing the documents on the department's disclosure log, would not address the fraud and security risk. If this approach were adopted, the FOI applicant may choose to place the documents, containing the public servant names and contact details, on the internet.

The risk is a 'third party' risk which arises independently of an FOI applicant and accordingly our approach does not rely on an assessment of the behaviour of a particular FOI applicant.

For these reasons, the department's general practice is to delete non-SES names and contact details before releasing documents to the FOI applicant.

Publicly available information provides guidance about fraud and security risk associated with release of names and contact details on the internet. Some of the guidance is listed below:

- Identity Crime and Misuse in Australia 2017 Australian Institute of Criminology

  https://aic.gov.au/publications/sr/sr10

- 'Identity Crime' Australian Federal Police

  https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime#q6

- Stolen mobile phone numbers (unauthorised mobile phone number porting)

  https://www.acma.gov.au/Citizen/Phones/Numbers/Keeping-your-number/stolen-mobile-numbers

- Notifiable Data Breaches Scheme 12-month insights Report issued 13 May 2019

  https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-scheme-12-month-insights-report

- Information from the Australian Cyber Security Centre about preventing and mitigating data breaches

  https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/information-from-the-australian-cyber-security-centre-about-preventing-and-mitigating-data-breaches

- Australian Government Information Security Manual

  https://www.cyber.gov.au/ism

The risks discussed include identity fraud, phishing, spear phishing, spoofing, vexatious or abusive calls, brute force attack, malware, and impersonation. The risks affect individual staff in their personal capacity as well as the department and therefore the individuals and entities whose data is held by the department. There may also be risks to the physical security of staff in their personal

capacity, as officers of the department, and to individuals and entities whose data is held by the department.

Apart from the above general fraud and security risks associated with release of names and contact details on the internet, risks specific to an individual officer may arise from the publication of their details. Our approach, of not releasing the names and contact details of non SES staff, also minimises the risk to any particularly vulnerable department employee, whose personal circumstances need not be disclosed to the department as an employer, such as where an individual department employee is in a difficult relationship or a situation of family violence.

Particular roles may attract specific risks due to the nature of the work, for example regulatory and compliance action and decision-making. The Information Commissioner has previously agreed with decisions taken by the Therapeutic Goods Administration (the TGA), a Group of the department, not to release the names of internal, or external, scientific and clinical evaluators in connection with their assessment of a particular therapeutic good. The Information Commissioner agreed with the TGA that it is unreasonable to release such information as the disclosure would, or could reasonably be expected to, have a substantial adverse effect on the nature of the regulatory work being undertaken by the TGA and more specifically, the proper and efficient conduct of the operations of the agency.[1]

The impact on the department's regulatory and compliance work arises because of the potential impact on decision-makers of any disclosure of their personal information. The integrity of assessment and compliance processes relies on decision-makers being able to provide candid assessments without fear of reprisal or other adverse consequences. Concerns have been raised that should their identity be disclosed it would expose them to undue influence and pressure from third parties which would have the effect of undermining the integrity of the department's assessment and compliance processes. Simple association of an assessment, compliance activity and/or decision contrary to a third party's interests could also expose decision-makers to undue harassment, unnecessary anxiety and stress and may unjustifiably damage their professional standing. These anticipated effects could reasonably be expected to adversely affect future recruitment for the department and to substantially adversely affect the proper and efficient conduct of the department's operations.

Notably, such decisions are made within a wider framework of administrative law and in which applicants can seek merits and/or judicial review. Consistent with providing information to promote informed decision making and enable greater scrutiny and review of the government activities, such review processes contribute to achieving an appropriate degree of scrutiny of decisions. In considering the policy framework underpinning FOI, the department considers it is appropriate for the OAIC to take into account the broader administrative law framework in which FOI sits.

Question Two: *Have your agency's views on this issue changed over time? If so, please describe any factors that have affected your agency's approach, including technological, environmental or legal factors.*

Department response: Yes.

The technological and environmental aspects have evolved. Public reporting and analysis around fraud and security risks, and public messaging urging caution before disclosing names and contact details on the internet to actively minimise and manage risk, has increased as the incidence of internet related crime has grown.

---

[1] *TFS Manufacturing Pty Limited and Department of Health* [2016] AICmr 73 (31 October 2016); *'E' and Department of Health and Ageing* [2013] AICmr 14 (28 February 2013) (the 2013 case involved s.47F (personal privacy).

Question Three: *Does your agency advise staff, including contractors undertaking functions on behalf of the agency, that names and contact details may be released in response to an FOI request as part of your agency's training and induction programs?*

Department response: Yes.

Staff and contractors are made aware of FOI, and IT security obligations and we provide training on fraud and security risks, including risk mitigation strategies to avoid malicious unauthorised access to information by third parties. Staff and contractors are aware names and contact details may be released. However, staff of the department, individuals and legal entities whose data we hold, understandably expect the department to act to minimise their exposure to fraud and security risks.

Question Four: *How do you balance work health and safety considerations with the objects of the FOI Act, which include increasing public participation in Government processes with a view to promoting better-informed decision making and increasing scrutiny, discussion, comment and review of the Government's activities?*

Department response: Work health and safety considerations are very carefully assessed in the department as are the fraud and security risks to which employees of the department may be exposed.

Question Five: *If your agency considers that disclosure of a public servant's name or contact details will negatively impact their health or safety, what evidence do you require before deciding that their name or contact details are exempt from disclosure?*

Department response: The department considers fraud and security risks arise from the publication of names and contact details on the internet. In particular cases we also assess whether the nature and context of a request, the history of the applicant or level of personal information requested represents a heightened risk.

Question Six: *Do you consider the FOI Guidelines provide enough guidance for agencies when considering these issues?*

Department response: No.

The FOI Guidelines do not appear to address the fraud and security risks arising from the placement of information on the internet. Rather they appear to focus on risks arising from the past behaviour of a particular FOI applicant.

It would be helpful for the guidance material to acknowledge the general risks that arise and the need to mitigate these risks. Over time FOI, responsible workplace practices, technology and the internet evolve.

In particular, in light of the above, we query the following phrase in the FOI Guidelines, regarding the s.47F (personal privacy) exemption: 'Where public servants' personal information is included in a document because of their usual duties and responsibilities, *it would not be unreasonable to disclose unless special circumstances existed*'. The technological and environmental risks arising from placement of names and contact details on the internet arise in most, if not all, FOI requests.

We also query the level of focus on prior behaviour of a particular FOI applicant. Although this can be relevant in a particular case where there is evidence of prior concerning behaviour, it is not relevant to third party risk arising from the placement of names and contact details on the internet.

In addition, given the amount of public information available from FOI case law indicating the behaviour of particular FOI applicants can involve security or health and safety risks, the focus on

waiting until *after* evidence of security or work health and safety issues has arisen regarding a particular FOI applicant appears to ask the department, and FOI decision makers, to 'shut the barn door after the horse has bolted'.

The department considers it should actively minimise exposure to fraud and security risks arising from release of public servant names and contact details, in a manner that does not focus unduly on the behaviour of FOI applicants as a whole or particular FOI applicants, and this does not impact unduly on the objects of the FOI Act.

Third parties, or FOI applicants, seeking to connect with particular individual public servants in the department, through names and contact details, rather than following department established methods of communication, which these days often involves group email boxes and phone lines, does not appear to particularly support transparent and accountable service by the department for the public as a whole.

Question Seven: *In what circumstances do you consider that a public servant's personal information (name and contact details) are irrelevant to the FOI request?*

Department response: FOI applicants usually agree not to seek access to the names and contact details of non-Senior Executive Service (SES) staff, or mobile numbers of any staff, as they usually consider these details irrelevant.

The names of SES staff and their position, but not their mobile phone number, is already publicly known from the Government Online Directory and department organisational charts on the internet, as part of the public face of the department. The names of staff below the level of SES are usually not publicly known on the internet as part of the usual operational business of the department.

Each FOI request made to the department is considered by an FOI delegate on a case-by-case basis, applying the *Freedom of Information Act 1982*, and having regard to the Information Commissioner's guidelines. For this reason, in particular cases, an FOI exemption may apply to the name and contact details of an SES or non SES staff member.

Question Eight: *Where you have withheld the names and contact details of public servants, what impact does deleting this information from documents have on the time it takes to process FOI requests?*

Department response: This process does not impact on compliance with FOI decision making deadlines.