Australian Government

Attorney-General's Department

MC20-015710

24 May 2020

Mrs Lucy Wicks MP
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600
jcpaa@aph.gov.au

Dear Mrs Wicks

Thank you for your letters of 24 April 2020 and 19 May 2020 to the Attorney-General regarding the Joint Committee of Public Accounts and Audit's (the Committee) *Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20)* and the Committee's invitation for the Attorney-General's Department to make a submission to the Inquiry. The Attorney-General has requested that I respond to you on his behalf.

Cyber security is an important priority for the Australian Government.

The Attorney-General's Department is responsible for setting Government protective security policy guidance, including for information security, through the Protective Security Policy Framework (PSPF). The PSPF assists Commonwealth entities to protect their people, information and assets, at home and overseas. The core requirements for information security are set out in policies 8 to 11 of the PSPF, covering *Sensitive and classified information*, *Access to information*, *Safeguarding information from cyber threats* and *Robust ICT systems.* The PSPF is publicly available at www.protectivesecurity.gov.au/.

The Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD) leads the Australian Government's operational cyber security capability. The ACSC is responsible for producing the Australian Government Information Security Manual (ISM), which is referenced in the PSPF as the key source of guidance for organisations in applying policies 10 and 11 (*Safeguarding information from cyber threats* and *Robust ICT systems*). The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.

In relation to cyber security, the PSPF requires non-Corporate Commonwealth Entities to implement four of the ACSC's eight essential mitigation strategies listed in the *Strategies to Mitigate Cyber Security Incidents* (known as the *Top Four*) – and strongly recommends the adoption of all eight. Entities must also consider other strategies included in the ACSC's *Strategies to Mitigate Cyber Security Incidents*.

These requirements are set out in PSPF policy 10 *Safeguarding information from cyber threats*. Policy 11 *Robust ICT systems* includes requirements about safeguarding information and communication technology (ICT) systems to support the secure and continuous delivery of government business.

As noted in your letter, the Minister for Defence recently tabled the *Report to Parliament on the Commonwealth's Cyber Security Posture in 2019* in Parliament. This Report provides the most current information on Commonwealth entities' cyber security posture. To ensure an integrated approach to information about cyber security, the Report included information about the PSPF, and high level results from the 2018-19 PSPF self-assessments relevant to entities' cyber security posture.

The security management approach to annual reporting was strengthened as part of the 2018 PSPF reforms. It is based on the entity's overall security position within its specific risk environment and risk tolerances. The new maturity self-assessment model supports each entity to consider the elements of its security capability. This includes:

- implementation and management of each PSPF core and supporting requirement
- achievement of security outcomes for governance, information, personnel and physical security
- security risks to people, information and assets
- risk environments and tolerance for security risks
- strategies and timeframes to manage identified and unmitigated risks.

As individual Commonwealth entities are responsible for their assessment in light of their risk environment, questions regarding PSPF implementation within an individual entity are best directed to that entity.

Thank you again for the opportunity to provide input to the Inquiry. The action officer for this matter is Elizabeth Brayshaw who can be contacted on [redacted]

Yours sincerely

[redacted]

Sarah Chidgey
Deputy Secretary
Integrity & International Group

[redacted]