Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation	Department of Immigration and Border Protection Neil Phillips (see contact details below)
Contact details	Neil Phillips Acting Assistant Secretary Information Management Branch Corporate Support Division Corporate Group [contact details redacted]

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? NO

Your submission

The Department of Immigration and Border Protection (the Department) welcomes the opportunity to provide this submission in response to the Exposure Draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Bill).

The Department supports the introduction of a mandatory data breach notification scheme. The Department appreciates the significance of the changing data retention landscape, noting the advances in technology and the implementation of laws relating to data retention and the corollary increase in the amount of information that is being retained by entities.

Whilst the Department is supportive of the terms of the Bill, the Department would like to take the opportunity to highlight certain issues that it considers would benefit from closer analysis prior to finalisation of the Bill.

Passage of time and the practical effect ss 26WC and 26WD

The Department acknowledges that subsection 26WC(2) is intended to provide entities with a level of certainty in terms of the period available (ie 30 days) to assess the relevant circumstances and that it would be open to entities to choose to complete the assessment in a shorter period if practical. However, the Department also notes that the timing of any mitigating steps taken after a privacy breach incident may be critical to their success. The Department considers that it is reasonable to anticipate that any harm that is to flow from a particular data breach incident will have occurred by 'day 30', and is concerned about the prospect of such a period elapsing before the mitigating steps in subsection 26WC(1) are undertaken.

Following on from this, it would seem that in the event no harm has actually occurred within 30 days of a data breach incident, there would be a real question as to whether the incident will in fact result in a 'real risk of serious harm' to individuals.

Further, the Department considers that there may be a question about the practical application of section 26WD which enables the Commissioner to direct an entity to provide notification of a serious data breach. For example, in the event that an entity determines that there are not in fact reasonable grounds to believe a serious breach has occurred and therefore, does not provide a

statement to the Commissioner, notify affected individuals or otherwise comply with subsection 26WC(1), there would seem to be a real question as to how the Commissioner would actually become aware of a serious data breach of an entity.

Finally, the Department considers that timing will be critical with respect to applications made under subsection 26WC(8)(b) for exemption from the requirements in subsection 26WC(1). As a practical matter, the outcome of an application for an exemption under subsection 26WC(8)(b) would need to be communicated to the entity as soon as possible. However, the Bill currently does not specify a timeframe for a decision or otherwise indicate when such a decision should be issued.

The Department is concerned that in circumstances where the Commissioner refuses an application for an exemption, the passage of time could undermine the mitigation objectives served by subsection 26WC(1). For this reason, the Department suggests that the Bill be amended to require that in circumstances where an entity applies for exemption under subsection 26WC(8)(b), notice of a decision be given to the entity 'as soon as practicable'.

In addition, the Department recommends that the period of time commencing on the date that the application for exemption is made and concluding on the date that the written notice of the decision is given, is taken into account in any assessment of whether an entity has complied with the 'as soon as practicable' timeframe in subsection 26WC(1).

Timeframe for notifying Commissioner of a serious data breach

The Department is concerned about the lack of certainty with respect to the timeframe for an entity to undertake the steps in subsection 26WC(1)(a)-(d) after it becomes aware or ought reasonably to have become aware, that there are reasonable grounds to believe that there has been a serious data breach.

Subsection 26WC(1) indicates that the steps in subsections 26WC(1)(a)-(d) must be undertaken 'as soon as practicable'. Subsection 26WC(2) indicates that the 'as soon as practicable' timeframe includes the time taken by the entity to undertake an assessment of whether there are 'reasonable grounds' to believe that the circumstances in question amount to a 'serious data breach', so long as that assessment is carried out within 30 days.

On that basis it appears that the effect of the provisions as they stand is that:

- agencies must undertake the steps in subsections 26WC(1)(a)-(d) of the Bill 'as soon as practicable' after the entity becomes aware or ought reasonably to have become aware, that there are reasonable grounds to believe that there has been a serious data breach; and

- the ‘as soon as practicable timeframe’ includes a period of time of up to 30 days for the entity to assess whether there are in fact, reasonable grounds to believe that the circumstances in question amount to a ‘serious data breach’.

Therefore, whilst the Bill clearly defines expectations in relation to the time agencies may spend on the assessment of ‘reasonable grounds’, it is not so explicit in relation to the timeframe for undertaking the steps in s 26WC(1)(a) – (d).

In the Department’s view, it is necessary for there to be a clear and mutual understanding of what constitutes a suitable timeframe for undertaking the notification requirements in subsection 26WC(1). The Department is concerned that this is not sufficiently clear in the Bill. The Department suggests that this may be clarified by way of an amendment, or alternatively, by way of an explanation in the guidance material as to the meaning of the phrase ‘as soon as practicable’ in the context of s 26WC(1).

Interaction between subsections 26WC(12) and 26WD(7) and secrecy laws

Subsection 26WC(1) of the Bill requires that an entity must prepare a statement, provide a copy to the Information Commissioner and notify affected individuals as soon as practicable after the entity becomes aware or ought reasonably to have become aware, that there are reasonable grounds to believe that there has been a serious data breach of the entity. Subsection 26WC(12) provides that the requirement in subsection 26WC(1) does not apply to an entity to the extent that it would be inconsistent with a provision of a law of the Commonwealth that prohibits or regulates the use or disclosure of information.

The intention of the Explanatory Memorandum appears to be that secrecy provisions ‘prevail’ over the requirement to notify. However, the Department notes that there is still some uncertainty in relation to the interaction between subsection 26WC(12) and those secrecy provisions which make exception for disclosures which are ‘required or authorised by law’.

For example, Part 6 of the *Australian Border Force Act 2015* (ABF Act) prohibits the recording or disclosure of information unless, relevantly, the making of the record or disclosure is required or authorised by or under a law of the Commonwealth, a State or a Territory (see subsection 42(2)(c) ABF Act). Section 70 of the *Crimes Act 1914* contains a similar exception for circumstances where the disclosure is made with ‘lawful authority’.

On the basis of subsection 26WC(12) as it is presently drafted, there is a question as to whether the obligation in subsection 26WC(1) is a legal ‘requirement’ and therefore, not inconsistent with secrecy provisions such as section 42 of the ABF Act.

If (as the Explanatory Memorandum suggests) the intention behind subsection 26WC(12) is for secrecy laws to prevail, it may be beneficial to amend subsection 26WC(12) in a manner that

clarifies that the obligation in subsection 26WC(1) does not amount to a 'requirement by law'. Alternatively, this may be a matter for further clarification in the guidelines.

The comments above apply equally in relation to subsection 26WD(7) which operates in circumstances where compliance with a direction provided by the Commissioner under subsection 26WD(1) would be inconsistent with a provision of a law of the Commonwealth that prohibits or regulates the use or disclosure of information.

Matters to be specified in regulations

The Department notes that the Bill provides for regulations to specify particular situations that may be serious data breaches even if they do not necessarily meet the threshold of 'real risk of serious harm'. The Explanatory Memorandum to the Bill indicates that the regulations could cover situations such as the 'release of particularly sensitive information such as health records which may not cause serious harm in every circumstance, but should be subject to the highest level of privacy protection.'

The Department notes that at this stage, there does not appear to be any further guidance about the circumstances and types of information that may be captured by regulations. The Department suggests that further guidance on this point would assist agencies to prepare for the introduction of the mandatory reporting arrangements.

OAIC Guidelines

The Explanatory Memorandum states that it is anticipated that the Commissioner will update the current OAIC guidelines, *'Data Breach Notification: A guide to handling personal information security breaches'* or release other guidance material to reflect the amendments to the *Privacy Act 1988*.

The Department supports the prospect of further guidance material, and in particular, the Department would welcome specific guidance on the following matters:

- the meaning of the phrase 'real risk of serious harm' in the context of subsection 26WB(2). The Department notes that section 26WG of the Bill provides that 'real risk' means a risk that is not a 'remote risk' and subsection 26WB(3) contains a list of relevant matters which an entity may have regard to for the purposes of determining whether there is a 'real risk of serious harm' to an individual. Practical guidance on the meaning of the threshold term 'real risk of serious harm' is likely to assist agencies in complying with the amendments.

- when it may be reasonable for an entity not to take any steps to notify individuals of the contents of a statement provided to the Commissioner under subsections 26WC(1)(b) or 26WD(1)(b). Subsections 26WC(1)(c) and 26WD(1)(c) of the Bill provides that an entity is

required to take 'such steps *(if any)* as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates'. The Discussion Paper on Mandatory Data Breach Notification (the Discussion Paper) provides some guidance on the circumstances in which it may be reasonable for an entity to take no steps at all (eg it is not possible to identify each individual, the entity does not hold contact details for each individual, or the cost of notifying each individual would be excessive in all of the circumstances). In the case of a 'serious data breach' arising from loss of information covered by subsection 26WB(2)(c) of the Bill, it is unclear whether the extent of any risk of harm to individuals would be a relevant factor when considering the entity's obligations to notify. Again, practical guidance on this matter in the guidelines would assist agencies to understand the scope of their obligation under subsections 26WC(1)(c) and 26WD(1)(c).

- the meaning of the phrase 'ought reasonably to be aware' in the context of subsection 26WC(1). The Department notes that the Explanatory Memorandum provides some guidance on the meaning of the phrase 'ought reasonably to be aware' and suggests that the threshold would not be met in circumstances where the evidence of the breach or the resulting risk of harm to individuals is obscure or unreasonably difficult to determine. Further guidance on the meaning of this phrase would assist agencies to understand the scope of their obligations under subsection 26WC(1).

- the types of steps that individuals could take in response to a serious data breach. The Department notes that in accordance with subsections 26WC(3)(d) and 26WD(2)(d), the statement prepared by an entity must set out recommendations about the steps that individuals should take in response to the data breach incident. The Department suggests that it would assist agencies if further guidance was provided in the form of a non-exhaustive list of recommendations which may be appropriate to give to individuals in response to a data breach incident.

Preparation of a statement and interaction with subsections 26WD(7) and 26WC(12)

The Department notes that in accordance with subsections 26WD(7) and 26WC(12) an entity is not required to comply with the requirements in subsections 26WC(1)(b) – (d) or 26WD(1)(b) – (d) if (in general terms) to do so would be inconsistent with a secrecy provision. The Department notes that subsections 26WC(12) and 26WD(7) do not exempt agencies from the requirement to *prepare* a statement.

The Department appreciates that there may be merit in the process of preparing a statement in those circumstances, however, this is not clear in the Bill or extrinsic materials. Specifically, it is not apparent from the Bill or the extrinsic material why a statement would be required in

circumstances where there is no further requirement do anything with such a statement. This may be an anomaly which needs correcting in the Bill. Alternatively, the Department suggests that the purpose of a statement in these circumstances should be explained in the Explanatory Memorandum.

Resourcing within the Department

The Department does not consider that the introduction of the amendments contained in the Bill would significantly impact on the Department's current resourcing.

The Department's current engagement with the voluntary data breach notification scheme is very high and the Department has taken steps to implement recommendations made in the context of own motion investigations conducted by the Commissioner.

The Department has established systems in place to facilitate reporting of data breaches. Under the current arrangements in the Department:

- business areas report breaches to the Department's Privacy and Reviews Section
- the Privacy and Reviews Section analyse the reported breaches and undertake the requisite assessments (including initial assessments as to the risks associated with the breach and post action assessments)
- the OAIC and affected individuals are notified as appropriate.

Given the arrangements that the Department currently has in place to respond to and manage data breach incidents the Department considers that the mandatory reporting scheme will not require a significant change to its current processes.