Australian Government
Attorney-General's Department

Deputy Secretary

Civil Justice and Corporate Group

[redacted]

9 November 2017

PGPA Review
Attention: Review Secretary
Department of Finance
One Canberra Avenue
FORREST ACT 2603

Dear Ms Balmaks

Submission to the Independent Review of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act)

The Attorney-General's Department welcomes the opportunity to provide input to the Independent Review of the PGPA Act and Rule.

The department supports the work the Department of Finance has done to streamline the PGPA Act and ensure its applicability to all Commonwealth Entities. Given that it has operated for three years some issues have been identified that if remediated have the potential to further streamline the department's operations. These are outlined in the department's submission (refer **Attachment A**).

Further correspondence in relation to this matter can be sent to [redacted]

Yours sincerely

[redacted]

John Reid

ATTACHMENT A

Independent Review of the Public Governance, Performance and Accountability Act 2013 (PGPA Act) and Rule

Attorney-General's Department submission

Introduction

The Minister for Finance, Senator the Hon Mathias Cormann, in consultation with the Commonwealth Parliament's Joint Committee of Public Accounts and Audit, commissioned an independent review of the *Public Governance Performance and Accountability Act 2013* (PGPA Act) and Rule in accordance with section 112 of the PGPA Act. The review will report to Minister Cormann in the early part of 2018.

On 9 October 2017, the Independent Review wrote to the Attorney-General's Department (the department) welcoming observations and input on the PGPA Act and Rule and how they affect the arrangements for and operations of the department. Following consultation across the department the following issues have been identified for consideration by the Independent Review.

Commonwealth Fraud Control Framework

The department administers the Commonwealth Fraud Control Framework, which sits under the *Public Governance Performance and Accountability Act 2013* framework. The fraud framework's purpose is to provide a coherent system of governance and accountability across entities for protecting public resources from fraud. The fraud framework consists of a rule (section 10 of the *Public Governance Performance and Accountability Rule 2014*), a policy and supporting guidance.

The fraud framework commenced in 2014 and reflects a shift to principles based regulation focusing on entities engaging with their risks rather than focusing on compliance. The fraud framework was updated further in 2016/17 to implement recommendations from the Belcher Review to remove duplication and streamline guidance. Feedback from entities about the fraud framework has been positive indicating support for the principles-based approach and noting the importance of the consistent legislative basis for fraud control applying to all entities. Australian Institute of Criminology (AIC) reports indicate that there was over $1.2 billion in reported fraud between 2012-2015 which has been handled by entities under the current and previous fraud frameworks.

Incorporating anti-corruption into the existing fraud rule

While the department supports the current fraud control arrangements, several entities have raised questions over whether the fraud framework should cover corruption. While there are significant levels of internal fraud identified in AIC reporting, the Australian Public Service Commission's *State of the Service Report 2015-16* indicated higher levels of corruption observed by employees, some of which does not overlap with fraud, such as nepotism and cronyism. These aspects of corruption fall outside of the fraud framework. As a result, measures to address these matters are not always given the attention warranted in entities' risk management arrangements. Entities are reporting confusion about handling corruption and sometimes either not addressing it or having a duplicative or separate framework for it.

Given the overlap and links between corruption and fraud risks and controls, and the impact of corruption on government integrity, accountability and assets, consideration could be given to including corruption in the fraud framework. An integrated approach to anti-corruption was recommended the *Independent Review of Whole-of-Government Internal Regulation* in 2015 by Ms Barbara Belcher

(Belcher Review) (recommendation 21.3). This could reduce red tape within entities as well as strengthening anti-corruption arrangements. Expanding the fraud rule to include corruption could also be particularly applicable to recommendation 1 of the *Select Committee on a National Integrity Commission Report* of September 2017, which recommends that the Commonwealth prioritise strengthening the national integrity framework to make it more coherent, comprehensible and accessible.

Incorporating protective security policy into the PGPA Act framework

The department recommends incorporating principles-based security obligations within the PGPA Act framework. Incorporating security obligations would:

- provide a legislative underpinning for protective security
- increase coherence between the Protective Security Policy Framework (PSPF) and the PGPA Act
- provide a consistent approach to accountable authority obligations, and
- address gaps in accountability across entities.

Security is a critical part of delivering the business of government. Traditionally security has been considered separately to financial management and for this reason was not considered for inclusion in the establishment of the PGPA Act. However, this leads to a gap in achieving the PGPA Act's objectives of 'establishing a coherent system of governance and accountability across Commonwealth entities' and 'to use and manage public resources properly'.

The PSPF is a policy of the Australian Government that sets out a framework for governance, accountability and performance on security within government. The PSPF relies on the PGPA Act to require non-corporate Commonwealth entities to apply the policy. There is no specific legislative underpinning for the policy.

While the PGPA Act requires entities to establish systems to manage risk and to act in a manner that is 'not inconsistent' with the PSPF, it does not impose duties or requirements concerning securely managing public resources. In addition, accountable authorities of corporate Commonwealth entities are **not accountable** for managing security through government policy unless required, to **act consistently** with a 'government policy order' in accordance with section 22 of the PGPA Act. Even if an order were made, it would not be able to be delivered coherently across entities due to the constraints imposed by the PGPA Act.

The department is currently implementing reforms designed to simplify the PSPF, transforming it to a principles and risk-based model which will better align with the PGPA Act and reinforce the objectives of both core risk-based frameworks.

Attachment B provides further details in support of this proposal and on possible options for providing a legal basis for security obligations.

Current requirement GOV-11 of the PSPF requires agencies to establish a business continuity management program to provide for the continued availability of critical services and assets, and of other services and assets when warranted by a threat and risk assessment. This requirement is likely

to be removed under current reforms. It would be helpful to include this requirement in the PGPA Act to give some authority and mandate to agency business continuity programs to ensure sufficient ongoing resources. Given that the risk of unauthorised access or misuse of information is one of the highest risks for many agencies, it would be helpful if Section 16 of the PGPA Act be extended to include reference to business continuity.

Commonwealth Grants Rules and Guidelines

The Commonwealth Grants Rules and Guidelines (CGRGs) are issued under section 105C of the PGPA Act to improve the transparency and accountability of grants administration.

Business units in the department have found that there remains some difficulty in undertaking certain aspects of grants administration with respect to the current CGRG's to ensure that PGPA Act obligations are met. These requirements change depending on whether the grant is one-off or recurring, and depending on the program's level of constitutional or program risk. The department has received differing advice about which Commonwealth agencies need to review and sign-off guidelines and risk assessments.

There is no single Commonwealth risk assessment template for the establishment of a grants program or a pro-forma contractual template where a program is assessed as high risk. While the department's risk assessment tool has been approved by the Department of Finance, risk assessment is managed differently across the Commonwealth, including by the centralised Commonwealth grants hubs which use a different risk assessment tool. Each agency has its own specific practices, different risk appetite and risk tolerance levels. A clearer framework for division of responsibility in relation to risk management between the owner of the policy function and the grants administrator (where this is a centralised hub) would be beneficial. Currently the Department of Prime Minister and Cabinet provides individual advice in relation to the application of risk management for all general grants programs. Clarity about what is a sufficient risk assessment may assist in the process of establishing new grants programs, particularly when operating within limited timeframes.

Performance Reporting

The department agrees that robust quality performance information, as sought under Part 2-3 of the PGPA Act and PGPA Rule, is critical to transparent and accountable government. The suite of documents, now including a Corporate Plan and Annual Performance Statement, should provide readers with a clear line of sight between what was intended and what was achieved, allowing judgements to be made on the public benefit generated by public expenditure. However, given the infancy of the performance framework and the ongoing challenge across entities to develop robust performance criteria, this still has some way to go.

The department notes the following challenges:

- **Development of performance criteria** – determining one high level criterion that is both meaningful and appropriate for a program that encapsulates a diverse range of tasks is extremely challenging. It is also difficult to identify appropriate performance criteria and

measures where a large proportion of the department's work deals with the formulation of policy (seeking to measure an outcome), rather than delivery of programs (an output). There are also challenges in balancing the resourcing and skills required to develop and undertake performance measurement versus the actual delivery of the work. This was recently raised at a hearing of the Joint Committee of Public Accounts and Audit (JCPAA) on 6 September 2017.

- **Guidance materials** – Although support by the PMRA staff at the Department of Finance has been positive, there has been an ongoing lack of clarity about the role of an audit committee with respect to the performance framework. The definition of 'appropriateness' and 'fit for purpose' continues to be the subject of much discussion. Audit committees are well-versed in providing assurance for financial statements. However, difficulties have arisen in trying to apply a similar process to non-financial performance information. Also, as discussed at the JPCAA hearing, audit committees who have traditionally audited financial statements may not have the skills to provide this assurance.
- **Earlier delivery and tabling of the annual report** would present significant challenges. As an entity operating on a financial year basis, it is not possible to confirm the required financial and non-financial content of the annual report until the middle of August. Other factors such as the availability of ANAO officers to consider and confirm financial information, the availability of audit committee members to sign off financial statements and annual performance statements, and the small printing market in Canberra would present significant logistical challenges to bringing forward the delivery and tabling date for the annual report.

AGD submission Attachment B
Incorporating protective security into the *Public Governance Performance and Accountability Act 2013* framework

The Protective Security Policy Framework (PSPF) is policy of the Australian Government issued by the Attorney-General. It sets out a framework for governance, accountability and performance to enable the business of government by securing public resources. The PSPF is risk-based and provides flexibility for entities to mitigate risks that might affect their business and assurance that entities engage with security using a consistent framework. The PSPF requires non-corporate Commonwealth entities (NCCEs) to manage risks to government resources, specifically information, assets and personnel. It also establishes a process for reporting on compliance with the mandatory requirements.

The PSPF does not have a legislative basis but is set as a government policy in accordance with the Administrative Arrangement Orders for 'protective security policy and coordination'. Under section 21 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), NCCEs are required to act in a manner that is 'not inconsistent' with the PSPF. It reflects better practice for corporate Commonwealth entities (CCEs) and Commonwealth companies, and is required to be applied by contractors to government.

The lack of a legislative basis for the PSPF poses a challenge for holding entities accountable for potential risks to government and to ensure policy is delivered with appropriate authority. Ineffective protective security undermines government business objectives and creates risks to the management of public resources. A risk-based approach enables NCCEs to apply mandatory requirements flexibly, but does not ensure they meet the minimum necessary required to manage security risks in a way that supports government business. As the PSPF only applies to NCCEs, there are challenges ensuring trust and confidence to share sensitive and classified information with CCEs. The lack of policy oversight means CCEs may not devote resources appropriately to mitigate security risks. There is also a lack of transparency as most CCEs do not voluntarily report on their compliance with the PSPF to the department. This translates to poor security culture and increased risks to Commonwealth public resources.

A recent example illustrating the limitations of government policy is set out in the Joint Committee of Public Accounts and Audit *Report 467: Cyber Security Compliance*. The report highlights that compliance with cyber security requirements of the PSPF needs to improve across government (the report cites 65 per cent of NCCEs report compliance). The report makes recommendations to improve regulation of entities handling of cyber security, including extending the existing PSPF mandatory requirements and making them mandatory for all entities under the PGPA Act.

The PSPF is currently being reformed to simplify and streamline the PSPF and address recommendations of the *Independent Review of Whole-of-Government Internal Regulation* of 2015 (Belcher Review). Amongst recommendations relating to the PSPF, the Belcher Review noted that the PSPF would benefit from being made more consistent with the PGPA Act framework.

On 3 May 2017 the Secretaries Board approved the department developing reforms to the PSPF over 2017-18 for implementation from 1 July 2018. This included AGD and the Department of Finance exploring options to incorporate appropriate security requirements as part of the implementation of the

PSPF reforms, including options that apply to accountable authorities within the PGPA Act framework.

Possible options

Providing legislative authority for the PSPF by incorporating relevant principles-based requirements on accountable authorities under the PGPA Act would improve coherence of requirements and duties for accountable authorities. Consistent, principles-based obligations would apply across all entities, not just entities bound by government policy. This simplification would enhance efficiency and reduce red tape by removing duplication. Possible options to achieve this are set out below.

1) Incorporate a new duty to manage public resources securely

Incorporating a new duty for accountable authorities and officials to manage business securely would supplement existing duties and align with other accountability duties of the PGPA Act. A new duty could frame additional principles-based requirements in a new PGPA Rule.

2) Develop a 'Protective Security Rule' in the PGPA Rule

A new rule could be incorporated into the PGPA Rule based on the Fraud Rule (section 10).

This option would place legal obligations on both NCCEs and CCEs and provide a legislative basis for supporting policy and guidance. The new section would set out minimum principles-based requirements for protective security applying to accountable authorities and entities (an indicative draft example is set out below). Prescriptive requirements in the PSPF could be removed or converted into guidance. This approach was successfully implemented for the Fraud Control Framework (see commentary in the Belcher Review, volume 2 at page 125).

3) Integrate security into the Fraud Rule

Protective security could be integrated into the fraud rule in section 10 of the PGPA Rule. As with option 1, this will capture both NCCEs and CCEs.

The Belcher Review recommended that the Commonwealth Fraud Control Framework and anticorruption measures could be integrated into the PSPF and better aligned to achieve more effective outcomes through risk-based decision-making (rec 21.3). Although the Belcher Review suggested integrating protective security and fraud (rec 21.3), this would be problematic as the obligations would not neatly align due to different focuses.

4) Continue to pursue a Government Policy Order

The department has previously explored extending the PSPF to CCEs and wholly-owned Commonwealth companies through a Government Policy Order (GPO). There are significant challenges in complying with requirements for implementing a GPO, including consultation requirements effectively requiring agreement by those entities. There is also a risk of inconsistent obligations could develop (a GPO would be frozen in time and not responsive to policy changes). A GPO could be used for:

- specific obligations that fall below requirements that would be included in a rule, or
- wholly-owned Commonwealth companies that would not be covered by a PGPA Act rule.

5) Standalone legislation for protective security

Developing primary legislation for protective security is not necessary given PGPA Act requirements, and espionage and secrecy legislation offences criminalise conduct in breach of the policy.

6) Status quo

Security would continue to be dealt with as a governance and accountability framework outside of broader government accountability requirements.

PSPF requirements can be aligned with PGPA Act requirements to the extent possible, but the issues of ensuring entities act consistently with the policy and differential accountability based on entity type will remain. CCEs would only be bound if a 'government policy order' is established. The lack of legislative obligation to comply with the PSPF would continue to impact entity security cultures and increase risks of compromise of classified government assets.

Example of a Protective Security Rule
Part 2-2—Accountable authorities and officials

Division 1—Requirements applying to accountable authorities

X Securing public resources

Guide to this section

The purpose of this section is to ensure that there is a minimum standard for accountable authorities of Commonwealth entities for managing protective security risks to their entity. It is made for paragraphs 102(1)(a), (b) and (d) of the Act.

(1) The accountable authority of a Commonwealth entity must take all reasonable measures to protect people, information and assets of the entity including by:

Governance

(a) having appropriate protective security governance structures, including measures that:

(i) determine appropriate risk tolerance and managing security risks;

(ii) develop an appropriate management structure to ensure accountability, investigation and response; and

(iii) develop an appropriate mechanism for monitoring and reporting the entity's level of protective security maturity.

Information

(b) maintaining the confidentiality, integrity and availability of all official information through:

(i) appropriately classifying and limiting access to sensitive information;

(ii) safeguarding of information from cyber security threats; and

(iii) maintaining appropriate information and communications technology systems.

Personnel

(c) ensuring officials are eligible and have ongoing suitability to access public resources, including meeting an appropriate standard of integrity and honesty; and

Physical

(d) maintaining effective physical security measures for their people, information and assets.