Australian Government
Attorney-General's Department
Intelligence and Identity Security Division

16/13472-03

19 June 2017

Senator Dean Smith
Committee Chair
Joint Committee of Public Accounts and Audit
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Chair

Cybersecurity Compliance – Inquiry into Auditor-General's report 42 (2016-17)

I am writing to provide supplementary information following the hearing on 2 June 2017 of the Joint Committee of Public Accounts and Audit – Inquiry into Auditor-General's report 42 (2016-17) *Cybersecurity Follow-up Audit*.

During the hearing, I explained the role and level of cybersecurity responsibility of the Attorney-General's Department in administering the Protective Security Policy Framework (PSPF) and the annual compliance reporting on the implementation of the PSPF provided by applicable entities. I would like to provide the Committee additional context on the applicability of the PSPF and the annual compliance reporting to inform the inquiry.

All non-corporate Commonwealth entities (NCCEs) under the *Public Governance, Performance and Accountability Act 2013* are required to report annually on the implementation of the PSPF. Corporate Commonwealth entities and Commonwealth companies are not required to report against the requirements of the PSPF, but some elect to report annually where they apply the PSPF as better practice. In the 2015-16 reporting period:

- ninety-two of the 94 current NCCEs reported against the PSPF requirements, and
- sixty-five percent of NCCEs reported compliance under the PSPF's information security requirement, INFOSEC4, which includes implementing the 'Top 4' strategies to mitigate targeted cyber intrusions.

Should the committee require further information on implementation of the PSPF, please contact the action officer for this matter, Doug Rutherford, by phone on [redacted] or by email at [redacted]

Yours sincerely

[redacted]

Andrew Rice
Assistant Secretary
Identity and Protective Security Branch
P: [redacted]