From:	Grant Ozolins
To:	Assistance Bill Consultation
Subject:	Submission to the Assistance and Access Bill
Date:	Monday, 10 September 2018 10:03:49 PM

Dear Sir / Madam,

While the fight against illegal activities is laudable, the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 relies on a fundamentally mistaken notion, namely, that it is possible to weaken encryption without making it useless.

There are essentially two methods by which weakening communications can be rendered readable by third parties (for the purposes of this submission, the third party is the relevant statutory authority that wishes to have access to that communication); these are by either using a cryptographically weak cypher, or by adding "backdoors" in source code that implements encrypted communications.

Both of these approaches render encryption useless for the many purposes for which it is necessary - allowing secure access to business resources, conducting commerce, and providing reasonably secure communication for citizens, all of which are very important in an age where unscrupulous actors are both able and willing to exploit any weakness for the purposes of fraud and illicit commercial gain.

By mandating cryptographically weak encryption, encryption is rendered meaningless. By adding "backdoors" to application source code, you introduce vulnerabilities that are likely to be exploited by malicious third parties.

In both cases you might enable access to encrypted communications for the purposes of crime fighting, but render Australia's businesses and citizens unable to conduct commerce and personal business securely. Not only would such measures make Australia the laughing stock of the online world, it would also make Australia a prime target for both private and state cyber criminals.

Your Sincerely,
Timothy Grant Ozolins