Australian Government
Attorney-General's Department
Deputy Secretary
Civil Justice and
Corporate Group

15/4059

Ms Tanja Cvijanovic
Executive Director
Office of Best Practice Regulation
Department of the Prime Minister and Cabinet
1 National Circuit
BARTON ACT 2600

Email: helpdesk-OBPR@pmc.gov.au

Dear Ms Cvijanovic

Regulation Impact Statement Privacy Amendment (Notifiable Data Breach) Bill 2016–final assessment second pass

I am writing in relation to the attached Regulation Impact Statement (RIS) prepared for the Privacy Amendment (Notifiable Data Breaches) Bill 2016. The regulatory burden to business, community organisations and/or individuals has been quantified and offsets have been identified and quantified using the Regulatory Burden Measurement framework. These have been agreed with your office.

I am satisfied that the RIS addresses the concerns Mr Tony Simovski, A/g Deputy Executive Director, Office of Best Practice Regulation (OBPR), raised in his letter of 19 September 2016. Specifically, you stated the RIS should better identify the size of the problem in relation to the failure to notify individuals of serious data breaches and the RIS should be transparent where there is a lack of evidence of this failure and statements summarising the net benefit as significant should reflect this uncertainty. In response the RIS has been amended to include a new section that discusses the lack of consensus and limited evidence on the underreporting of breaches to individuals. The section also makes clearer the possible nexus between the possible underreporting to individuals, identity theft and crime and why data breaches are a problem. The RIS has been amended to qualify the nature of the level of the net benefit to reflect the uncertainty around whether there is an underreporting of serious data breaches to individuals.

You stated the RIS should identify the existing mechanisms that help to address the problem. In response the RIS has been updated to include information about the remedies available under the *Privacy Act 1988* (Privacy Act) should an individual be the subject of a data breach, including if they incur a loss as a result of the breach.

You stated the RIS should clarify what other processes are currently underway to address the significant issues of non-compliance and identity theft. In response the RIS has been updated to

include reference to what remedies are available under the Privacy Act in the event that an entity subject to the Privacy Act is in breach of the information security requirements in Australian Privacy Principle 11. In addition, the RIS has been updated to include information on the Australian Government's National Identity Security Strategy that aims to prevent identity crime, assist victims to restore their compromised identities and to enhance the security and integrity of the systems used by government agencies to issue and maintain documents used by Australians as evidence of identity.

You stated the RIS needs to state the status of the RIS at each major decision point. In response the RIS has been updated to include a new section outlining the status of the RIS at each major decision point. You stated that the regulatory burden will need to be formally agreed with the OBPR prior to the second pass assessment. The Department has liaised with the OBPR and the regulatory burden has been finalised which the OBPR has formally agreed with. The burden will be offset by a number of measures as specified in the attached RIS. The estimated regulatory cost of the introduction of a mandatory data breach notification scheme has increased from the estimated regulatory cost contained in the RIS circulated during the 2015−16 consultation (consultation RIS). This increase does not reflect a change in the proposed scheme nor is it a result of consultation submissions. Rather, it reflects the advice from the OBPR, adopted in the RIS, that the approach taken to non-compliance costs in the consultation RIS was inconsistent with the Office of Deregulation's *(Revised) Guidance Note – Regulatory Impacts from Non-Compliance and from the Administration of Courts and Tribunals*.

You stated the one page RIS summary will need to be formally agreed with the OBPR prior to the second pass assessment and that the RIS summary should more clearly indicate that a number of submissions from businesses to which the legislation applies are either opposed or have little problem with the existing arrangements. In response the one page RIS summary has been updated to be more consistent with the RIS and include a summary of businesses that were opposed to the legislation or thought the current voluntary notification system sufficient. The OBPR has formally agreed with the one page RIS summary.

Accordingly, I am satisfied that the RIS now meets best practice consistent with the Australian Government Guide to Regulation.

I submit the RIS to the Office of Best Practice Regulation for formal final assessment.

Yours sincerely

Iain Anderson
28 September 2016