From: MAS Panel <MASPanel@finance.gov.au>
Sent: Friday, 29 May 2026 12:48 PM
Subject: MAS Panel - Notification of Significant Event (KPMG) [SEC=OFFICIAL]

Follow Up Flag: Follow up
Flag Status: Completed

OFFICIAL

Australian Government
Department of Finance

Strategic Contracting

Notification of Significant Event: KPMG

Dear entities,

The Department of Finance (Finance) advises that it has received a Notification of Significant Event (NoSE) under the Management Advisory Services (MAS) Panel Head Agreement from KPMG Australia (KPMG).

KPMG has advised that the notification relates to governance and conduct matters identified through ongoing investigations concerning historical whistleblower allegations. As outlined in the notification, KPMG has also advised of changes in senior leadership, including:

- the resignation of the Chief Executive Officer, Mr. Andrew Yates
- the resignation of the National Managing Partner – Audit and Assurance, Mr. Julian McPherson
- the appointment of an Interim Chief Executive Officer, Mr Stan Stavros

Finance is reviewing the notification in accordance with its responsibilities under the MAS Panel Head Agreement. At this stage, there is no action required by entities.

Finance will keep entities informed of any further developments.

Regards,

Strategic Contracting Branch | Procurement Division

Commercial Group | Department of Finance

E: maspanel@finance.gov.au | A: One Canberra Ave, FORREST ACT 2603

The Department of Finance acknowledges the traditional custodians of the land on which we work and we pay our respects to Elders past, present and future.

s 47F(1)

From: s 47F(1) on behalf of Procurement
Sent: Wednesday, 3 June 2026 1:55 PM
To: s 47F(1)
Subject: FW: MAS Panel - Update on Notification of Significant Event (KPMG) [SEC=OFFICIAL]
Attachments: MAS Panel - Notification of Significant Event (KPMG) [SEC=OFFICIAL]

OFFICIAL

Hi Guys,

As you have a currently active contract with KPMG I am sending this through as an FYI - Please see both the below and attached email.

Feel free to reach out if you have any questions.

Kind Regards,

s 47F(1)
Assistant Director Procurement and Contracts
Finance and Procurement – Deputy Director-Generals Department

NATIONAL ARCHIVES OF AUSTRALIA

t +61 2 6212 3455
e s 47F(1) @naa.gov.au
Kings Avenue, Parks ACT 2600
PO Box 4924 kingston ACT 2604 | naa.gov.au

National Archives of Australia acknowledges the Traditional Owners and Custodians of Country throughout Australia and acknowledges their continuing connection to land, sea and community. We pay our respects to the people, their cultures and Elders past, present and emerging.

OFFICIAL

From: MAS Panel <MASPanel@finance.gov.au>
Sent: Wednesday, 3 June 2026 1:04 PM
Subject: MAS Panel - Update on Notification of Significant Event (KPMG) [SEC=OFFICIAL]

OFFICIAL

Notification of Significant Event: KPMG

Dear entities

The Department of Finance (Finance) is continuing to assess the notification received from KPMG Australia (KPMG) in accordance with its responsibilities under the MAS Panel Head Agreement and is monitoring the matter.

As previously advised in Finance's update on Friday 29 May 2026, no action is required by entities. However:

- Entities may seek assurance from KPMG that no individuals engaged on their work orders are associated with the matters currently being raised.
- If any individuals associated with work orders are identified as linked to these matters, entities should consider whether additional risk mitigation steps may be required.
- Entities retain the contractual right to request the removal of specific personnel from work orders consistent with the Head Agreement.

KPMG has advised of further changes to its senior leadership, including:

- Scott Guse is appointed as National Managing Partner, Audit and Assurance
- Gayle Dickerson is appointed as National Managing Partner, Deal Advisory and Infrastructure
- Eileen Hoggett is stepping aside from her executive role as COO while investigations are pending.

Finance will continue to keep entities informed of any further developments.

Regards

Strategic Contracting Branch | Procurement Division

Commercial Group | Department of Finance

E: maspanel@finance.gov.au | A: One Canberra Ave, FORREST ACT 2603

The Department of Finance acknowledges the traditional custodians of the land on which we work and we pay our respects to Elders past, present and future.

s 47F(1)

From: Gill Savage
Sent: Friday, 5 June 2026 8:33 AM
To: Simon Froude
Cc: Phoebe Morrison; Brooke Anderson; Josephine Secis; Danniella McGowen; Executive Support; s 47F(1) Natalie Williams; s 47F(1)
Subject: FW: [EXT]Confirmation of procedures for handling National Archives' information [SEC=OFFICIAL]
Attachments: KPMG Client Confidentiality.pdf

OFFICIAL

Simon

I advised late last week that s 47F(1) (Partner KPMG) contacted me about the allegations (tabled in Parliament) that KPMG had disclosed client audit data to other KPMG clients. s 47F(1) phoned to assure me that National Archives data has not been 'accessed, used or implicated' in the matters raised in Parliament.

Given the range of audits recently completed and in the final stages, I have copied in others for awareness, visibility and appropriate action.

The email below and attached PDF outlines measures KPMG has in place to safeguard client data.

Happy to discuss

Gill Savage
Deputy Director-General

NATIONAL ARCHIVES OF AUSTRALIA

m s 47F(1)
e gill.savage@naa.gov.au
Ngunnawal and Ngambri Country
Kings Avenue, Parkes ACT
PO Box 4924 Kingston ACT 2604 | **naa.gov.au**

National Archives of Australia acknowledges the Traditional Owners and Custodians of Country throughout Australia and acknowledges their continuing connection to land, sea and community. We pay our respects to the people, their cultures and Elders past, present and emerging.

OFFICIAL

From: s 47F(1) @kpmg.com.au>
Sent: Thursday, 4 June 2026 6:37 PM
To: Gill Savage <Gill.Savage@naa.gov.au>
Subject: [EXT]Confirmation of procedures for handling National Archives' information

EXTERNAL EMAIL: Do not click links or open attachments unless you trust the sender and know the content is safe.

Good evening Gill,

Some of our clients have requested written confirmation that their data has not been misused or compromised following the events recently reported in the media. In light of this, I am writing to confirm that no KPMG staff involved in the National Archives' internal audit work have been involved in the matters raised. I confirm that no National Archives information has been accessed, used or implicated in those matters.

I would like to reassure you of the controls we have in place to protect National Archives information and maintain strict confidentiality.
At a practical level, the key safeguards are:

- Security-cleared personnel – Staff working on National Archives engagements hold Australian Government security clearances, typically at NV1 or higher.
- Data handling model – Where there is any sensitivity or concern, we can work entirely within National Archives systems, with no requirement to store information on KPMG environments.
- Contractual and legal protections – We operate under strict confidentiality obligations and are comfortable executing Non-Disclosure Deeds to further formalise these commitments.
- Strict confidentiality framework – All staff operate under mandatory confidentiality, ethics and independence policies, supported by training, annual certification and disciplinary consequences for non-compliance.
- Controlled access to information – Client data is treated as confidential by default and access is restricted to the engagement team on a least-privilege basis, with technology controls preventing unauthorised access or sharing.

I have attached a more detailed summary of our controls, including those specific to our work with the Commonwealth.

Please let me know if you would like to step through any of this in more detail.

Kind regards,

s 47F(1)

Partner
Governance, Regulation and Assurance
Consulting

KPMG
Level 9, Constitution Place, 1 Constitution Avenue
Canberra City ACT 2601 Australia

Tel +61 2 6267 5104
Mob s 47F(1)
s 47F(1) @kpmg.com.au
kpmg.com.au

EA – s 47F(1)
Contract details: s 47F(1)@kpmg.com.au
Contact numbers: 07 3237 5482 / s 47F(1)

Level 9, Constitution Place
1 Constitution Avenue
Canberra City ACT 2601

PO Box 7396
Canberra Business Centre ACT 2610
Australia

ABN: 51 194 660 183
Telephone: +61 2 6248 1111
Facsimile: +61 2 6248 1122
www.kpmg.com.au

Following is a summary of the arrangements in place for managing Commonwealth information accessed or held by KPMG.

Policies

There are prescribed policies, procedures and guidance, combining regulatory, independence and ethical requirements that all partners and staff must adhere to. This includes the KPMG Global Code of Conduct, all firm policies and associated procedures published on the KPMG Australia policy site, and the policies and procedures set out in the Australian Quality & Risk Management Manual ("AQRMM").

The AQRMM is based on a globally developed manual, reflecting the key elements of the International Ethics Standards Boards for Accountants (IESBA) Code of Ethics combined with Australian-specific provisions. Where applicable, US Securities and Exchange Commission (SEC), US Public Company Accounting Oversight Board and other regulatory requirements are included. The maintenance of confidentiality is a fundamental ethical requirement set out in the KPMG Code of Conduct and supported by the following policy requirements in the AQRMM and supporting policy:

- *Policy 5.3.1 Obligation of Confidentiality* – defines confidential information and the authorised purposes for the use of confidential information.
- *Policy 5.3.2 Disclosure of Confidential Information* – sets out the policies and expectations for maintaining confidentiality and taking steps to minimise inadvertent disclosure.
- *Policy 5.3.3 Obtaining Consents to Use and Disclose Confidential Information* – requires compliance with all necessary consent to use and disclose confidential information in accordance with applicable laws, regulations or professional standards.

- *Policy 5.3.4 Personal information* – includes additional requirements with regard to the protection, disclosure and distribution of personal information and shall respect the privacy and confidentiality of personal information.
- *Policy 12.11.N1 KPMG Australia Disciplinary Framework* - established guidelines for actions to be taken against individuals for violation(s) of Ethics and Independence policies.

There are a range of supporting policies and requirements pertaining to information security and access as detailed further in this letter.

Mandatory training and certification

All Partners and professional staff are required to complete Security Awareness For Everyone (SAFE) training, Privacy, Ethics and Independence training and pass the related assessment by the earlier of 30 days of commencing employment or returning to work with the firm, or annually thereafter, by the completion timeframe set by the Firm. Training is mandatory and non-compliance is subject to disciplinary action.

All Partners and staff are required complete an annual confirmation of compliance stating that they have remained in compliance with applicable ethics and independence policies and other relevant policies throughout the year covered by the confirmation, by the completion timeframe set by the Firm.

s 47(1)(b)

Information Security

Confidentiality of client information is enforced through policy and enforced technology controls that cover segregation of engagements and controlled access to information. All client data is treated as confidential by default.

Access to information is explicitly provisioned, governed by role-based access controls, and enforced through identity and access management mechanisms aligned to least privilege. Access control and segregation are designed to prevent access by individuals who are not part of an engagement and include the following (not exhaustive):

- Role-based access controls (RBAC) restricting data access to defined engagement teams, with access controlled through secure login and identity management.
- Access to collaboration sites (e.g. SharePoint), folders and files restricted through Engagement Leader approved permissions aligned with classification and contractual requirements.

- Document repositories are structured around engagement workspaces in iManage (KPMG's Document Management System) with access again restricted to assigned engagement team members approved by Engagement Leader.
- Data movement controls to limit transfer of client data to approved and governed channels. These include Microsoft Information Protection (MIP) to enforce classification labels; technology restrictions over removable media, personal emails and data extraction; public AI restrictions; and cloud security controls.
- Detective monitoring controls over attempted data exfiltration, large data movement, anomalous or unauthorised usage patterns.
- s 47(1)(b)

Information security controls are aligned to policy mappings and subject to internal audit and audit under the DISP. KPMG Australia is ISO 27001:2022, ISO 27017:2015, and ISO22301:2019 certified and undergoes surveillance audits every year.

Security accreditation

The large majority of Australian Government engagements must be delivered by staff with a security clearance.

KPMG is a member of the DISP, aligning to applicable controls under the Australian Government Protective Security Policy Framework (PSPF), Defence Security Principles Framework (DSPF), and the Information Security Manual (ISM).

KPMG has appointed a Canberra-based partner to be the DISP Chief Security Officer (CSO), responsible and accountable for the firm's security settings. The DISP CSO reports to the National Executive Committee and the Board on security related matters. The DISP CSO is supported by a Deputy Chief Security Officer and dedicated Protective Security Team (PST).

The DISP CSO chairs a whole-of-firm Protective Security Working Group, ensuring a coordinated approach across to the four domains of security: Governance, Personnel Security, Physical Security, and Info/Cyber Security. The DISP CSO is also a member of the Insider Threat Working Group.

KPMG has developed and implemented appropriate governance to drive security uplift in the management of Commonwealth information and resources. Specific security accreditation standards and activities include:

- *Training:* whole-of-firm security awareness training, with a specific focus on supporting work with government and critical infrastructure clients.

- s 47(1)(b)
- *Onboarding:* KPMG workplace screening is aligned to the Australian Standard AS4811:2022 standard covering all KPMG personnel are eligible and suitable to access Australian Government resources.
- s 47(1)(b)

Contractual controls

The **Management Advisory Services Panel** (MAS) Standing Offer Notice (SON3751667) includes clear requirements and expectations for the management of confidential information. In this context, Confidential Information means any information and all other knowledge at any time disclosed (whether in writing or orally) to KPMG by the Commonwealth or other engaging parties, or acquired by KPMG in performing the services which:

- is by its nature confidential;
- is designated, or marked, or stipulated as confidential; or.
- KPMG knows or ought to know is confidential.

Taken together, these contract controls impose obligations for KPMG to disclose any conflicts of interests to the Commonwealth and maintain confidentiality and security of information received as part of this engagement.

Where requested, we also complete and sign Non-Disclosure Deeds relating to the non-disclosure of Confidential Information.

High risk government engagements

For government engagements involving classified information or confidential industry information; we consider that Government systems are generally best placed to manage this information. s 47(1)(b)

- Requirements of all team members to have signed an individual non-disclosure agreements prior to accessing tender documentation and working on engagement. This further restricts the need-to-know principle and governs information sharing within and external to the Commonwealth.
- s 47(1)(b)

s 47(1)(b)

- s 47(1)(b)

The Digital Risk and Security Governance function, and particularly the Government Risk team, supports the Firm by uplifting knowledge, advising on Australian government policy and contract compliance, improving processes and providing resources to support compliance.

Non-compliance

KPMG, like all organisations, face the risk of misconduct or breaches of law or unethical conduct. Breaches of confidence can arise in a number of ways, both intentionally and inadvertently. KPMG encourages the reporting of any suspected or actual wrongdoing, misconduct, or an improper state of affairs, including conduct that is dishonest, corrupt, illegal or unethical, or concealment of such conduct. We also encourage the reporting of any suspected or actual breaches of KPMG's Code of Conduct, policies, procedures or the KPMG Values or any contravention of Human Rights. KPMG's DISP CSO is consulted when matters involve security cleared KPMG personnel and facilitates reporting to AGSVA or the relevant Department or Agency (as required).

If individuals become aware of an actual or suspected breach of confidentiality, they are required to promptly take the relevant following action:

- In respect of privacy and/or data breaches, report a Privacy Data Incident to the Privacy Officer; and notify the Cyber Security Operations (CSO) team via the IT Service Desk.
- In respect of all other actual or suspected breaches of confidentiality, notify the Office of General Counsel; and in addition, where the breach relates to Government engagements, notify the KPMG PST.

Alternatively, if an individual wants to report a concern and remain anonymous, the *KPMG Whistleblower Policy* sets out the procedures and avenues available to a whistleblower reporting to KPMG. While the whistleblower laws under the *Corporations Act* do not apply to partnerships or to employees reporting personal work-related grievances, the KPMG Whistleblower Policy has been developed in accordance with applicable legislation and regulatory guidance, including Regulatory Guide 270, Whistleblower Policies (RG270).

KPMG provides a Speak Up hotline for Australia, as well as an international whistleblower hotline. Both hotlines are independently operated and open to all whistleblowers. KPMG does not tolerate any form of retaliation or adverse action

resulting from a whistleblowing disclosure. The Whistleblower policy is available to all officers, Partners and employees of the company on the Intranet. External parties can obtain access via KPMG's external website.

s 47F(1)

From: s 47F(1)
Sent: Thursday, 11 June 2026 9:27 AM
To: s 47F(1)
Cc:
Subject: FW: KPMG - Notice of Significant Event [SEC=OFFICIAL]

OFFICIAL

Hi s 47F(1),

Il just wanted to touch based to ask if you think that the recent media attention re inappropriate handling of documents by KPMG puts the contract that we have with KPMG at risk?

Has any advice been given to your team about managing the KPMG contract in terms of risk mitigation.

We do have this clause in the contract:

Confidential Information	Confidential information should not be disclosed in any circumstances without prior consent from the Agency and owner of the confidential information. Confidential information includes: • Agency data, • Any Personal Information held by the Agency, • Security Classified Information, All deliverables under the work order including recommendations.

Regards,

s 47F(1)
Digital Archiving Service Design (DASD) Project Manager
Digital Archives Preservation & Research (DAPR)
t +61 2 9782 5340
mob. s 47F(1)
Workdays: Mon-Thurs

OFFICIAL

From: s 47F(1) @kpmg.com.au>
Sent: Wednesday, 10 June 2026 10:27 PM
To: s 47F(1) @naa.gov.au>
Cc: s 47F(1) @kpmg.com.au>; s 47F(1) @kpmg.com.au>
Subject: [EXT]KPMG - Notice of Significant Event

Good morning s 47F(1)

Hope all is well.

Acknowledging KPMG are due to commence the Digital Archiving Service Design Transition Plan engagement with you on 24 August, I wanted to update you on the recent media and senate matters.

On Friday 29th May 2026, KPMG notified the Department of Finance formally of a notifiable significant event (under the MAS Panel) in relation to the inappropriate sharing of client documents on certain non-government

engagements. We have taken this matter very seriously, but I did want to confirm that the matters being reported do not involve any NAA engagements.

Consistent with the requirements for Significant Event disclosure, I can confirm that:

- none of the matters subject to the Notice, and described further below, concern the performance of services to the NAA.
- none of the Specified Personnel or other personnel engaged in connection with the Services to NAA were involved.

The matters raised relate to corporate audit engagements and proposals and do not relate to engagements for government clients. As this is still ongoing, KPMG continues to work with the Department of Finance to meet our obligations under the MAS panel.

I would like to reassure you of the controls we have in place to protect National Archives information and maintain strict confidentiality. At a practical level, the key safeguards are:

- Data handling model – Where there is any sensitivity or concern, we can work entirely within National Archives systems, with no requirement to store information on KPMG environments.
- Contractual and legal protections – We operate under strict confidentiality obligations and are comfortable executing Non-Disclosure Deeds to further formalise these commitments.
- Strict confidentiality framework – All staff operate under mandatory confidentiality, ethics and independence policies, supported by training, annual certification and disciplinary consequences for non-compliance.
- Controlled access to information – Client data is treated as confidential by default and access is restricted to the engagement team on a least-privilege basis, with technology controls preventing unauthorised access or sharing.

I can be contacted at any time either via email or mobile (s 47F(1)).

Kind regards

s 47F(1)

Partner, Transformation Delivery

KPMG

Level 9, Constitution Place

1 Constitution Avenue

Canberra City ACT 2601

Pronouns: she/her

Mob s 47F(1)

s 47F(1)@kpmg.com.au

kpmg.com.au

I acknowledge the Traditional Owners and Custodians of the Land I live and work on as the First People of this Country.
