# 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**<br><br>*(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)* | Terry Darling |
| **Contact details**<br><br>*(one or all of the following: postal address, email address or phone number)* | [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The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.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? YES / NO

# Your submission

*Insert your text here and send the completed submission to the Attorney-General's Department, preferably via privacy.consultation@ag.gov.au*

### 1. Need for Clarification of key Terms

The current use of the phrases "serious data breach", "serious harm" and "real risk" within the proposed legislation are not well defined.

A critical consideration in determining the seriousness of a breach and whether to notify affected individuals should be whether the breach discloses "exploitable" information. That is information that directly enables further economic, social or reputational damage to an individual or organisation through other future incidents. Obvious examples of such exploitable information would include banking credentials, ATO and other government identifiers.

A beneficial characteristic, however, of referring to exploitable information is that such information is typically associated with a non-trivial ability by an affected individual or organisation to mitigate the potential damage e.g. by changing the credential or taking other mitigating action.

Reference to exploitability or expectation of further consequential impact will foster greater response to breaches by affected parties, which is the ultimate goal of the proposed legislation.

The use of both "psychological harm" and "emotional harm" in Section 26WF appears un-necessary and neither are readily quantifiable. In terms of actual consequential effects of a data breach to an individual these possible harms might best be subsumed under harm to reputation.

While the legislation is to be affirmed for attempting to relate a need to notify to the issue of harm, the effect of any failure to more closely define these keys terms will be to increase the level of notifications and potentially further overload the Office of the Australian Information Commissioner (see Section 4 below)

### 2. Legislation should include Potential or Suspected Breaches

The use of the phrase "ought reasonably to be aware" or similar statement to refer to potential or suspected data breaches should definitely remain in the legislation.

The evidence from historic security incident data is that many incidents, which eventually prove to be highly serious, are either initially dismissed as not fully confirmable or the nature and extent of incidents is greatly expanded as investigations and response are performed.

Accordingly entities should be required to notify potential breaches as these are these are suspected to have occurred. The small risk of potential over-reporting (of false positive incidents) outweighs the risks and impacts of under reporting (of false negative incidents) in the writer's direct experience.

## 3. Definition of Security Measures That Exempt Notification

The current proposed definition of protective security measures under Division 2, Para. 3f should be elaborated to include examples of specifically permitted measures that exempt notification.

For example, one such exemption could useably comprise the use of "effective encryption". This could be defined as: "encryption using (i) a publicly recognised encryption protocol or product for example any ASD Approved Cryptographic Protocol, US National Institute of Standards protocol or (ii) any cryptographic product on the ASD Evaluated Products List in combination with (iii) adequate key management and access controls so as to prevent the data being decrypted."

Generally, the inclusion of more specific exemptions based on definable best security practice would make the proposed legislation more consistent with a number of other national data protection and breach notification statutes.

## 4. Resourcing of the Office of the Australian Information Commissioner

Given the funding cuts undertaken in the 2014 and 2015 Federal Budgets[1] to the OAIC it is the opinion of the writer that the Office is not currently resourced to perform the important administrative functions required by the proposed legislation.

The legislation or other Parliamentary or regulatory measures should ensure that the Office is adequately resourced to perform its role as required.

## 5. Recognition of Wider Potential Benefits

The ultimate benefit of the legislation may be that management will come to realise that their organisations cannot comply with the statute – that is notify occurrence of a breach – without making other significant investments in information security.

That is, the legislation may provide the incentives to make the "upstream" investments in capabilities that actually minimise the likelihood and impact of incidents in the first place and then, for those incidents that necessarily cannot be avoided (as inherently some will still occur), to perform effective incident response and root cause elimination.

[1] For example see:http://www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273