Report of the Independent Review of inadvertent data release of Management Advisory Services (MAS) Panel details

Michael Manthorpe PSM

3 April 2024

CONTENTS

Introduction

On 20 February 2024 I was approached by the Department of Finance (Finance) and asked to undertake a short administrative review of two serious, related data breaches which had occurred in the Department.

The breaches, which occurred in November 2023 and February 2024, involved the release of personal and commercial-in-confidence information of the Management and Advisory Services Panel (MAS Panel) to sub-sets of the Panel, that resulted in the disclosure of:

(a) contact information for suppliers, including mobile phone numbers; and

(b) pricing points of all suppliers (the pricing data of MAS Suppliers before the latest repricing exercise).

In both cases Finance promptly responded when it became aware of the issue, to minimise the impact of the breaches. However, the release of the data presented risks to the integrity of a very wide array of Government procurement, with serious potential commercial or value for money consequences, and associated risks to the reputation of the Department and trust in its important role in the management of whole of Government procurement activity.

The full Terms of Reference for the review are at Appendix A. In essence, however, I was asked to consider:

(a) the facts of the two incidents, to determine what led to the disclosure of personal and commercial in confidence information

(b) the Department's response on becoming aware of the inadvertent disclosure and the effectiveness of that response

(c) whether the Department has effective policies, processes and organisational culture for the management of personal and commercial in confidence information collected as part of the management of the MAS Panel

(d) making recommendations, as I saw fit, relating to systems, processes, controls and culture to improve Finance's handling of sensitive information and responses to incidents if and when they occur

(e) addressing further matters identified during the course of the Review.

Following my appointment by the Department's Executive, I undertook the Review independently and impartially, and was assisted by various officers from the Department, who I thank for their assistance.

Although the review was completed quickly, I am confident that I was able to access the people and documents needed to form a reasonable view of what went wrong and why. Relevant officials were forthcoming in their cooperation with the review and I was authorised by the Secretary to undertake any reasonable activity associated with the gathering of evidence relevant to the task.

More specifically, I undertook interviews with relevant officials from Procurement Division, Commercial Group and other areas within Finance that were able to contribute relevant information. I also met the National Data Commissioner, who occupies a statutory office within the Finance Department and engaged with a small number of MAS Panel Suppliers[1] directly impacted by the breaches associated with the unauthorised release of

[1] Mark Nixon, Partner, EY; Lara de Masson, Business Group Leader, GHD Advisory; David Robjent, Chief Executive Officer, Grey Advantage Consulting.

Commonwealth information, so as to gain some sense of their perspective on the data breaches and the Department's response.

I accessed a variety of records considered relevant to the incidents, including emails, advices, procedural and policy documents. I was given an expert demonstration and inspection of the relevant parts of the AusTender platform (which was the source of Breach 1) and the Excel spreadsheets with hidden worksheets (which were the source of Breach 2).

All notes of interviews, documentation and other evidence gathered as part of this review that is referred to or relied upon in this report, are available to the Department of Finance.

What is the MAS Panel?

The Department of Finance (Finance) plays a critical leadership role in the administration of Commonwealth procurement and the Commonwealth Procurement Rules made under section 105B(1) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

Whole of Australian Government Arrangements for procurements are established for Commonwealth entities to use when procuring certain goods or services. These are either coordinated or cooperative procurements, some of which are mandatory for use, and generally result in overarching contracts or standing offer (panel) arrangements.

Coordinated procurement arrangements are established for commonly used goods or services by the Commonwealth. These arrangements are intended to ensure more efficient processes to deliver better prices, service and quality for the Commonwealth. Coordinated procurement arrangements also offer increased transparency for purchasers, standard terms and conditions and should deliver improved contract management that benefits both the government and suppliers.

Where established, coordinated procurement arrangements are mandatory for NCEs and optional for CCEs and Commonwealth companies, including GBEs, authorised by Finance to use the Panel.

The Management Advisory Services (MAS) Panel (SON3751667) is a coordinated procurement arrangement established to improve the quality, consistency and efficiency of the procurement of Management Advisory Services by Commonwealth entities. The Services provided under the MAS Panel are commonly known as management consultancies. To provide some sense of the significance of the MAS Panel, it contains 412 members drawn from all the large and many small consulting firms that provide services to Government.

In 2022-23, 1,107 contracts were awarded to members of the MAS Panel, with a combined value of $282.3 million. The MAS Panel represents nearly half the value of contracts published on AusTender as consultancy arrangements, which had a combined value of $600 million. Given the significance of the Panel, upholding probity and ensuring integrity and fair competition in the pursuit of value for money in its administration are of great importance to suppliers, purchasers and the taxpayer.

Breach 1

Breach 1: Facts

Breach 1 occurred on and from 2 November 2023 when the MAS Supplier Matrix,[2]which lists the rates for all suppliers on the MAS Panel among other details, was inadvertently released to 22 suppliers on the MAS Panel.

More specifically, the error occurred because the MAS Supplier Matrix was uploaded by Finance to the wrong area of the AusTender Dynamic Sourcing for Panels (DS4P) Platform as an 'optional' RFQ document. This meant that purchasing agencies could see and select a link to the MAS Supplier Matrix in the fields of AusTender that could then be used to populate RFQs to be sent to suppliers; rather than the fields of AusTender which are intended to be for the confidential information of potential purchasers.

The actual disclosure occurred when Commonwealth entities selected the MAS Supplier Matrix from the 'optional' RFQ documents list on the DS4P to be attached to the RFQ to be issued to selected suppliers.

This impacted 6 RFQs that were issued between 3 November 2023 and 9 November 2023 by the Department of Health and Aged Care (4), the Department of Veterans' Affairs (1) and Geoscience Australia (1).

To illustrate how this played out, it appears the Department of Health and Aged Care (Health), RFQ (16445) was published on AusTender by Health at approximately 12.20pm on Thursday 9 November, attaching the MAS Supplier Matrix in error. Health was advised of the error by a MAS Panel Supplier at approximately 12.35pm that RFQ (16445) attached the MAS Supplier Matrix. Health advised Finance they had accidently selected a commercial in confidence document (later confirmed to be the Supplier Matrix) and attached it to RFQ (16445) which was issued to several suppliers. Health assured Finance that the RFQ would be cancelled and re-issued without the MAS Supplier Matrix and that Health would contact the suppliers to delete the document if they had downloaded it.

On the same day, the Department of Veterans Affairs (DVA) provided e-mail notification to the MAS Panel mailbox at approximately12.49pm that DVA unsuccessfully attempted to amend RFQ (16431) to remove the MAS Supplier Matrix. DVA subsequently cancelled RFQ (16431) shortly thereafter and issued a new RFQ (16440) without the MAS Supplier Matrix.

Similarly, prompted by the incorrect availability of the MAS Supplier Matrix on the wrong side of the AusTender platform, three further RFQs from the Department of Health and Aged Care, and one from GeoScience Australia made their way into the supplier domain.

Finance was also alerted to the inadvertent release of the MAS Supplier Matrix by a Partner in a MAS Panel supplier.

As part of the review, staff with the necessary technical expertise demonstrated to me how the error by Departmental staff was made. Members of the team responsible for the mistake also spoke to me and touched on the following points:

1. That many of the processes involved in administering the Panel are manual and laborious;
2. That staff turnover had been a challenge in the team around the time of the mistake, and that the individual who made the mistake was new to the role and still being trained in how the systems operated;

[2] The MAS Supplier Matrix is identified as Confidential Information in accordance with Schedule 9 of the MAS Panel Head Agreement.

3. The supervisor who was working with the individual who made the mistake failed to "spot" the error when it occurred;
4. A contributing factor to point 3 was that there had been, not long before the mistake was made, a change to the work process for editing, publishing and reviewing material on DS4P, which resulted in another team undertaking the publishing step. This meant that the MAS Panel team was not alert to how the published change would have appeared on the "live" system until some time after the other team published the material. While the MAS Panel team could have picked up the error at the "editing" point, had it also "published" the change it is possible that it would have seen how the change appeared on the system and therefore had an opportunity to correct the error.
5. It appears that the procedural documentation that guides how staff work with the relevant systems, although quite detailed, did not provide adequate or clear guidance to staff about the importance of placing sensitive pricing information materials in the correct field of the DS4P platform; and nor had it kept up with the work process change mentioned at point 4 above.

Breach 1: Departmental response

Upon learning of the release of the MAS Supplier Matrix on 9 November 2023, Finance took action to prevent the further distribution of the material including:

- Contacting the relevant Commonwealth entities to provide advice on the next steps to contain the disclosure including seeking confirmation of whether they have contacted the suppliers to request that they delete the MAS Supplier Matrix from their systems;
- Requesting relevant Commonwealth entities to re-issue the RFQs removing the MAS Supplier Matrix; and
- contacting the suppliers who were inadvertently issued the RFQs requesting they delete the MAS Supplier Matrix if it had been received.

On 17 November 2023, Finance requested that the 22 Service Providers who received the Supplier Matrix sign a Statutory Declaration for Personnel; a Personnel Confidentiality Undertaking Deed Poll; and a Supplier Confidentiality Undertaking Deed Poll. These documents, signed at both a personal and organisational level, require that the Supplier Matrix is kept confidential and is not disclosed further or used for any purpose. The Supplier Confidentiality Undertaking Deed Poll also requires the supplier to interrogate its records and delete the Supplier Matrix from its IT systems, including any electronic back-up files.

These documents were a critical part of the containment strategy to ensure that the information contained in the Supplier Matrix was not further disclosed. I am advised that the Service Providers are liable at a company level for breaching the Deed of Confidentiality. The MAS Panel Head Agreement requires confidential information be kept confidential. The Supplier Confidentiality Undertaking Deed Poll and the Personnel Confidentiality Undertaking Deed Poll also requires the confidential information be kept confidential and not be used. Under the MAS Panel Head Agreement, acting in good faith (Clause 10.1.1(b)) and maintaining confidential information (Clause 22.1.1) are key obligations for Service Providers.

Based on the information available to Finance, a total of 12 Service Providers downloaded the Supplier Matrix upon receiving the RFQs and 10 Service Providers did not view or download the Supplier Matrix.

All 22 Service Providers returned the appropriate executed Statutory Declaration for Personnel, Personnel Confidentiality Undertaking Deed Poll, and the Supplier Confidentiality Undertaking Deed Poll to Finance. Appropriate sanctions are available under the MAS Panel Head Agreement, such as suspension (Clause 25) or termination (Clause 26) from the MAS Panel, for a Service Provider that breaches their obligations.

The Department's approach was informed by consultation with and advice from its Legal team as to the appropriate approach to the privacy and commercial sensitivities associated with the breach, involving as it did the distribution of highly sensitive commercial information amongst competing firms. While the steps outlined above were particularly directed towards containing the impact of the inadvertent release of the supplier pricing data, they also addressed the potential impact of the release of personal information – predominantly business contact information. Having regard to the types of personal information involved, the circumstances of the breach, and steps taken in response, Finance's assessment was that the privacy breach was not likely to result in serious harm to affected individuals. Nevertheless, the Secretary wrote to the Australian Privacy Commissioner advising her of the incidents and of the commissioning of this review.

As part of its response, Procurement Division also considered specific measures that could be taken to avoid a repeat of placing sensitive pricing information on the "supplier facing" fields of AusTender. It did not, however, appear to consider whether broader procedural or policy review was necessary to avoid some other kind of future breach.

The Department also planned two further steps to minimise the risks arising from the inappropriate use of the data that was inadvertently released. First, the Department intended to commence spot-checks of prices charged by the 22 suppliers who had received the data, to see whether their pricing strategies may have changed, informed by accessing the commercial information of their competitors. Second, the Department brought forward a regular re-pricing exercise so as to provide a limited opportunity to vary prices which would render the wrongly released information at least marginally out of date. Unfortunately, just prior to beginning the first of these further mitigations, the repricing exercise itself resulted in the second data breach, as described below.

Breach 2

Breach 2: Facts

Breach 2 occurred on 14 and 15 February 2024 when Finance, as contract managers for the MAS Panel, emailed 240 suppliers with details of their updated pricing which, as noted above, was brought forward to help mitigate the risks arising from Breach 1. Unfortunately, the email included information in the form of hidden worksheets sheets in an Excel document that contained third-party confidential information, i.e. the pre-existing pricing of all 412 suppliers.

A demonstration to the review revealed that the third-party confidential information in the Excel worksheet can be accessed by right clicking on a tab in the worksheet and unhiding sheets. One sheet, which was visible once unhidden, contains the contact information for suppliers, including mobile phone numbers. One other sheet revealed the previous pricing of all suppliers (that is, the pricing data of MAS Suppliers before the repricing exercise). While an unskilled user of Excel would be unlikely to have identified the hidden sheets, a skilled user could locate the sheets quickly were they inclined to look.

Finance was made aware of the breach on the afternoon of 19 February 2024, when the MAS Panel team received a call from a MAS Panel supplier. During the call, the supplier

indicated that they had discovered some hidden data within the spreadsheet, in particular that which contained the contact names and telephone numbers of all MAS Panel suppliers. Urgent review within Finance subsequently revealed that pricing data for all MAS Panel suppliers could also be found.

The review has inquired into how hidden worksheets contained in a spreadsheet, containing highly sensitive commercial information about suppliers, could be sent to the majority of those suppliers.

To this end, interviews with relevant team members revealed that one member of the team specialised in the use of Excel. That person had created a comprehensive Excel spreadsheet to reduce the manual work needed to maintain all the panel details that were otherwise contained in multiple, sometimes inaccurate data sets. This Excel spreadsheet was then used by another team member to execute the new pricing structures for suppliers in the MAS Panel using the data in the worksheets, in which some worksheets were hidden.

The Director of the MAS Panel team reviewed the spreadsheet that was being sent to suppliers and did not identify any hidden data or errors during the checking process. The team member who sent the emails to suppliers also did not know about the hidden data. Prior to sending the emails, the MAS Panel team did try to convert the spreadsheet to a Word document, but for technical reasons did not proceed with this option. Meanwhile, the team member who was aware of what the spreadsheet contained was not aware that it was to be used for external purposes. In other words, there was a simple but very unfortunate lack of communication within a relatively small team about the tools they were using. Generally, I am advised that new rates for suppliers are sent out to them by way of supplier-specific PDFs which cannot be changed and contain only the data about the individual supplier. However, this option was not chosen on this occasion in the interests of finishing the repricing task quickly.

Breach 2: Departmental response

Finance called (or attempted to call) all 240 suppliers who were sent the email and attachments that contained the third-party confidential information. A further reconciliation is taking place to ensure all MAS Panel suppliers that received the original emails have been contacted through calls and/or follow up communications on and after 21 February 2024.

Procurement Division took external legal advice to assist in seeking to minimise the potential harm associated with this second data breach. In particular, in order to prevent the disclosure and/or use of any third-party confidential information, on 21 February 2024, Finance used its power under clause 10.2.1(a) of the MAS Head Agreement to direct Service Providers to comply with written directions and issued a requirement to comply for Service Providers to:

- delete the subject e-mail and attachments Finance sent to Service Providers on 14-15 February 2024 from Service Provider IT systems and destroy any physical copies; and
- ensure that to the extent any other entity or person over whom the Service Provider exercises control has been provided with the e-mail or its attachments, or provided with a physical copy, those copies are deleted from IT systems and physical copies destroyed.

Suppliers were directed to not use or disclose (including to any Personnel) any third-party information contained in the e-mail or its attachments. Once completed Service Providers were required to notify Finance that the actions relating to the written direction were complied with.

Observations, findings, recommendations

1. Preliminary comments

On the basis of the discussions I have had with Finance officials, I offer the following high level observations:

1. All the officials, from the most junior to the most senior, sincerely regret the inadvertent data releases that are subject to this review. Although mine is a relatively short administrative review, rather than anything more onerous, I have no reason to suspect that anything other than human error was the source of both breaches.

2. That said, the breaches are serious. While it is reasonable for Finance to rely on the MAS Panel Head Agreement to seek to ensure that the wrongly distributed data is deleted and not used to gain inappropriate commercial advantage in actual tender processes, it is unfortunate that Finance itself appears to have twice breached the same confidentiality provisions that it now asks suppliers to abide by.

3. There is an inevitability of human error in large complex administrative activity. For this reason systems, structures, processes, policies, risk management activity and organisational culture all have a part to play in mitigating the risk of human error, to the extent possible.

4. Overall, I am satisfied that the Department's response to both breaches has been as administratively thorough and urgently pursued as is reasonably possible. Yet, to be true to Finance's own Data (Privacy) Breach Response Plan, a critical component of responding to a data breach is to prevent its recurrence. It is troubling that in this case there was a recurrence; this fact alone calls for very careful focus going forward in the relevant Branch. It calls on the whole Department to build capability to avoid a similar incident elsewhere. It is also the case that, no matter how thorough the response has been, it is impossible – once the data was wrongly released – to be 100% certain that no supplier has taken commercial advantage of their possession of the data, however brief that possession may have been. To be clear: I have no evidence that this has occurred, and it is also important to note that the data that was distributed was *maximum* rates data, which may differ from rates that, on any given procurement process, suppliers *actually* charge. However, as one supplier told me, provider rates are at the absolute heart of their strategy for pursuing business with the Commonwealth. Once other providers know the rates of their competitors "what they have seen cannot be unseen".

5. Finance is entrusted with a leadership role with respect to data governance which, among other things, goes to the appropriate protecting, sharing and using of data for the greater good. The data breaches that are subject to this Review provide an opportunity to take a fresh look at how the Department manages its own data, and how it might build maturity in this space.

More detailed commentary on the above themes is contained below. The commentary then provides a basis for recommendations, some of which go to whole of Department activity; some of which pertain more specifically to Procurement Division and/or Strategic Contracting Branch.

The material also provides reflections arising from interviews conducted with a small number of suppliers and other material I have accessed in relation to individual suppliers. In the time available to undertake this review, I do not assert that I have captured all or a truly representative record of supplier views. Nevertheless, I thought it important to at least capture some of the sentiments that were raised with me, to help inform the Department's response.

2. Data Governance

Finance is responsible for the whole of government Data Governance Framework, which defines common rules, processes, and accountabilities for adoption across the APS to ensure privacy and compliance of government data is maintained. The Framework provides APS agencies with direction on how to ensure the quality, integrity, security, discoverability, accessibility, and useability of data assets.

The *Data Availability and Transparency Act 2022* (DAT Act) establishes a scheme for sharing Australian Government data, supported by strong safeguards and consistent, efficient processes. The DATA Scheme seeks to increase the availability and use of public data to deliver public benefit. The National Data Commissioner is the regulator of the DATA Scheme and provides advice and guidance about its operation. The National Data Commissioner also has a role in providing advice and guidance on best practice and handling of data and the ONDC provides guidance on Data breach responsibilities under the DATA Scheme Guidance note 2023:4 Preventing, preparing for and responding to Scheme data breaches.

Finance is not an accredited entity under the DAT Act and does not currently have accredited capability in managing data. DAT accreditation is required to participate in the DATA Scheme which captures expected characteristics for user accreditation and sets out best practice for data governance. The Commissioner assesses the data governance for data management in practice before accreditation is granted.

The data breaches subject to this Review are not captured by the DAT Act. Nevertheless, the principals of good data management remain applicable, and provide a good way to frame the Department's response.

The Department has already taken steps to improve data governance. It has established a Data and Governance Analytics Branch, headed by the Chief Data Officer (CDO), reporting to the Performance and Risk Committee, providing the Executive Board with strategic advice on risk, security information and data governance. While the ONDC has a Whole of Government role, the CDO responsibility has an internal focus with an expectation of ensuring Finance can work towards being accredited under the DATA Scheme.

I was struck by the enthusiasm of the CDO and by the opportunity that exists for that Office to play a stronger role in data management within the Department, albeit in a "federated" system where data ownership rests with relevant line areas. The CDO has already produced a draft Data Governance Framework, which – once finalised – provides a basis for clear allocation of roles and responsibilities and, among other things, highlights the need for data access to be undertaken in a "timely, secure and consistent manner". Indeed, had the principles contained in the draft Framework been applied in practice, the data breaches subject to this review would not have occurred.

Recommendation 1: The review recommends that the Department move quickly to settle its Data Governance Framework to drive rigorous data management into the future.

The National Data Commissioner has also produced a variety of materials and tools to guide agencies across the APS about how to lift their degree of "data maturity" so as to build trust in the way Governments use data about the citizenry. Once the Data Governance Framework is in place, and informed by my conversation with the National Data Commissioner, there is merit in undertaking a self-assessment of data maturity across the Department. This would have the advantage of testing, in the absence of a high profile breach, whether and the extent to which high level concepts and principles to guide the safe stewardship of data are actually operating in practice.

Recommendation 2: The review recommends that, once Recommendation 1 is adopted, a good next step at a whole of Department level would be to undertake a self-assessment of data maturity, with reference to the tools that have already been developed by the National Data Commissioner.

Legal and Assurance Branch provides advice to line areas within Finance about risks that may arise from a data breach, and supports agency compliance with the Privacy Act and other legislative obligations. There is a risk, however, that these responses will be specific to a breach that has just occurred, rather than taking a broader whole of Department and preventive focus. The Chief Data Officer could play a more prominent role when supporting the department's response to data breaches, particularly focusing on future risk reduction and organisational learning. The CDO is also well placed to participate in other whole of APS initiatives relevant to data, such as those being undertaken through the APSC and the APS Data Profession Stream.

Recommendation 3: The review recommends that the CDO is notified of any future data breaches so that she, in consultation with Legal and Assurance colleagues, can consider any whole of Department initiatives or learnings that might arise from specific breaches.

Practices and Procedures: Procurement Division

As noted above, the review is confident that both breaches were caused by human error and that relevant officials accept responsibility for the errors that occurred and regret what occurred. However, on initial observation, more could be done to mitigate the risk of human error through building Procurement Division's capability through the review or refinement of procedures with a practical application in line with the principals contained in the draft data governance framework, and the imperative for stronger security of information.

At a practical level there needs to be a more consistent, secure, repeatable approach to data management and access, and less use of ad hoc, untested approaches. Indeed, although the two breaches occurred through different work process failings, a common theme is that both occurred as a result of using new or untested processes that, with the benefit of hindsight, lacked the necessary supporting documentation, change management and related discipline. As an aside, I note that after Breach 1 the MAS Panel team identified some specific steps which, if implemented might have prevented a recurrence of the specific mistake that gave rise to it. These steps appeared sensible, but did not contemplate any wider risks that might arise in future pricing changes or other processes.

Procurement Division executives have already been turning their minds to how their internal practices might be improved. A good place to start would be to refrain in future from using Excel spreadsheets as a tool for providing confidential pricing information to suppliers, given the risks inherent in their use for this purpose.

Recommendation 4: The review recommends that the Procurement Division refrain from using Excel spreadsheets as a tool for communicating sensitive pricing information outside the Department. It would appear that the use of PDF has been a safer option in the past and ought be deployed for the next pricing adjustment. The review understands that is the intention of Procurement Division's Management team.

There are also structural and procedural considerations. With respect to the first breach, consideration should be given to which teams within Procurement Division carry out which tasks. At the time of that breach there had been a change to the MAS Panel team's system access. Previously the MAS Panel team would 'edit, review, and publish' in real time when making changes in DS4P. The MAS Panel team contended that such a checking process was robust and would have picked up that the Supplier Matrix was uploaded into the wrong area of DS4P post publishing. At this stage, corrective actions could have been undertaken deleting the document and placing it into the correct area of DS4P. I am advised that following the change in process, another team in Finance, the Procurement and Contracting Team (PaCT)[3] assumed responsibility for the 'review and publish' steps. The PaCT role is to support procurement capability uplift within Finance. Post incident, it would appear that neither PaCT nor the MAS Panel team undertook a quality assurance process that might have picked up the error that had been made.

While the new process may have been well-intended, any new process involving the handling of sensitive information needs to be subject to strong "change control" procedures, so that among other things everyone involved is clear about which task sits with which person or team.

The review was informed that there may also be structural change options that would strengthen Procurement Division's operations, in a way that improves consistency in the way that all the various panels (not just the MAS Panel) are administered. This is worth exploring for consistency and efficiency reasons, so long as any change is complimented by strong change management activity.

Recommendation 5: The review notes that the Procurement Division executive is considering possible structural and procedural changes, particularly within Strategic Contracting Branch. Should this be pursued, it is recommended that strong change management controls are put in place so that better outcomes are not jeopardised in a manner that arose in advance of Breach 1.

The Department's response to Breach 1 appears to be have been sound and administratively comprehensive. In particular, it urgently sought to mitigate commercial risk to suppliers and loss of trust by seeking assurance that the confidential data was deleted and not used for inappropriate purposes. I am advised that Finance is satisfied that relevant suppliers deleted the information, and Finance required appropriate confidentiality deeds to be completed. Finance has reported a 100 per cent completion rate for Confidentiality Undertaking Deed Poll or Statutory Declaration by suppliers in relation to Breach 1. Of course, no matter what assurances are provided, there is always a residual risk, however small, of inappropriate use of sensitive data once it has been wrongly distributed.

Progress is also being made to mitigate the risk arising from Breach 2. I am advised that, as of 27 March 2024

- 235 suppliers (98 per cent) have confirmed deletion of the original email.
- 224 suppliers have returned executed Confidentiality Undertaking Deed Polls. Finance is continuing to follow up the remaining 15 suppliers who have not executed these documents. (Note: Finance has advised me that 1 supplier that had been sent the email attaching the spreadsheets containing commercial data did not in fact receive the email, so the total number of suppliers that did is 239).

[3] Previously known as the Procurement Quality Review Team (PQRT)

- Of the 224 suppliers that have returned Deed Polls, 45 considered there was a need for individual Statutory Declarations to be completed by one or more staff. This has generated 68 Statutory Declarations, including 12 from individuals who confirmed they had not seen the relevant commercial in confidence information.

3. Risk and Culture

The PGPA Act establishes several legislative requirements in relation to the management of risk for Commonwealth entities:

- Section 16 requires the accountable authority of a Commonwealth entity to establish and maintain systems and appropriate internal controls for the oversight and management of risk for the entity; and
- Section 25 establishes a duty of care and diligence for all Commonwealth officials to exercise their powers, perform their functions and discharge their duties with the same degree of care and diligence that a reasonable person would exercise if they were an official of the entity and occupied that position. This reasonable person test is similar to the common law reasonable person test. An official has to consider whether they have taken reasonable steps, given the circumstances, to assess the consequences of their actions. To take reasonable steps, the person needs to be appropriately informed, capable, aware of the law, and fair minded. This requires officials to consider reasonably foreseeable risks that arise in relation to the performance of their duties in administering the operations of an entity.

The Revised Commonwealth Risk Management Policy 2023 sets out the principles and mandatory requirements for effectively managing risk. It is mandatory for all non-corporate Commonwealth entities and recommended as best practice for corporate Commonwealth entities. The Policy requires entities to have arrangements in place for identifying, managing and escalating emerging risks, the inclusion of specific risk management responsibilities that should be defined in an entity's risk management framework and the simplification and consolidation of existing elements, including the use of clearer language and a reduction in complex risk management terminology.

Finance guidance in relation to section 25 duty of care and diligence provides that in a high-risk activity or decision-making process such as engaging in significant business contracts with third parties, an official could exercise more caution to inform themselves of all the circumstances in order to make a reasonable decision.[4]

Finance Accountable Authority Instruction (AAI) 1.1: Risk management[5] establishes risk requirements for Finance officials. It provides that:

- all SES facilitate, challenge and drive risk management within their area and the department; model good risk management behaviours; contribute to the development of the department's enterprise risk profile; ensure the management of risks is consistent with the department's risk management framework in their area; and support staff to engage with risk in an appropriate and informed manner.
- Managers and Supervisors identify, review and manage the risks and risk profiles of their business units; recognise risk management behaviours (positive or negative) in their teams; ensure staff are managing risk in line with the department's risk management policy; and communicate risk information to relevant stakeholders in a timely and accurate manner where necessary.

[4] ASIC v Lindberg [2012] VSC 332

[5] Accountable Authority Instructions (AAIs) are made under section 20A of the PGPA Act and are written instruments issued by the accountable authority to instruct officials on matters relating to the finance law.

The AAI 1.1 also notes that Section 19 of the PGPA Act requires the Secretary to keep the responsible Minister and Finance Minister informed of any significant decision in relation to the department or significant issue that has or may affect the department.

Review findings

The Department of Finance has rightly pressed other agencies for many years on the need to develop a "positive risk culture" in which people at all levels of an agency take an active interest in identifying and treating the risks they confront.

More needs to be done to focus on effective risk management in Strategic Contracting Branch. The fact that not just one, but a second breach occurred in relation to the same highly sensitive data, but through a different failure in work process, highlights the need to take a fresh look at how risk in relation to sensitive data, and indeed the wider work of the Branch, is managed.

Renewed work on data governance and possible structural adjustments, discussed above, may be helpful but need to be integrated with and informed by a consistent approach to training, procedural guidance and related activities. All officials share a responsibility to ensure that risk is addressed; this is not merely good practice. A fresh whole-of-Branch risk management plan may be a way to draw all of the local strands of activity together consistent with the notion of creating a positive risk culture, where everyone thinks about and engages with risk as a team.

Recommendation 6: The review recommends that Strategic Contracting Branch use a fresh risk management planning exercise to draw together process, procedure, training, structure and other activities to help mitigate against further breakdowns in crucial controls and to build a positive risk culture.

Although I am not qualified to make a legally definitive finding on the point, the two breaches taken together are also likely to meet the threshold for a significant non-compliance with the Finance law in relation to the general duties of officials under the PGPA Act (see Section 25 re the duty of care and diligence), the Accountable Authority Instructions in relation to risk and/or the Commonwealth Procurement Rules. The breaches are of public interest, politically sensitive, impact the public perception and reputation of Finance and in relation to the breach of the general duties of officials, where it is considered significant, it is a requirement for it to be reported to the Minister for Finance where there is also a connection to the management of public resources. While the Minister has clearly been advised of the breaches when they became known, it would be appropriate for the Department to check that it has fulfilled its various reporting obligations in regard to them.

Recommendation 7: The review recommends that the Department consider seeking advice in relation to whether there are any outstanding reporting obligations to the Minister under section 19 of the PGPA Act, or otherwise.

Additional matter raised in relation to Breach 2: Cultural capability

While the primary focus of this review pertains to the circumstances and handling of the two data breaches that occurred, a further issue came to light during the project which raised concerns about the cultural capability of officials in Procurement Division. It is important to note that the Division has amongst its responsibilities a role in relation to the Government's Indigenous Procurement Policy, which seeks to advance the use of Indigenous suppliers in Government procurement.

On Friday 23 February 2024 the Minister for Finance received a written complaint from an Indigenous supplier on the MAS Panel, concerning the cultural insensitivity of colour coding for Indigenous suppliers on the inadvertently revealed spreadsheet. The supplier noted that Indigenous suppliers had been identified by colouring the cells in a particular orange/brown colour and that Indigenous suppliers were the only ones identified with a consistent colouring system.

The intent of the colour coding was to identify Indigenous suppliers on the MAS Panel to assist agencies in meeting their Indigenous Procurement Policy targets. I am aware that the colour has been used publicly in some other contexts that promote or celebrate Indigenous programs or policies; that the colour coding has been in place on the relevant spreadsheet for some time; and am assured that the team had no intention to cause offence in the choice of colour coding.

All that said, it is not surprising that its adoption without any apparent collaboration or engagement with Indigenous suppliers, and its revelation at a moment at which trust with suppliers (Indigenous or otherwise) had been compromised, caused offence to at least one supplier. I am advised that Procurement Division in Finance has apologised for any offence caused to the Indigenous supplier. It has taken steps to change how Indigenous suppliers are identified for legitimate purposes related to the Indigenous Procurement Policy. Procurement Division has advised the review that it will ask relevant staff to undertake culture and diversity awareness training, and indeed a cultural briefing has recently been conducted.

In my view, the steps taken by Procurement Division appear to be appropriate and will need to be sustained.

4. Technology solution

One way to reduce the risks that led to the two breaches subject to this review may be to invest in improved technology. The following material outlines some of the challenges associated with current work processes in the MAS Panel team and work that is underway to modernise government procurement activity through a future IT system called GovPanels, which is currently in development.

AusTender

Based on discussions with team members, there does appear to be significant manual processing involved in the work of the MAS Panel team. For example, the team maintains a large Excel 'master spreadsheet' which includes all the supplier details. This needs to be maintained perfectly as the data is used for updates to other information points including AusTender SON notices, AusTender Dynamic Sourcing for Panels (DS4P) which NCEs use to issue requests for quotes (RFQs) to suppliers, the MAS Panel Search Tool, and the MAS Panel RFQ and Order for Services SmartForms. One error in the data, in one location, can have significant consequences. For example, if an email address is incorrect, it can result in

a supplier not receiving an RFQ through DS4P. These information points for the MAS Panel website are manually updated on a regular basis. Requests for changes come through via the MAS Panel e-mail box and are addressed manually, and this can create a heavy load of manual processes given the size of the MAS Panel. It is difficult for the team to keep pace with manual updates flowing through all elements of the system. I was also briefed by the team on the way in which multiple manual processes are not linked together. For example, the review heard that a change of address could result in manual updates across five different information points.

There is considerable reliance on Excel spreadsheets to manage data inside the team, yet clearly there are various levels of skill and familiarity with Excel which created the exposure that led to Breach 2. An inexperienced user of Excel could and did fail to recognise that there were hidden data sets in workbooks contained within the relevant Excel spreadsheets. More skilled or inquisitive users of Excel could locate the hidden data quite quickly if they were inclined to look.

Future System: GovPanels

The GovPanels platform is planned to replace the AusTender Dynamic Sourcing for Panels (DS4P) Platform. On the basis of a briefing provided to the review, it would appear likely that GovPanels will mitigate the risks that caused both data breaches in whole, or in part.

It is envisaged that the GovPanels system will have three broad components:

1. Allowing officials to undertake a procurement process;
2. Allowing Suppliers to access and manage their own information; and
3. Allowing panel managers to manage details regarding the panel and gather information regarding the utilisation of the panel.

Procuring officials will be able to log-on to GovPanels and undertake a procurement following step-by-step requirements; identify which panels to approach to access specific services and identify the different types of panels, suppliers and standard pricing for those suppliers. Functionally, the system will allow the procurement process to be undertaken within the system, including e-mail notifications and forwarding the proposed procurement decisions to the PGPA Act s23 delegate for initial authorisation, suppliers will respond to the RFx in the system; and evaluation will be undertaken based on that information.

Suppliers will be able to log-on to GovPanels and have their own compartment within the platform which they will manage; it will be possible to have consistent trusted attributions e.g. for Indigenous suppliers; it will also be possible to have other tags not verified e.g. if a supplier identifies themselves as a veteran supplier. The supplier will be able to see the panels they are a member of, including their pricing information.

The Panel Manager will be able to see all rates for their suppliers. They will be able to update rates for each supplier. Under the system there will be no capacity for another supplier to access another supplier's information. The rates and supplier information will effectively be de-coupled; each supplier will be separately allocated an identification code/number; this should reduce the risk of inadvertent release of data; and there will be no single/individual document, for example a spreadsheet that aggregates all suppliers and rates.

GovPanels is largely on track:

- Phase 1. 'Explore Panels' is largely complete and proceeding on time;
- Phase2a 'Approach the market' is currently under development;
- Phase 2b 'Panel Administration' is moving from scoping and design into development shortly; and

- The supplier portal element is planned to commence in approximately six months.

If the proposed timelines hold, the GovPanels platform, and the Supplier Portal, are expected to be online by July 2025.

As things currently stand, an inherent risk of accidental data leakage arises by virtue of all supplier rates and identifying details being available in a consolidated form, not only to relevant Finance officials but also to relevant staff in numerous purchasing agencies. By decoupling supplier rates and supplier information within GovPanels, this risk ought be reduced, but in the meantime there may be merit in Finance reminding agencies of the need to secure the data appropriately.

Recommendation 8: The review recommends that the development of GovPanels continue as a medium-long term means by which some, if not all, of the failings that gave rise to the two breaches subject to this report, might be rectified. However, it is important that more immediate work, canvassed in the earlier recommendations, not be put off in the hope that a future IT solution will deliver all the answers.

5. Supplier perspectives

As noted above, in the time available to undertake this review, it has not been possible to engage with a large sample of suppliers. Nevertheless, I thought it important to speak to a small group and to otherwise familiarise myself with some of the issues that have arisen from a supplier perspective as a result of the two data breaches.

As a result of those inquiries, I make the following observations.

Commercial confidentiality is a central underpinning to the operation of a fair and competitive procurement system. As a result, there are strong provisions in the MAS Panel Head Agreement to ensure that neither the Commonwealth nor suppliers share confidential information other than where authorised in the MAS Panel Head Agreement. At the core of commercial confidentiality are the rates quoted by each supplier on the Panel. It is little wonder that some suppliers expressed strong disappointment about the fact that not just one, but two, breaches of rates data have occurred.

Following the breaches, for some suppliers the task of deleting emails, signing statutory declarations and the like, so as to comply with Finance's directions which are aimed at mitigating the risks arising from the breach, has been straightforward. For others, particularly if the relevant materials have been distributed internally, the task is likely to have been more onerous. That said, I am not aware of any supplier who has, at this stage, made a claim that any actual procurement process has been compromised by either data breach.

While there have been various expressions of concern, it is also fair to note that some suppliers appreciate that the breaches were accidental, they recognise they were the result of human error and that the Department has acted quickly to mitigate the risks involved. Such suppliers continue to seek to engage constructively with the Department in a spirit of mutual respect.

The administrative response to the most recent breach has been intensive and rapid. However, the Department will now need to rebuild trust with Panel members, some of which

are also feeling commercial pressure as a result of the policy goal of reducing reliance on consultants and the operation of the Panel more generally.

More particularly, once the immediate “crisis management” task of getting past the second breach is concluded, it would be timely to ensure that any residual correspondence and issues that arose as a result of the two breaches are considered and responded to in a constructive way, so as to re-focus on the strategic goals of managing a competitive, good value procurement system.

Recommendation 9: Once the immediate tasks associated with managing the data breaches are in hand, the review recommends that the Department ensure that any significant outstanding correspondence or issues raised by suppliers are given appropriate attention, in the interests of re-setting relationships and re-focusing on broader goals.

APPENDIX 1: Terms of reference for review

Independent Review- inadvertent data release of MAS Panel details

Background

In the past 6 months there have been two separate breaches of personal and commercial-in-confidence information of the Management and Advisory Services Panel (**MAS Panel**) that resulted in the disclosure of:

(a) contact information for suppliers, including mobile phone numbers; and

(b) pricing points of all suppliers (the pricing data of MAS Suppliers before the latest repricing exercise).

In both cases, the Department promptly responded when it became aware of the issue, to minimise the impact of the breaches.

Terms of reference

The reviewer must consider the two separate breaches to gather all relevant information for the purpose of determining:

(a) the facts of the two incidents, to determine what led to the disclosure of personal and commercial in confidence information

(b) the Department's response on becoming aware of the inadvertent disclosure and the effectiveness of that response

(c) whether the Department has effective processes and organisation culture for the management of personal and commercial in confidence information collected as part of the management of the MAS Panel

(d) recommendations relating to systems, processes, controls and culture to improve the department's handling of sensitive information and responses to incidents if and when they occur.

Should any further matters be discovered during the course of this review, the reviewers must refer this matter back to the Department to determine the relevance of the allegation/s to this review and if necessary, to amend the Terms of Reference.

Review methodology

The reviewer is authorised to undertake any reasonable activity associated with the gathering of all evidence relevant to this review. These activities could include, but are not to be restricted to, the use of the following:

- Access, obtain, retrieve and copy all agency records considered relevant to these allegations.
- Attend and inspect all relevant agency facilities and/or premises.
- Make reasonable attempts to access any other evidence (i.e. not held by the agency) which is considered relevant to these allegations.
- Give appropriate directions which may be required during the course of this review. For example, that an employee to maintain confidentiality.
- Conduct interviews with persons who can contribute information relevant to the review.

- Seek to conduct interviews with relevant persons who are not employees of the Department, if required.
- Conduct interviews with individuals in relation to their alleged involvement in this matter and record their responses to the interview.

Report

On completion of the review, prepare a written report for the Department's consideration. This report should include the following elements:

- An analysis of the evidence gathered in relation to each incident.
- A description of any systemic or management issues/system deficiencies revealed during the course of the review, that the reviewer/s considers may have contributed to the complaint or incident and make recommendations for systems improvement.
- Recommendations for how systems, processes, controls or culture should be changed to improve the Departments handling of sensitive information.

All interviews, documentation and other evidence gathered as part of this review that is referred to or relied upon in the report, is to be made available to the Department for consideration.

Reviewer's obligations

The review must be undertaken in an impartial and objective manner. During inquiries, should the reviewer/s discover a potential, actual or perceived conflict of interest has arisen, they should immediately cease the review and report the matter to the Department to determine what risk mitigation strategies should be implemented.

Timeframe

The proposed timeframe for completion of a draft report is two weeks from commencement of the appointment. A final report is requested no later than four weeks following the receipt of the draft report.

The reviewer should advise in a timely manner of anything likely to cause delay.

Review Plan

The reviewer is to prepare a Review Plan as soon as possible, articulating their approach and timeframes.

APPENDIX 2: Glossary

APS	Australian Public Service
AIATSIS	Australian Institute of Aboriginal and Torres Strait Islander Studies
AusTender	Australian Government's procurement information system
CBMS	Central Budget Management System
CC	Commonwealth company identified in subsection 89(1) of the PGPA Act.
CCE	Corporate Commonwealth entity identified in subsection 11(a) of the PGPA Act.
CDO	Chief Data Officer
CPRs	Commonwealth Procurement Rules
CRMP	Commonwealth Risk Management Policy
DAT Act	*Data Availability and Transparency Act 2022*
DGF	Data Governance Framework
DVA	Department of Veteran Affairs
Finance	Department of Finance
DS4P	Dynamic Sourcing for Panels (DS4P) Platform
EL1	Executive Level 1
GBE	Government Business Enterprise defined in section 8 of the PGPA Act
Health	Department of Health and Aged Care
MAS	Management Advisory Services
MAS Supplier Matrix	Confidential Information in accordance with Schedule 9 of the MAS Panel Head Agreement.
NCE	non-corporate Commonwealth entity identified in subsection 11(b) of the PGPA Act.
NIAA	National Indigenous Australians Agency
ONDC	Office of the National Data Commissioner
PACT	Procurement and Contracting Team
PEMS	Parliamentary Expenses Management System
PGPA Act	*Public Governance, Performance and Accountability Act 2013*
Procurement Rules	*Commonwealth Procurement Rules* under section 105B(1) of the PGA Act.
Review	Independent Review of inadvertent data release of Management Advisory Services (MAS) Panel
RFQ	request for quote

APPENDIX 3: Senior Commonwealth officials and MAS Panel Suppliers interviewed by the Reviewer.

Interviewee	Position
Senior Commonwealth Officials	
Rob Bradley	Assistant Secretary, Strategic procurement Branch
Andrew Danks	First Assistant Secretary Procurement Division
Andrew Jaggers	Deputy Secretary Commercial Group
Gayle Milnes	National Data Commissioner
Nhi Nguyen	A/g Chief Data Officer Data Governance & Analytics Branch, Budget Policy & Data Division.
Gareth Sebar	Assistant Secretary Procurement Policy and Systems Branch
MAS Panel Suppliers	
Lara de Masson	GHD Advisory, Business Group Leader Government Advisory
Mark Nixon	Partner, EY Oceania Government and Public Sector Consulting Leader
David Robjent	CEO, Grey Advantage Consulting Pty Ltd