Australian Government
Department of Defence

Senator Jenny McAllister
Chair, Senate Standing Committees on Finance and Public Administration
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Senator

SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION INQUIRY INTO THE DIGITAL DELIVERY OF GOVERNMENT SERVICES.

Thank you for the opportunity to make a submission to the inquiry into the digital delivery of government services. The Australian Signals Directorate (ASD) can assist the Committee in its considerations of item a(ii) from the terms of reference:

> **whether planned and existing programs are able to digitally deliver services with due regard for security.**

I will limit my response in this regard to this question only.

One of ASD's functions, which are defined in the *Intelligence Services Act 2001*, is to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means.

ASD performs this function in part by making advice available to government agencies, allowing them to consider the cyber security aspects of all programs regardless of what stage of planning they are at. This advice includes but is not limited to the following:

The Australian Government Information Security Manual (ISM)

ASD has a role prescribed by the Attorney-General's Protective Security Policy Framework to define the information security requirements for government networks, systems and online services. ASD delivers this through the publication of the ISM.

The ISM helps Australian government agencies to apply a risk-based approach to protecting their information and systems. The controls in the ISM are designed to mitigate the most likely and highest severity threats to Australian government agencies.

UNCLASSIFED

Strategies to Mitigate Cyber Security Incidents and the *Essential Eight*

ASD's flagship *Strategies to Mitigate Cyber Security Incidents* is a prioritised list of practical actions government agencies can take to make their information systems and online services more secure.

Each agency should customise these strategies to fit its particular risk and resource profile. At a minimum, ASD recommends that all government agencies – and all Australian businesses – implement the *Essential Eight* package of strategies. This package establishes a cyber security baseline by protecting against:

- targeted cyber intrusions
- ransomware
- malicious insiders
- business email compromise
- threats to industrial control systems
- adversaries who have destructive intent.

While cyber security threats are constantly evolving, the advice that ASD provides to Australian government agencies, when applied by an agency head as the system owner, should result in digital services that have been designed with due regard for security.

I continue to be available to work with the Committee on this inquiry. My contact for all matters relating to ASD's information security mission is Mr Chris Brookes, Acting Deputy Director for Cyber and Information Security and Acting Coordinator of the Australian Cyber Security Centre, who can be contacted on

Yours sincerely,

Dr Paul Taloni
Director
Australian Signals Directorate
Department of Defence

29 September 2017