Department of the Prime Minister and Cabinet

Privacy Impact Assessment on the case management system – independent complaints and support service for serious incidents

Updated October 2021

Contents

1 Purpose

This Report has been prepared by KPMG for the Parliamentary Workplace Support Service (**PWSS**) to support PWSS's compliance with its obligations in the Privacy Act 1988 (Cth) and the APS Code. It documents the Privacy Impact Assessment (**PIA**) that KPMG has conducted on the implementation of a case management system (**CMS**) that will be used by the Serious Incident Team (**SIT**) to support the independent handling of complaints or reports of serious incidents in the workplace and to provide support services to eligible staff and parliamentarians. The SIT and CMS were originally designed by the Department of Prime Minister and Cabinet (**PMC**) in response to recommendations outlined in the *Review of the Parliamentary Workplace: Responding to Serious Incidents*. The project was transferred to the PWSS in the later stages where the SIT and CMS were formally established. The service will be delivered by PWSS for the foreseeable future.

This PIA considers how personal (including sensitive) information is collected and processed by the SIT in the CMS, assesses the privacy impacts and identifies key privacy risks as well as benefits associated with the CMS in light of the action taken by the PWSS to meet its privacy obligations and address the privacy risks identified during the assessment.

This Report includes information to provide context to the assessment and a table summarising the key risks and recommended steps for PWSS to take or continue taking to address and mitigate these risks, together with some additional observations.

We note that, as the CMS evolves and cases are received by the SIT, other mitigation steps may be taken and/or further privacy risks and impacts may be identified and reflected in this Report by PWSS. These may alter the nature of some of the current risks identified in this Report from the PIA undertaken at a point in time. We also note that the PWSS Privacy Officer intends to revisit the PIA at 6- and 12-month intervals. The PIA may therefore be updated further should any additional risks arise, or any risks already identified be further mitigated.

2 PIA Approach

The PIA enables PWSS to meet its obligations under Part 3 of the *Privacy APP (Australian Government Agencies) Code 2017* (**APS Code**) to consider the relevant information flows and determine whether the CMS configuration appropriately considers and manages privacy obligations. It also outlines practical steps that can be taken to address any privacy risks identified.

The PIA assesses the handling of personal information against the Privacy Act, in particular the Australian Privacy Principles (**APPs**), based on our understanding of the key personal and sensitive information flows in the CMS as documented in the Report.

Given the sensitivity of and purposes for which the information is being handled by the CMS and the SIT, we have also considered the role of employees and their values and expectations in relation to privacy and confidentiality.

As part of this PIA, we have:

- ✓ Assessed the intended scope of the CMS implementation project – including how personal (including sensitive) information will be collected, used, stored and disclosed in connection with the provisions of support services and the review of serious incidents.
- ✓ Interviewed the key stakeholders in PM&C and the SIT as set out in **Appendix 1.** who are involved in the development, implementation and use of the CMS.
- ✓ Reviewed the relevant documentation provided by DP&C set out in **Appendix 2**.
- ✓ Assessed the privacy impacts of the CMS against the Privacy Act and the APPs.

The PIA was originally completed by KPMG on behalf of PMC in August 2021. As the team, system and documentation were still under development at that time it was agreed to update the PIA once more evidence of actions taken could be reviewed. This review was completed in October 2021. As such, the risks ratings, observations and recommendations in this Report reflect KPMG's updated assessment and risk ratings. The main findings section of the Report contains both the original and updated risk assessment the executive summary and risk table reflect KPMG's assessment and ratings as the time of this Report.

3 Disclaimer

This report is solely for the purposes set out in Part 1 of this report for the Commonwealth Parliamentary Workplace Support Service information and is not to be used for any purpose not contemplated in the engagement contract with the Commonwealth Parliamentary Workplace Support Service or distributed to any third party without KPMG's prior written consent. This report has been prepared at the request of the Commonwealth Parliamentary Workplace Support Service in accordance with the terms of KPMG's applicable engagement contract. Other than our responsibility to the Commonwealth Parliamentary Workplace Support Service , neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility. The information contained in this report is of a general nature and is not intended to address the specific circumstances of any individual or entity. Appropriate professional advice should be obtained before acting on this information.

4 Key Findings and Recommendations

4.1 Positive observations

PWSS has established policies and processes which apply to privacy management within PWSS and discussions with key PMC stakeholders demonstrated that a proactive approach was being taken to implement privacy by design in the CMS. This opinion was further confirmed in the follow-up review of the steps and the various documents and artefacts that had been drafted to support and govern the SIT and CMS.

We have also observed that there is a strong emphasis on ensuring that the privacy of individuals accessing the SIT's services is maintained in the SIT's approach to case management.

Some examples of this include:

- The CMS has been designed to enable client consents to be captured on an ongoing basis: Case co-ordinators are able to log the details of what has been consented to, how consent was obtained, the time and date of capture.
- Further, the nature of service delivery means individuals will generally be well-informed and in control of what information is collected about them and when. Case co-ordinators will explain options available to individuals whenever they provide support. This will include an explanation of what information might be required and how this will be disclosed in order to carry out the proposed action. In this way, case co-ordinators will effectively provide just-in-time privacy notices that are relevant to the next steps.
- Detailed guidance for individuals who wish to access the service has been developed and is available online on the PWSS website. It explains in detail the SIT's service, how it is operated, what happens in each scenario where a person seeks support, or where a case is escalated to an independent review. This includes explaining what information is required, when it is required, how it will be used and to whom it will be disclosed.
- There are strong technical controls in the system, including access management, security, and information and records management, which mitigate the risk of a data breach occurring and support greater control over the information captured in the system. While information collected will currently be permanently retained (there is a records retention freeze in place for records relevant to the Jenkins review) , stakeholders have proactively considered long-term issues for data management and the CMS is designed to comply with PWSS's records management policies with a planned review to take place within the next 7 years to implement a retention schedule.

- Case co-ordinators will operate under a principle of confidentiality and anonymity first, meaning information will only be captured when absolutely necessary, collection will be minimised to only what is needed to carry out an action or support the individual, and individuals can withhold their identities until the point they choose to proceed with a formal investigation.
- The system is set up under the Parliamentary Services Commissioner so will be separate from MOPS staff and maintain independence.

Positive findings have been detailed further below against the relevant APP in section 7 below.

4.2 Key risks identified and recommendations

Given that the SIT is newly established, it has been acknowledged by the SIT and PWSS that a continuing focus on privacy management and compliance will be necessary going forward to ensure privacy risks are identified and mitigated and the privacy of individuals is not compromised, as it is essential to the services which the SIT will provide. This PIA has been completed in 2 stages –the assessment was conducted at the time of the development of the SIT and establishment of the team - and a review was undertaken once the SIT and CMS were established and various documents and artefacts were drafted. The Privacy Officer at PWSS has also committed to carry out 6- & 12- month reviews to consider whether any further risks have emerged through the operations of the service.

The key risks identified in this PIA and their ratings are summarised in the table at **Appendix 3.** More detailed assessments are in the sections of this document (under each relevant APP) with both the original assessment and risk ratings and the updated review and ratings reassessment for continuation and transparency purposes.

It is worth noting that risk ratings have been significantly reduced since the initial PIA was conducted in August 2021. This is due to two reasons:

1. Several documents had not yet been drafted, or were only partially drafted, at the time of review in August, meaning ratings were inflated on the basis that it could not be confirmed whether the documents would be drafted in time or whether the documents would be adequate; and

2. The significant work done by the PWSS and SIT team since the initial PIA, and the quality of documents, actions an evidence reviewed in October.

To highlight this: the initial PIA identified 1 Very High risk, 2 High risk 5 Medium risk, 1 Low to Medium risk, and 6 Low risk ratings. The outcome of the updated review and assessment resulted in 1 Medium risk, 11 Low risks and 3 Very Low risks.

As of October 2021, the main residual risk to the CMS will continue to be the Workforce Reviewers. This is because, while the PWSS has implemented several strong controls to ensure the security and integrity of the information that Workforce Reviewers have access to, these reviewers are still external parties to the PWSS and do not work on site at PWSS offices. Given the nature and sensitivity of the information the Workforce Reviewers have access to, the potential for political backlash and reputational damage to the PWSS and DP&C and the potential harms to individuals should such information go public, this risk remains at a Medium but controlled level.

The summary of recommendations has also been included under **Appendix 4.** This summary includes the recommendations provided in the initial August PIA, as well as the current status and commentary as necessary.

Of the 23 recommendations provided in August 2021, 17 have been marked as complete as of the October review. Of the 6 remaining, 3 require only minor follow-ups to close out, 1 is to be considered further by PWSS on whether it would like to proceed or reject the recommendation to conduct a data breach simulation exercise (**11.7**), and the remaining 2 relate to a 6- and 12-month review (**5.1**) taking place on the PIA (which cannot happen until the specified time) and one is open due to a retention freeze (**11.5**) impacting PWSS's ability to dispose of personal information.

These statuses and commentaries can also be found under section 7 alongside the rationale and detailed assessment.

4.2.1 Draft Privacy Policy

In the course of undertaking the PIA, KPMG developed a draft Privacy Policy for the SIT based on a high-level draft which was provided by the SIT. This reflects feedback from our consultation with all key stakeholders and our review of the documents provided. This Policy has been developed to enable the SIT to meet the transparency and collection notice requirements of APPs 1 and 5 and our review and assessment reflects the content of the draft. Feedback on the draft has been provided by the SIT and it will need to be finalised for publishing.

4.2.2 Nature of the SIT's services

In conducting the PIA and after discussion with the SIT, PWSS and PMC stakeholders, the PIA has taken the approach that the SIT counsellors will not be providing a health service (as defined in section 6 of the Privacy Act) to individuals who they provide support services to. This is because the purpose of the service is workplace related and care plans or ongoing counselling will not be provided. Instead, the SIT team will refer individuals to any health service they consider appropriate. However, given the definition of 'serious incident' and the purpose of the SIT, it will be dealing with individuals who may have suffered serious harm in the workplace which has impacted their health and which is likely to result in the SIT collecting health information.

We note that the SIT has, in any event, adopted the approach that all information it collects will be sensitive and will be afforded a similar level of protection as 'sensitive information' (as defined in Section 6 of the Privacy Act) is given under the APPs, such as in relation to consent. This will help ensure privacy risks are managed and the APPs complied with.Background to the CMS

5 Background to the CMS

5.1 Review of the *Parliamentary Workplace: Responding to Serious Incidents Report*

On 16 February 2021, the Prime Minister, the Hon Scott Morrison MP, requested a review of the procedures and processes involved in identifying, reporting and responding to serious incidents that occur in the parliamentary workplace during employment. For the purposes of the PIA and this Report, the term 'serious incident' is interpreted as an incident or pattern of behaviour that causes serious harm to someone and includes assault, sexual assault, sexual harassment and serious and systemic bullying or harassment. This review was conducted by Stephanie Foster PSM, Deputy Secretary of PMC, with a draft report (consultation copy) first released in June 2021. The final report has now been published and is accessible here (the **Foster Report**).

At a high-level, the Foster Report explores the set-up of the parliamentary workplace, risk factors for serious incidents, the existing Department of Finance policies and processes and the effectiveness of current systems with respect to handling serious incidents. The Foster Report identified that existing processes for responding to serious incidents are tailored to responding to those of a less serious nature and are usually only effective where parties are in general agreement as to outcomes. Specifically, they were found not to be fit for purpose when it came to dealing with serious incidents. As a result, the Foster Report provided recommendations aimed at facilitating the uplift of serious incident management going forward. These recommendations focused on ensuring independence from the employer in such processes, empowerment to victims, and timely, effective and ongoing services and support.

The Foster Report emphasised that the sensitivity and complexity of issues that may be reported require significant consideration when implementing new processes. Above all, the Foster Report acknowledged that individuals who are already vulnerable may find themselves subjected to further harm if their privacy were to be breached. In the course of researching best practice, the Foster Review noted the role that new complaint handling processes and CMS could play in providing accurate and comprehensive information to senior leadership about complaint rates and trends. However, it also pointed out the need to balance competing considerations of doing no further harm to victims while still giving them choice and control over the process; providing procedural fairness for the person(s) subject of an allegation; and allowing PMC to enforce work health and safety obligations, so as to prevent future serious incidents.

5.2 The Serious Incident Team (SIT) and Workplace Reviewers

As a result of the Report, the SIT has recently been established to support a safe parliamentary workplace. The SIT is an independent and confidential support and complaint service for current or former *Members of Parliament (Staff) Act 1984* (**MOPS Act**) staff and parliamentarians who have been affected by a serious incident during parliamentary employment and that have occurred since May 2019. Specifically, the incident must have occurred within the current term of the Parliament.

The SIT is established as a function of the Parliamentary Service Commissioner (**PSC**) under the *Parliamentary Service Act 1999* (Cth) and is fully independent of employing parliamentarians, the Executive Government and political affiliations. The PSC retains oversight of the SIT, but is not directly involved in daily operations, nor can access the CMS.

The SIT is comprised of highly skilled counsellors and Case Co-ordinators who have expertise in trauma-informed support and administrative and employment law.

Case Co-ordinators are responsible for responding to inquiries and requests for support, receiving reports made to the SIT and assessing whether a serious incident has occurred. They will work with individuals to determine the most appropriate course of action in relation to their circumstances, whether that be immediate support and/or advice regarding options for further action.

Depending on the nature of the incident and the individual's preferences, case-co-ordinators can provide support and counselling services, or they can refer the matter on to other appropriate services, including supporting a person to make contact with the police; or initiate a local resolution, or workplace review, by formalising a complaint.

The SIT will take a 'no wrong door' approach to any serious incident in the parliamentary workplace, including those involving other building occupants. For individuals affected by a serious incident in the parliamentary workplace who are not MoP(S) Act employees or parliamentarians, the SIT can provide initial support and direct the individual to the appropriate service in order to receive ongoing support.

As the service is available to MoP(S) Act employees, the Department of Finance (**Finance**) retains certain responsibilities regarding workplace arrangements. Where the SIT supports an individual, who requests reasonable work adjustments (such as being able to work from home or reducing hours for a period), the SIT will request these from Finance on the individual's behalf. The SIT will not provide details of the individual's case but simply make the request for the adjustments to take place. The functions of the SIT and relationship between the SIT and Finance are outlined in the

Memorandum of Understanding (**MoU**) For the Independent Complaints Mechanism and Handling of Complaints and Reports Concerning Parliamentary Workplaces.

When an individual wishes to escalate their incident to formal investigation, the SIT will gather relevant information and brief an independent expert workplace reviewer (**Reviewer**). Reviewers are retained under a Commonwealth panel arrangement and will be contracted under a signed Statement of Work (**SoW**). A standard SoW is included under Appendix 2.

5.3 The CMS

To facilitate the work of the SIT, the CMS will be used to record and manage cases of serious incidents as they are reported and the SIT's engagement with clients who seek their services. The CMS will be an internally built and customer relationship management (**CRM**) system built on the Microsoft Dynamics platform hosted in the PM&C01 Microsoft Azure environment. The CMS went live on 30th August 2021.

The CMS will be hosted by PMC using the PMC IT infrastructure. Services are delivered under an ICT Security and Human Resources Services Schedule (v1.0 as at December 2019) which is related to an overarching MoU – Head Agreement (v1.0 as at 19 December 2019) between PMC and the Australian Public Services Commission (**APSC**). The services schedule allows for the full provision of IT Service Desk support, including developing the system, hosting the system in Microsoft Azure, providing IT support, managing access, and infrastructure and applications support.

The CMS will allow Case Co-ordinators to create and edit incident records to ensure individuals receive appropriate levels of support and referrals where required. The CMS will be underpinned by the following principles:

- **Safety** – privacy and confidentiality of personal information and anonymity where appropriate.
- **Trust** – the service is sensitive to peoples' needs.
- **Choice** – the service provides opportunity for choice and allows individuals to have appropriate control over what is reported.
- **Collaboration** – communicate with a sense of unity.
- **Empowerment** – the individual has control over what happens and how their needs are responded to.
- **Respect for Diversity** – respect diversity in all its forms and record information according to the individual's preference.

At the time of the PIA it was anticipated that the SIT had the need for around 10 Case Coordinators in the first year, many of which were being recruited at the time of the initial PIA.

6 Data flows

Where an individual has experienced a serious incident in the parliamentary workplace, they may contact the SIT via several channels, including the following on the basis there is no 'wrong door' for accessing its services:

- By phone or text
- By email
- Face to face

While there are different avenues for communicating with the SIT, a case is generally handled according to the following protocols:

- When an individual first contacts the SIT, a Case Co-ordinator will make them aware of their privacy rights, regardless of the channel used to make contact, or the reason for contact (i.e. support and/or advice only, or formalising a course of action).
    - Where contact is made via phone, the caller will be read the privacy collection notice or be played a recording of the privacy collection notice.
    - Where contact is made by email, consent will be implied, and the email will be responded to by a Case Co-ordinator.
    - Where contact is made face-to-face, the individual will be provided with the privacy collection notice (either as a document or verbally) and consent will be obtained verbally.
- An individual has the option to remain anonymous (or use a pseudonym) in their dealings with the SIT. If an individual chooses to remain anonymous, the case coordinator will provide support, but may need to note that the decision to remain anonymous may limit the options for formal resolution of any complaint.
    - Where an individual chooses to remain anonymous (or use a pseudonym), a record will be created in the CMS and a unique case identifier will be generated. However, no personal information will be collected, or inputs made to the record without the client's express consent.
    - Where an individual consents to being identified, their personal information will be collected, and a record will be created in the CMS. A unique case identifier will then be generated.
    - Examples of where some identifying information will be required would be when escalating a complaint to a formal review process (this is outlined in more detail below) or where the SIT contacts the Finance to request workplace adjustments, such as asking for the individual to be allowed to work from home. This is further detailed under APP6 'Use and Disclosure of Personal information'.
- Best efforts will be made to ensure that cases are generally handled and accessed by only one Case Co-ordinator. In the event that a Case Co-ordinator

is on leave, or otherwise unavailable – a SIT Case Co-ordinator will work with the individual to determine whether they are comfortable and consent to their case being accessed and handled by another Case Co-ordinator, or whether they would prefer to work with their original Case Co-ordinator when they are available again. If the individual is comfortable for another case co-ordinator to handle their matter, it will be expected that the second Case Co-ordinator will take reasonable steps to confirm the identity of the individual they are speaking with.

- Each time an individual contacts their Case Co-ordinator, they will be presented with options as to how they can proceed with their matter. If they choose to continue with further action, the Case Co-ordinator will outline next steps and seek consent to proceed. In doing this, consent is gathered organically at various stages of the engagement and privacy notice information is provided through the explanation of what information is necessary in order to progress with a given option.
- Case Co-ordinators can choose to make notes about any interaction they have with individuals. These notes may either be hand-written or typed directly into the relevant CMS record.
    - Where Case Co-ordinators choose to make hand-written notes, it is expected that they will take significant care to ensure that their security and confidentiality is not compromised. Further, it is expected that Case Co-ordinators will transcribe or scan their notes into the relevant record in the CMS before destroying any physical copies.
- Where an individual wishes to, and consents to, their case proceeding to a workplace review, the SIT will engage a Reviewer. A panel of Reviewers will be engaged in accordance with a Commonwealth contract for consultancy services. They will be individuals who will use their own devices (i.e. laptop, phone) to conduct their reviews.
- The Case Co-ordinator will prepare a review brief based on the information collected to date which will include information from the individual's case record, including their personal and sensitive information. It is intended that this brief will be provided to the Reviewer by secure file transfer rather than email.
    - At the end of the workplace review, the Reviewer will be required to return all the information they have collected in relation to the review they conducted – they will not retain any of the information.
- Reports prepared by Reviewers must be in the form of a template as provided by the SIT. The final report will be delivered to the Head of the SIT and may be tailored, as required. Versions of the reports will be required to be drafted for the complainant, the respondent, the relevant parliamentarian, and the PSC.

- A second, internal review “on the papers” can take place if requested by either party.

Figure 1 and 2 below provide a high-level visual representations of the case management process:

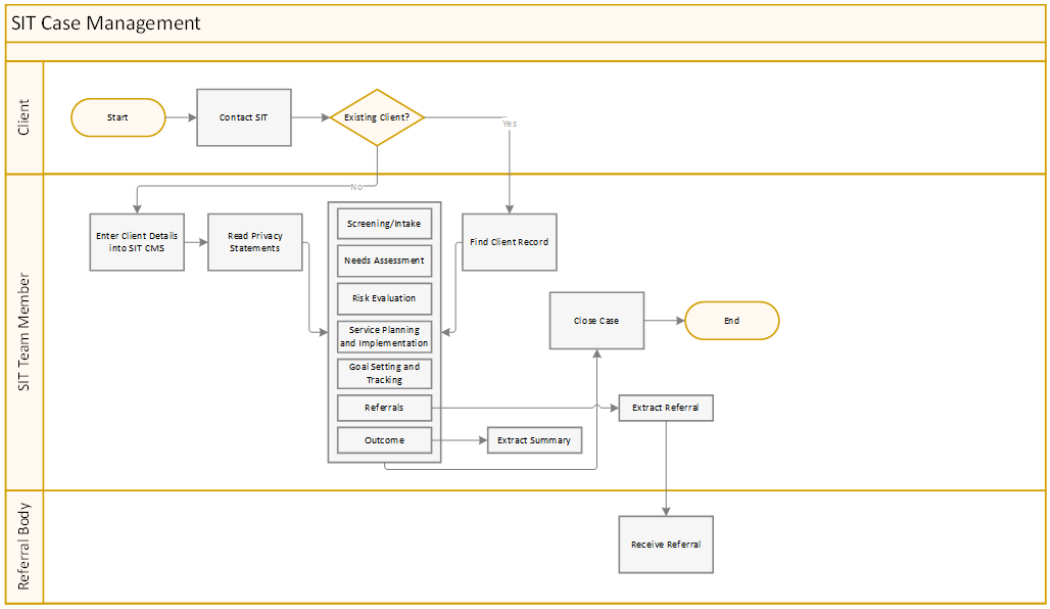

Figure 1 – SIT case management process diagram

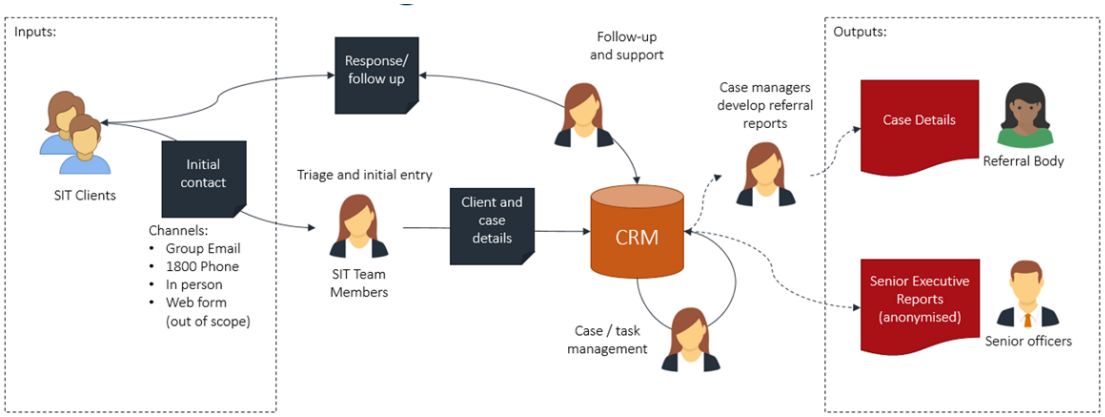

Figure 2 - Business process flow diagram

7 Detailed Assessment

7.1 APP 1: Open and transparent management of personal information and privacy by design

The SIT must develop practices, procedures and systems relating to its functions and activities that ensure it complies with the APPs and enable it to handle any complaints or inquiries about its compliance. It must also have a clearly expressed and up to date Privacy Policy that explains it information handling practices and make it publicly available and provide it on request.

Given the unique nature and purpose of the SIT and that it is newly established, it is still developing some of its policies and procedures and finalising the design of the CMS. It also has not yet collected any client data.

7.1.1 Policies and procedures

The SIT should ensure that staff clearly understand which policies and procedures they must comply with and that apply to the CMS. These may be SIT-specific policies, APSC policies or PM&C policies where appropriate (i.e. the PM&C Retention and Destruction of Original Records Policy).

7.1.2 Compliance

The SIT Compliance Officer will be responsible for monitoring compliance with applicable legal obligations, including privacy and workplace health & safety. The Compliance Officer is responsible for ensuring compliance with agency codes and relevant legislation. At the completion of this PIA it was not confirmed if this role was the appointed Privacy Officer, however it was noted that this would most likely be the case. will continually monitor the handling of personal information and make recommendations as required. They may also coordinate any data breach responses and investigations. The appointed Privacy Officer should have the role of overseeing compliance with the Privacy Act, understanding how personal information is collected and managed in the SIT, and reviewing and reporting on data breaches.

7.1.3 Privacy Policy

KPMG prepared a draft Privacy Policy for the SIT to review and finalise. It will apply to the handling of personal information collected by the SIT. The Privacy Policy must explain the types of personal information the SIT may collect, about whom, the sources of information, the methods and purposes of collection, how it will be used, to whom it will usually be disclosed, how to make access and correction requests and how these

will be handled by the SIT and how to make a privacy complaint and how the SIT will handle complaint. The Policy must also outline whether the SIT is bound to any codes in relation to the personal information it handles.

7.1.4 Data breach response plan

We have been provided with copies of PM&C's data breach response plan which provides guidance for the SIT. However, we understand that a SIT-specific data breach response plan is to be developed prior to the launch of the CMS. The plan and recommendations have been addressed in APP 11 below.

7.1.5 SIT website

The SIT website will provide detailed information about what services and support the SIT can provide, what actions it can take, types serious incidents, and what to expect when interacting with the SIT. It also explains how personal information will be kept confidential, how consent will be sought, the circumstances in which personal information might be disclosed to other parties, including what happens if an individual decides to proceed to a formal workplace review of the serious incident and when the accused party might be informed of the complaint. Further information about privacy notices is outlined under APP 5.

7.1.6 Practices

As a matter of practice, SIT Case Co-ordinators will explain each step that an individual can expect to happen during their case, and provide the choice and control to the individual to decide on a course of action they wish to take and whether they wish to provide their personal information. Formal complaints will not be briefed for independent review by a Reviewer unless the individual consents and it will be made clear to them that they may no longer remain anonymous if they wish to progress to formal workplace review. Consents, use and disclosures are further addressed under APP 6.

7.1.7 Collection notices

'Just in time' privacy collection statements may be available at points where an individual provides personal information, to ensure individuals understand how that information may be used and to capture consent to further actions. This is further addressed under APP 5.

7.1.8 APP1 Risk Ratings

Risk 1

If the relevant policies and procedures are not adequately defined and documented before the SIT and CMS become operational, and if a Privacy Officer is not nominated, there is a risk that personal information will not be managed in accordance with the APPs and SIT staff may not be sufficiently aware of their responsibilities under the APPs.

Risk rating: High

Risk 15

Further privacy risks that may arise as the SIT begins operating and takes on cases are not documented and addressed.

7.1.9 APP1 Recommendations

1.1 The SIT should review and consult with relevant stakeholders on the draft Privacy Policy and once finalised it should be published on the SIT's website before the SIT opens for service. It should also be available in hard and soft copy to be provided on request, for example when anyone visits their office in Parliament. **1.2** The SIT should confirm who the nominated Privacy Officer will be. The Privacy Officer should have responsibility for receiving and handling complaints, access and correction requests, data breach responses and other relevant privacy issues.
1.3 Revisit the PIA at 6 and 12 months and update this Report to identify capture any additional privacy risks and identify steps to mitigate or eliminate them to ensure the CMS and approach to privacy continues to ensure a privacy by design approach.

7.1.10 October 2021 Review

To support the development of the SIT, KPMG drafted a privacy policy for the SIT which was given to PMC. This was subsequently provided from PMC to PWSS and the final version has been published under the resources section of the PWSS website as both a webpage and a PDF version. The policy covers all the requirements of APP1 and is easy to read and understand. The structure clearly articulates how personal information is collected, used, disclosed, and stored, as well as how individuals can make enquiries or complaints.

The privacy section of the PWSS website contains some APP5 collection notice information related to PWSS services and use of the website and these contain links to the full privacy policy housed under the resources section which is available as a web-page and PDF.

The Legal and Governance Officer of PWSS has been nominated as the Privacy Officer and will have responsibility for receiving and handling privacy complaints, complex access and correction requests, data breach responses and advising SIT staff on general privacy matters.

The nominated Privacy Officer has committed to revisit the PIA within 6- & 12-months. This review should consider how the SIT and CMS are operating in practice and whether any additional privacy risks have been found through practice.

7.1.10.1 Reassessment of APP1 risk ratings

Risk 1: The risk rating has been changed to low to reflect that significant work has been done to develop the policies that relate to the personal information handling at PWSS by the SIT team.

Risk rating: Low

Risk 15: The risk has been updated to low to reflect that the Privacy Officer has been appointed and has committed to review the PIA at 6- & 12- month intervals to assess whether any privacy risks arise through the course of operating the service that have not been proactively identified in this PIA. The rating also represents that a lot of work has been done to reduce the risk ratings identified throughout the PIA through the implementation of various policies and processes.

Risk rating: Low

7.1.10.2 Updated APP1 recommendations:

1.1 This recommendation has been marked as complete

1.2 This recommendation has been marked as complete

1.3 This recommendation is still effective as of October 2021 review

7.2 APP 2: Anonymity and pseudonymity

The CMS will allow individuals to remain anonymous (or use a pseudonym) when they engage with the SIT. When an anonymous case is created, a unique case identifier will be generated, and it will not be necessary for a Case Co-ordinator to create a profile which contains an individual's personal information. Further, there will be information

recorded in the case notes which could lead to an individual being identified. A case record may, however, be used for KPI and auditing purposes to demonstrate interaction statistics, etc. For example, where an individual only wants to understand the processes and support available, or the likely events that would occur should they report an incident.

Where an individual does not wish to provide their contact details or other information which could identify them, but wishes to continue interacting with the SIT, a Case Co-ordinator will refrain from collecting contact information and instead agree a time to meet with the individual (either in person or by phone). Where this appointment is scheduled by phone, the SIT Case Co-ordinator will provide the individual with the SIT contact number and the onus will be on the individual to call at the agreed time.

If the individual is happy for notes to be taken during an interaction, particularly where they wish to receive support services, a more detailed case file may be created. In these circumstances it may not be possible for full anonymity, however the individual may still use a pseudonym. This can either be the case identifier, an individual identifier created by the CMS, or a pseudonym of the individual's choosing.

If an individual forgets or loses their case identifier, the assigned case co-ordinator will be able to retrieve it from the CMS. As a general principle, case co-ordinators will aim to minimise the amount of personal information captured while working with the individual and agree on how to address what the individual is comfortable having recorded.

If an individual wishes to progress their complaint to a formal investigation and review, it will no longer be possible for them to remain anonymous. Case co-ordinators will explain this and the likely series of events to individuals and will only progress with the individual's explicit consent. This will result in the details of the complaint being disclosed to the Reviewer to conduct an independent investigation. The accused party will also be informed.

Should the individual wish to request workplace arrangements then some information will also be required and disclosed to Finance. Only enough identifying information will be required to implement the arrangements. No details about the individual's circumstances or reported incident will be shared.

7.2.1 APP2 Risk Ratings

Risk 2

If information-recording protocols are not adequately defined for cases in which an individual wishes to remain anonymous, there is a risk that Case Co-ordinators could unwittingly record information that identifies an individual.

Risk rating: Medium

Risk 3

It may not be clear how individuals can request access to information, or what information is necessary to collect in order to provide such access. This is especially relevant in cases where individuals chose to remain anonymous.

Risk rating: Low

7.2.2 APP2 Recommendations

2.1 The collection notice should make clear that an individual may remain anonymous and Case Co-ordinators should explain this to individuals who contact the SIT for support. They should also be able to explain the circumstances in which individuals may not be able to remain anonymous.

2.2 Case Co-ordinators should have documented guidance detailing the protocols for recording information and progressing anonymous complaints. This guidance should detail what can and cannot be recorded in the case notes of an individual who wishes to remain anonymous, and should highlight the point at which the individual will need to identify themselves in order to proceed with the matter.

2.3 A process for providing access to personal information where an individual choses to remain anonymous, or was using a pseudonym, should be developed. This could be by using the case identifier and asking the individual to provide details only they would know to verify the case. Alternatively, an individual may wish to provide a passcode to be quoted whenever discussing the case.

7.2.3 October 2021 review

Since the initial PIA, PWSS has drafted a privacy policy which contains information explaining an individual's ability to remain anonymous when liaising with the SIT team and when this might not be possible. Information about anonymity has also been embedded into the conversation when an individual contacts the SIT team. The PWSS Procedures_Referrals and Intake document advises SIT staff on how to set up a client record when an individual wishes to remain anonymous and the SIT CMS – User

Guide v1.1 contains a section advising the reader how to create anonymous client records in the CMS. The PWSS Templates_Intake Form with Prompts asks for a name or pseudonym and contains talking points in the appendices related to consent and confidentiality.

It is clear from the guidance and procedural documentation that an individual can always remain anonymous when interacting with the SIT team, and that steps have been taken to ensure this anonymity can be managed, unless an individual wishes to refer their case for workplace review in which case they must forego anonymity in order for a formal investigation to take place.

When an individual chooses to remain anonymous, they may either use a pseudonym or their case file number instead to continue discussing their case. They may also set a password to access their case to enhance security and confidentiality. While the SIT Team acknowledge that situations may arise where they cannot verify the identity of an individual (such as if the individual forgets their passcode), these procedures will generally satisfy the obligation to ensure individuals can access their personal information on request.

7.2.3.1 Reassessment of risk ratings:

Risk 2: Anonymity procedures have been well considered, designed, and implemented. These are sufficiently communicated at several points during an interaction between the SIT team and an individual. This risk has therefore been re-assessed as low.

Risk rating: Low

Risk 3: Procedures have been put in place to ensure individuals can remain anonymous but still access their information. The use of a passcode and a pseudonym means an individual may continue to interact with the SIT team in a secure manner and that the SIT team can be assured they are speaking with the same individual. This also ensures individuals can be verified for the purposes of information access requests without compromising their anonymity.

Risk rating: Very Low

7.2.3.2 Updated Recommendations:

2.1 This recommendation has been marked as complete

2.2 This recommendation has been marked as complete

2.3 This recommendation has been marked as complete

7.3 APP 3: Collection of solicited personal information

APP 3 permits personal information to be collected by an agency if it directly relates to, or is reasonably necessary for, one or more the agency's functions or activities. Personal information will generally only be collected with consent.

The SIT service is set up to collect information in relation to serious incidents (as defined above) and to provide support services as well as other activities defined in the draft Privacy Policy. While not all of the personal information that may be collected, falls within the definition of 'sensitive information' in Section 6(1) of the Privacy Act (see also Section 4.2 above in relation to our findings about the nature of the SIT's service), given the purpose for which it is being collected and the nature of the SIT's functions and activities, all information collected will be considered to be sensitive and will not be generally be collected without the consent of individuals.

The draft Privacy Policy details some of the information that the SIT expects to collect. Further, the SIT website is being designed to describe its services and what an individual can expect when interacting with the SIT, including the information they may be asked to provide. Case co-ordinators will also explain this to individuals and seek consent at various stages in the management of the case prior to collecting information, or before making a disclosure. These consents will be logged in each case record in the CMS under the 'privacy notices' section. Drop-down menus can be selected to explain how consent was collected (i.e. orally, in writing, etc.).

For the purposes of the CMS and the SIT's service, implied consent is considered to be obtained when an individual emails the SIT or approaches and proactively provides information. However, Case co-ordinators will always endeavour to explain to individuals what to expect in relation to the collection and handling of their information and the options available so that they are empowered at every step of the process to control decision-making in relation to progressing their cases and the information they are comfortable providing. As a result, an initial implied consent to collect information will later be superseded by explicit consent to take further action (i.e. prior to commencing a workplace review which may result in the collection of further information).

While consent to collect personal information that is not sensitive information is not required by APP 3, the SIT's decision to treat all information it collects as sensitive means that it will generally seek consent prior to collecting any personal information.

The SIT may also collect information about individuals when referrals are made to it by the Australian Federal Police (**AFP**), Department of Parliamentary Services and its "1800" support line. It is also possible that personal information may be received from Finance when the SIT is seeking to confirm an individual's status as a MOPS employee. However, this would only occur with the individual's knowledge and consent.

Given the nature of the SIT's service, it may collect information about individuals such as accused parties without the knowledge of those individuals. This information may be necessary in order to support the complainant in the management of their case.

Further, when a workplace review occurs and support is provided to the respondent or another staff member or witness, personal information about an individual may also be collected in this way.

7.3.1 APP3 Risk Ratings

Risk 4

If the SIT does not obtain valid consent, particularly to collect sensitive information, there is a risk that it will breach APP 3. Further, there is also a risk that consent may not be adequately captured where an individual was referred to the SIT, or where consent was implied or gathered orally.

Risk rating: Medium

7.3.2 APP3 Recommendations

3.1 Consideration should be given to the collection of an individual's personal information from a third party. The SIT should adopt a clear and consistent approach to the collection of this information and that individuals are informed of the potential for the SIT to collect it. It may not be practical or possible for the SIT to obtain specific express consent to the collection of such information. However, where information is obtained via a referral, the SIT should ensure the referring party has obtained consent and, where necessary, seek further consent from the individual to take further action.)

3.2 The SIT should ensure that in each case where consent is collected the consent is valid. That is, while the consent may be express or implied; it must be informed, given

voluntarily, time-bound, specific and the individual must have had capacity to understand and communicate it.

7.3.3 October 2021 Review

The newly drafted PWSS Privacy Policy explains that PWSS may collect personal information from third parties including government agencies, witnesses, complainants, respondents and authorised representatives. It outlines when this may happen in a manner that was solicited or unsolicited as well as how PWSS will go about gathering consent and the circumstances where consent may not be feasible or required.

The PWSS Procedures_Referrals and Intake document provides detailed guidance to the SIT team about how to handle referrals from third parties, including that unsolicited information or information gathered without appropriate consents will not be recorded. Where a SIT team member contacts an individual, they will go through the PWSS privacy and confidentiality information with them to ensure that any further collection of information, or any concerns about how consent was previously captured by a third party, will be managed.

Further, the CMS includes consent gathering mechanisms which are explained in the SIT CMS – User Guide v1.1. The PWSS Templates_Intake Form with Prompts provides guidance around consent as well as a consent capture box, however the consent box reads as though it is asking whether a discussion about consent took place, as opposed to whether the individual consented to the collection of their personal information. While oral consent is a valid form of capturing consent, for the avoidance of doubt it would be recommended that the language on this form be updated to ask whether the individual has consented to the collection of their personal information.

7.3.3.1 Reassessment of Risk ratings:

Risk 4: The risk has been updated to low given the amount of notice information and guidance that has been developed since the August review. While there is still a risk that consent could be contested based on the language of the intake form, this risk is low given it is based on a discussion that happens between the SIT team and individuals and that the intent of the form is to act as a temporary document for the information to be later transferred into the electronic CMS with the appropriate consents chosen in the system. That said, it would be recommended to update the language on the intake form for the avoidance of doubt.

Risk rating: Low

7.3.3.2 Updated recommendations:

3.1 This recommendation is marked as complete

3.2 This recommendation is marked as still effective on the basis of the consent language in the intake form only. It is recommended that the consent box language be updated so that, instead of suggesting it is a tick box to confirm that conversations about consent took place, it captures consent for the individual's personal information to be collected for the purposes of creating and managing a case.

7.4 APP 4: Dealing with unsolicited personal information

As outlined above, information will generally be solicited from individuals who will control decisions upon how to progress their case. Information may be unsolicited even where it is proactively provided by the individual.

Given its functions and the publicity about its establishment and work, over time, the SIT could receive anonymous reports about conduct of MOPS staff or parliamentarians.

If it receives unsolicited reports, the SIT will need to determine whether it relates to a serious incident, whether it directly relates to its functions and activities, whether it needs to delete the record in accordance with the agreed records management process, or to send the information to another agency or Department.

7.4.1 APP4 Risk Ratings

Risk 5

If professional judgement is incorrectly or inconsistently applied, there is a risk that unsolicited personal information could be recorded on an individual's case record.

Risk rating: Low

7.4.2 APP4 Recommendations

4.1 Develop guidance for staff that outlines how to consider and handle unsolicited information. As a general principle, information should only be recorded in the CMS that is necessary and directly relevant to the functions and activities of the SIT (i.e. that is necessary in order to support the individual).

7.4.3 October 2021 Review

PWSS have developed and delivered privacy training to SIT staff. These include a general overview of al the APPs, as well as a more detailed training focused on APP4 – collection of unsolicited personal information. This training provides a thorough overview of the obligations under APP4 and includes questions and key considerations which are tailored to PWSS employees. It also includes some examples and scenarios to apply the learning to.

The training also builds on use and disclosure (APP6) and security (APP11) as they relate to APP4 to give recipients a well-rounded understanding of what must be done when handling unsolicited information, as well as any exceptions or whether the collection or handling might constitute a breach and, if so, what steps to take.

Other documents drafted by the PWSS also provide guidance in relation to unsolicited information. As mentioned under APP3 above, the PWSS Privacy Policy outlines how PWSS will handle unsolicited information, and the PWSS Procedures_Referrals and Intake document provides detailed guidance to the SIT team about how to handle referrals from third parties, including that unsolicited information or information gathered without appropriate consents will not be recorded. The PWSS Templates_Intake Form with prompts also includes advice around consent.

7.4.3.1 Reassessment of risk ratings:

Risk 5: The risk is rated as low as the PWSS has developed several documents, including training, procedures, forms and policies, to ensure SIT staff are aware of the risks of unsolicited information and how to manage it.

7.4.3.2 Updated recommendations:

4.1 This recommendation is marked as complete.

7.5 APP 5: Notification of the collection of personal information

A draft collection notice has been developed by the SIT. This briefly explains that the SIT is a function of the PSC, outlines when personal information is collected, and provides a link to the SIT Privacy Policy. A draft Privacy Policy has been drafted by KPMG in consultation with the SIT which also contains relevant information.

We understand that a collection notice will always be presented, whether verbally or in writing, or via a recorded message.

The use of a collection notice supports the SIT to take reasonable steps to make individuals aware of certain matters prescribed in APP 5. What information needs to be provided and what the person will be aware of will depend on the nature of the SIT's relationship with the individual and status of their case, as well as the nature of the engagement.

The matters prescribed in APP 5 are:

- The SIT's identity and contact details;
- The facts of and circumstances in which the information is collected;
- Whether the collection is required or authorised by law;
- The purpose(s) of collection;
- The consequences if personal information is not collected (i.e. if they wish to remain anonymous or not provide the information);
- The usual disclosures that the SIT may make of the personal information it collects;
- Information about the SIT Privacy Policy and reference to the ability to make access and correction requests and privacy complaints; and
- Whether the SIT is likely to disclose personal information to overseas recipients (please note, we have determined that this not applicable).

Case co-ordinators will typically respond to the information presented by providing an explanation as to the options available to the individual and seek consent to progress. This will effectively act as a 'just in time privacy notice' and explicit consent to continue to collect it.

7.5.1 APP5 Risk Ratings

Risk 6

Collection notices are not finalised at the time of writing this PIA. If a privacy collection notice is not used when personal information is being collected, there is a risk that individuals contacting the SIT are not adequately aware of the matters referred to under APP 5 (please see above). If this occurs, it may result in the SIT being in breach of their duty to take reasonable steps to make people aware of these matters.

The detailed web guidance drafted by the SIT helps to mitigate this risk as well as the general approach the Case co-ordinators will adopt, which involves always informing the individual and seeking consent to continue.

Risk rating: Medium

7.5.2 APP5 Recommendations

5.1 Various formats of collection notices should be developed and used at each specific point that an individual may use to contact the SIT having regard to the above. Some examples include:

- A short collection notice to auto-play to a person who calls in to the SIT phone number. It should outline key information and refer to the Privacy Policy online.
- An auto-response email that is sent to the individual when they email the SIT, as above.
- A leaflet or other form of hard copy collection statement available at reception for 'walk-ins' as well as copies of the Privacy Policy.

7.5.3 October 2021 Review

The PWSS has developed two specific privacy collection notices for individuals which are available on the PWSS website. The ‘Individual accessing services of the PWSS – APP5 notice’ (1) relates to individuals accessing the service, interacting with Case Coordinators and providing personal information in relation to an incident. The ‘Accessing the PWSS website – APP5 notice’ (2) relates to the use of the PWSS by any visitors to that site, and how the website collects personal information. Both collection notices are available under the ‘privacy’ section of the website.

Each collection notice meets the requirements of APP5. In particular, collection notice 1 outlines who personal information may be received from or disclosed to in relation to the management of a serious incident or a workplace review, when personal information might be collected, used or disclosed without consent, and how an individual can make enquiries. It also links to the privacy policy listed under the resources section of the website.

The PWSS_Templates Intake Form with Prompts also advises Case Coordinators to discuss privacy and confidentiality with an individual and to obtain consent before any of their personal information is recorded and includes useful information for discussion in the appendix. This can also be shown to an individual if the meeting is face to face. Training modules also advise Case Coordinators to ensure they provide relevant collection notices to individuals and that consent is captured before proceeding to gather and use personal information.

Further collection notices are intended to be developed on an as-needs basis if the PWSS Privacy Officer deems this appropriate during the 6- & 12-month follow-up reviews of this PIA

7.5.3.1 Reassessment of risk ratings:

Risk 6: The rating has been reassessed to low on the basis that adequate collection notices are available online, and that the procedures, forms, policies and training all encourage and support Case Coordinators to provide notice and collect valid consent - of which adequate notice is a requirement. It is also understood that the need for further or enhanced notices will be under constant review, and will be revisited during the 6- & 12-month follow-ups to this PIA by the Privacy Officer.

Risk rating: Low

7.5.3.2 Updated recommendations:

5.1 This recommendation is still effective on the basis that the Privacy Officer has committed to continue to review and update notices on an as-needs basis, and to review during the 6- & 12-month PIA follow-up reviews.

7.6 APP 6: Use or disclosure of personal information

The draft Privacy Policy sets out the purposes of collection and uses and disclosures the SIT may make of personal information it collects.

Typically, personal information collected by the SIT will only be for the primary purpose of providing the services to carry out the SIT's functions and activities. Such services may include: guiding and supporting the individual through strategies, keeping them updated, signposting to support services, liaising with stakeholders such as line managers or Finance to support the individual with working from home or time off arrangements, or supporting the individual to make an official complaint to trigger an independent workplace review. As outlined in section 5.2, any disclosures to Finance will operate under the MoU and will not include details of the individual's

Disclosures may also occur where the individual nominates a support person, requests a review or agrees that the SIT may refer their case to a third party.

If it does not have consent or the SIT could not demonstrate that the individual would not reasonably expect it to use or disclose their information for a particular purpose, the SIT may rely on a relevant 'permitted general situation' (Section 16(A) Privacy Act) such as where:

1) The SIT reasonably believes disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety and it is impracticable to obtain consent;
2) The SIT is taking appropriate action in relation to suspected unlawful activity or serious misconduct relating to its functions or activities; or
3) It is necessary to conduct an alternative dispute resolution process.

There are limited circumstances in which exception 1) would apply.
Given the nature of the SIT's services, exception 2) may apply if it determines that a serious incident has occurred. However, this use or disclosure is likely to be consistent with the primary purpose for which the information was collected in the first place.

The SIT also provides a dispute resolution mechanism. Should an individual, whether the complainant or person accused, be unsatisfied with the result of an investigation,

the individual may request a second review ('on the papers') of the incident take place by a different independent reviewer. In this event, personal information related to the case may be disclosed to a third party in order to validate or challenge the initial investigation findings.

Given the nature of the SIT's service, it may use the information it collects about individuals such as accused parties without the knowledge of those individuals. This information may be necessary in order to support the complainant in the management of their case. The SIT website content sets a reasonable expectation that an individual's personal information may be collected without that individual providing consent, insofar as that information is relevant and necessary to investigate or review a case.

The PM&C provides the SIT with ICT support including the CMS, communications services and other relates services. As outlined under Section 5.3 above, the ICT services are supplied under a schedule of services under an overarching MoU. Accordingly, specific individuals within PM&C ICT will have access to the systems and data. Infrastructure specialists will have access to the technology infrastructure to provide support, but will not have access to data. Staff with access to backend data and software will not have access to infrastructure. Neither of these staff will have control over access. Access requests will be managed by a manager in the SIT as outlined under APP11. No additional disclosures will occur beyond that which is necessary for PM&C to supply the services.

7.6.1 APP6 Risk Ratings

Risk 7

Disclosure of information may not be consistent with APP 6 if consent has not been obtained. As such, an individual may not understand that their information being disclosed to a Reviewer if they wish to progress their case to a workplace review. Their consent in this instance should therefore be explicit and not implied. It will not be necessary to seek consent where the Case Co-ordinator reasonably believes a person is in immediate risk of serious harm, however such incidents should involve a validation process with a trained supervisor or other adequately experienced employee where possible. We understand that where a call is received out of hours, that this may not be possible and the Case Co-ordinator should, therefore, rely on their professional judgement in the situation (i.e. prioritising the wellbeing of the individual at risk).

Risk rating: Low to Medium

7.6.2 APP6 Recommendations

6.1 Although an exception may apply, the SIT should still ensure that affected individuals are made aware of the potential for disclosure of their information and to whom. For example, this could occur in the collection notice, the Privacy Policy, and on the SIT website and during discussions with them.

6.2 When a case is to be referred for independent review, there should be a proceed for seeking explicit consent, such as the individual signing that they agree to the disclosure.

6.3 Where the SIT may use or disclose information to lessen or prevent a risk of serious harm, there should be an escalation or validation step where possible and reasonable.

7.6.3 October 2021 Review

Since the initial PIA, the SIT have drafted and published the Privacy Policy and privacy notices on the PWSS website. As previously noted, this policy outlines the circumstances in which personal information might be used and disclosed, as well as when such uses and disclosures may take place without consent. The collection notices also advise how personal information is collected, used and disclosed and is clear about the purposes and when information might be used without consent. The PWSS Procedures_Referrals and Intake document outlines the steps for Case Coordinators to follow when collecting, using and disclosing personal information, which include steps to verify the use cases match APP6 obligations to minimise legal and privacy risk, and includes guidance on how to advise individuals about these processes. The PWSS Templates_intake Form with Prompts document includes an appendix of information which includes information around consent and personal information handling by PWSS to be discussed with individuals during face-to-face meetings.

In addressing recommendation 6.2, the PWSS Procedures_Referrals and Intake document clarifies the steps when receiving referrals to the PWSS or when collecting personal information from individuals and this is also mentioned in the relevant privacy policies, notices and forms. The FINAL Handling personal and sensitive information, also outlines rules for consent and transparency and individuals are informed that in order to progress to workplace review, further consent to do so is required and the individual would no longer be able to remain anonymous, meaning additional personal information will need to be collected and disclosed in cases where an individual had relied on a pseudonym until now. The PWSS Procedures_Workplace Review for Case Coordinators also explains the procedure for making referrals and how to engage with

individuals to proceed with such reviews, including confidentiality requirements and steps an individual must take to sign their consent.

Further, a Memorandum of Understanding (MoU) has been drafted between the PWSS and Department of Finance which clarifies the situations when information might be disclosed from the PWSS to the Department of Finance, and the responsibilities and permitted uses by each party over such personal information. Additional documents, including the PWSS Procedures_Release of Information (Incl WHS risk) document specifies when and how personal information should be released from PWSS in situations where consent might not be feasibale (such as for serious incidents or imminent risks of danger to individuals), and the contracts drafted for signing between PWSS and Workplace Reviewers also outline the permitted purposes, uses and disclosures relating to personal information shared as part of a workplace review.

7.6.3.1 Reassessment of risk ratings:

Risk 7: This risk has been updated to a low rating to reflect that considerable work has been done by PWSS to document procedures, guidelines and expectations. Notices clearly articulate to individuals how their personal information will be used and disclosed, and various arrangements are in place to govern this, including MoUs and contracts with Workplace Reviewers.

Risk rating: Low

7.6.3.2 Updated recommendations:

6.1 This recommendation is marked as complete

6.2 This recommendation is marked as complete

6.3 This recommendation is marked as complete

7.7 APP 7: Direct marketing

The SIT will not use personal information it collects for direct marketing purposes.

7.8 APP 8: Cross-border disclosure of personal information

All personal information will be hosted in Australia in a Microsoft Azure cloud server and will not be disclosed or transferred to any overseas recipients.

7.9 APP 9: Adoption, use or disclosure of government related identifiers

The SIT will not collect, use, or disclose government related identifiers.

7.10 APP 10: Quality of personal information

APP 10 requires the SIT to take reasonable steps to ensure that any personal information it collects and uses or discloses is accurate, up to date and complete and (for uses and disclosures) relevant.

Given the sensitivity of the information being collected and its potential impact, what will be considered reasonable steps for the SIT to take may be more onerous to ensure the quality of the information being recorded in the CMS and used or shared.

While the CMS contains free-text fields, the SIT has defined some specific fields which are necessary to collect regarding a case as the case develops. Further, the SIT is in the process of developing guidance about what information should be entered into these fields, and how it should be entered. We acknowledge that the SIT and CMS are not yet operational, so further review of this guidance may be required as the SIT gains a better understanding of the way Case Co-ordinators are using free-text fields. We also acknowledge that some flexibility is necessary as each case will be different and it would be unreasonable to explicitly define or categorise all cases.

Going forward, the intention is for Case Co-ordinators to be trained and educated upon what information needs to be gathered and how it should be entered into case records in the CMS.

7.10.1 APP10 Risk Ratings

Risk 8

If there is a lack of consistency in the way free-text fields are used, this could result in inconsistencies in the quality of information recorded against different case records. This could impact the effectiveness and the outcome of a workplace review.

Risk rating: Low

7.10.2 APP10 Recommendations

10.1 While training will help to ensure the quality of the information being collected by the SIT, further steps should be taken to maintain the integrity of the data given its

particularly sensitive nature. Additional mechanisms designed to safeguard the integrity of the data are could include:

- Outlining the circumstances in which individuals should be contacted, or other records checked before their information is disclosed, for example to a Reviewer; and
- Ensuring updated or new personal information is promptly added to relevant existing records.

10.2 Develop guidelines that Case Co-ordinators will follow when entering personal and/or sensitive information in any free-text fields. These free-text fields should be reviewed after the SIT and CMS has been operational for 12 months to determine whether new prescriptive text fields need to be created. For example, these guidelines may address:

- Protocols that ensure personal information is collected and recorded in a consistent format. For example, noting on a record when the personal information was collected and the point in time to which it relates, and if it is an opinion, or fact.

7.10.3 October 2021 Review

Since the initial PIA, the design of the CMS has been finalised and implemented. Free text fields were reviewed and additional fields have been added to reduce the need to rely on free text. In particular, the following fields have been included:

Employers (MoPs)

- Referral Methods
- Referral Channels
- Nature of Incident
- Relationship to Incident
- Services Requested
- Referral Reasons (referrals out)
- Referral Bodies
- Activity Purposes
- Relationship Types

There are also specific fields for Title; Name, Pseudonym and preferred name; contact information; and address. While these fields are also free text, they have separate fields

for entry than the free text commentary fields, which allows a level of control over the visibility of this information and allows it to be tagged, searched and edited as necessary.

Further data fields, including screenshots of the CMSD, are contained in the SIT CMS – User Guide v1.1.

The guidance included in the user guide, as well as the strong emphasis on training and various guidance documents including the PWSS Protocols_Case Notes, the PWSS Procedures_Referrals and Intake and the FINAL Handling personal and sensitive information documents decrease the likelihood of free entry fields being used inconsistently.

7.10.3.1 Reassessment of risk ratings:

Risk 8: This rating has been updated to very low to reflect the additional fields embedded into the CMS and the range of targeted guidance and training which reduce the likelihood of errors or inconsistencies in data entry.

Risk rating: Low

7.10.3.2 Updated recommendations:

10.1 This recommendation is marked as complete

10.2 This recommendation is marked as complete

7.11 APP 11: Security of personal information

7.11.1 Security and access

APP 11 places two obligations upon the SIT. The first is to protect personal information from misuse, interference and loss (11.1(a)); and from unauthorised access, modification or disclosure (11.1(b)). The second requires the SIT to take reasonable steps to destroy or de-identify personal information if it is no longer required (11.2)

PM&C will protect personal information via the use of ICT security and access controls. The PM&C01 Microsoft Azure environment will house the CMS. PM&C01 is a hybridised environment which is integrated with the PM&C protected network. PM&C01 has been security risk assessed and is secured in accordance with Protective Security Policy Framework (**PSPF**) protocols. PM&C01 is authorised to hold information classified at the Official/Sensitive level and documentation is currently underway to authorise the environment to hold Protected information.

At a granular level, security of the CMS will be ensured by the completion of a security risk assessment prior to the system going live. At this point in time, this assessment has not yet been completed so no comment can be made as to the finding of any risks which could alter our conclusion of any security risks.

Access requests for the CMS will be handled by the SIT Manager. An access request form must be filled out and submitted via ServiceNow for access to be approved and provisioned by the service desk team. With this application, requestors will need to show evidence of their completion of mandatory privacy training. There are two role profiles which can be assigned to users (i.e. SIT Team Member and SIT Manager). When access to the CMS is granted, users will be able to login via single sign on (**SSO**) protocols. Users will also be granted with access to the linked SharePoint site.

Complete audit trails will be kept of all access and amendments to case records. These trails will track who accessed the record, when they accessed it, and what was changed or added. This will apply to all fields, including free-text case notes.

If a user leaves their role, their access to the CMS will be terminated as their SSO credentials will be terminated. If a user moves roles within PM&C or APSC, it will be the responsibility of the SIT Manager to ensure that their access to the CMS and accompanying SharePoint site is promptly revoked.

Access management processes have been defined and documented in draft in the SIT Case Management Design Document.

In addition to the user access management processes, there will also be the ability for individual case records to be locked down to select users only.

We understand that Reviewers will be independent contractors who will be collecting information and performing their workplace reviews using their own devices (such as a laptop) and may use unsecured third-party email applications, such as Gmail or other systems. As discussed with the SIT, it intends to share briefs with Reviewers by a secure file transfer link. However, this has not yet been established. Further, it is not clear whether Reviewer panel members have each been risk assessed.

7.11.2 Physical access

The CMS will only be accessible on PM&C devices and accordingly, the PM&C Working from Home Policy will apply. This Policy outlines how sensitive information should be treated and handled when working remotely.

7.11.3 Retention

We understand that implementation of the CMS has been conditionally approved, subject to recommendations by the PM&C Records Management team. While PM&C's Retention and Destruction of Original Records Policy and Information Management

Policy, will be applied to CMS case records, a decision has been made to retain case records for an indefinite period until a review is conducted to revise retention requirements for the case information. This is a risk-based judgement founded in the rationale that there is insufficient clarity pertaining to the exact information that will be collected and stored by the SMS. Further, the CMS cannot currently facilitate audit logging for case record deletions, but we do acknowledge that deletion of records will not be possible by SIT staff.

7.11.4 Data breach response plan

The development of a plan for the SIT was discussed during consultations to me the SIT's Notifiable Data Breaches scheme obligations (in Part IIIC of the Privacy Act).

7.11.5 APP11 Risk Ratings

Risk 9

If there is a lack of appropriate governance over user access reviews, there is a risk that necessary user account terminations may not be completed in a timely manner. This could result in unauthorised access to, and use of, personal information held in the CMS.

Risk rating: Low

Risk 10

There is a risk that case records could be retained for longer than the permitted period if requirements are not formally defined.

Risk rating: Low

Risk 11

Given that Reviewers will be individuals who will not be working from a secured enterprise work environment and will be using their own devices to conduct reviews and may be collecting and sharing information via unsecured third-party systems, there is an increased risk that a complainant's personal information may be stored insecurely or exposed to a data breach.

Risk rating: Very High

Risk 12

There is a risk that data breach incidents may not be appropriately handled and reported (where relevant) if a response plan is not formally documented and communicated. This could result in negative consequences for the SIT and other relevant parties, including reputational damage, fines, and harms to individuals.

Risk rating: High

7.11.6 APP11 Recommendations

11.1 Ensure that PM&C and SIT staff are adequately training and informed of their respective roles and responsibilities in relation to information security (i.e. SIT Managers having the responsibility to approve access requests and PM&C having the responsibility to co-ordinate user access reviews).

11.2 Ensure that governance requirements are outlined for user access reviews (i.e. require SIT Manager to action/validate user listing with PM&C support team within 48 hours, etc.).

11.3 Reviewer panel members should be risk assessed before they are employed under the Commonwealth contract for consultancy services. The risk assessment should consider the Consultant's working environment, capabilities to protect information, policies and processes or ability to adhere to the SIT's policies, and other factors that may create security or other risks to the SIT or MoP staff.

11.4 Ensure that a secure file transfer mechanism has been set up and is operational to enable briefs, reports and other information to be securely shared with Reviewers or other third parties. If it is established that independent reviewers do not have secure environments to work from, the SIT should establish a process whereby Consultants access the files within the PM&C environment and are unable to extract information. In such cases, controls will need to be in place to maintain the independence of the Consultant, such as ensuring Case Co-ordinators are unable to access the folders that the independent Consultants work from. The SIT should also ensure Reviewers follow any protocols that support the security of case information and reports when collecting, storing or sharing these.

11.5 Once the CMS has been operational for a period of time (no greater than 7 years), conduct a review of case record retention requirements and formally define them. This

review should also address retention and destruction requirements for paper-based notes.

11.6 PM&C ICT staff should carry out a security risk assessment prior to the system going live.

11.7 Once the CMS and SIT are operational, the data breach response plan should be developed using a best practice approach reflecting the guidance and processes in the PM&C's documented plan. This should reflect the broader PM&C data breach response plan and address different types of incidents that could result in a data breach, such as a compromise of the CMS, an action of SIT staff or Reviewers, including human error and the leaking of reports. PM&C and the SIT should consult together to ensure that the roles and responsibilities as well as accountabilities of the PM&C and SIT are clear in the event of a breach impacting the SIT or CMS, the steps that they will take in the event of a suspected breach, and how and when to notify the OAIC and impacted individuals as well as any other relevant parties together with any remediation solutions that may be made available to affected individuals. A breach simulation exercise to test the plan should be undertaken, and templates developed for communicating incidents and data breach notifications.

7.11.7 October 2021 Review

7.11.7.1 Roles & responsibilities relating to information management and security

Roles and responsibilities in relation to privacy and data breaches are articulated in the Privacy Policy and the FINAL Data Breach Response Plan document. The SIT team also receive training which covers notifiable data breaches and how to respond if a breach is suspected.

Other responsibilities and escalation paths are outline in relevant documents as relates to the particular process or request. For example, the PWSS Procedures_Workplace Review for Case Coordinators document articulates the steps to follow when preparing a case to be disclosed to a workplace reviewer including the role the head of the PWSS will play in reviewing the report from a workplace review.

Other documents, including the MoU with Finance and the Contracts in place with Workplace Reviewers, articulate the roles of each party and broader governance arrangements in relation to cases and workplace reviews. The PWSS Procedures_Release of Information (Incl WHS risk) also cover steps and decision

making criteria for when information is to be disclosed without consent, and who should be notified in such scenarios.

Finally, documentation including the FINAL Record keeping procedure and the FINAL Handling personal and sensitive information documents articulate the importance of good information management, and the expectations and required steps to follow, to guide SIT staff on their responsibilities as well as how they can seek support.

7.11.7.2 Information access management

The PWSS has agreed an onboarding and offboarding process with DP&C (as the IT provider) in relation to access to systems and information. Role-based access is provided on the basis of specifically configured role profiles and it is a requirement that Workforce Reviewers and SIT staff have at least NV1 security clearance. If a member of staff leaves the team or firm their access will be revoked. An exit checklist has been developed which staff must follow when leaving the team.

Workforce Reviewers will be provided a laptop with access to PWSS systems and must conduct their work using this device. It is prohibited for information to be transferred from the PWSS device without PWSS approval.

As previously mentioned in the PIA, monthly access reports will be provided on a monthly basis from DP&C IT to PWSS. These reports will highlight who accessed SIT team files, including client cases in the CMS. Any unusual activity will be flagged and investigated.

7.11.7.3 Consultancy contracts and arrangements

Consultancy contracts have been drafted which must be signed by a Workplace Reviewer prior to them engaging in any work on behalf of PWSS. Contracts include sections related to expected conduct, applicable standards & performance measures, and notifiable data breaches.

Workforce reviewers must also sign a deed of confidentiality. This deed defines personal and confidential information and includes restrictions on use and disclosures, disclosures required by law and privacy expectations.

Workforce Reviewers must undergo privacy and security training before they can access any PWSS data or systems. This covers similar topics to the SIT team training and makes the Workforce Reviewers aware of their obligations of privacy when handling SIT cases, as well as relevant policies and guidance documents.

AS mentioned under information access, Workforce Reviewers will also work from a PWSS device with direct access to the PWSS system and must have a minimum of NV1 security clearance.

7.11.7.4 Secure file transfer

Since the August review it has been determined that workplace reviewers will carry out their work from a PWSS device. As a result, there is no longer a requirement for a secure file transfer mechanism to send case files for workforce review.

7.11.7.5 Security risk assessment

The DP&C IT security team, as thew IT provider, conducted an IT security risk assessment on the CMS prior to the system going live. The risk assessment methodology aligns with the controls defined under the Australian Cyber Security Centre (ACSC) Information Security Manual (ISM). The risk assessment found that the system complied with all required ISM control elements. 2 key risks were flagged.

1. As all personal information in the system can be considered sensitive it carries a heighted level of intrinsic risk and therefore any unauthorised access or use, or any errors, misconfigurations or unauthorised disclosures, could result in reputational damage to PM&C and PWSS. This risk has been mitigated through several controls in place, such as those mentioned above related to access management, onboarding, the requirement for NV1 security, and further technical controls.
2. There is a risk of system unavailability as the system is hosted in the cloud. If the cloud becomes non-operational then the CMS will not be functional until the cloud is restored. This has been mitigated through the use of multiple hosting environments and backups. The system has also not been assessed as 'essential' meaning it is not critical to PWSS operations and Case coordinators can rely on intake forms until the system is back online. DP&C also note that their experience of system outages with Microsoft indicates a quick resolution time and that agreements are in place with reasonable downtime thresholds.

Both risks have been assessed as low with a recommendation to accept.

7.11.7.6 Data breach response plan

A data breach response plan has been drafted. The plan outlines the steps that SIT staff must follow if an actual or suspected breach has occurred, expected timelines/deadlines for action to commence, who will carry out and be responsible for each step in the process, and includes a template to support the reporting of a breach to the Privacy Officer. The document also defines what a notifiable breach is and

provides a helpful table to support the SIT team in understanding whether a use or disclosure of personal information was authorised or not. The document follows the OAIC structure of containing, assessing, notifying and reviewing the breach. Finally, the document references the PWSS Records Management policies and processes to highlight how a breach interacts with the PWSS's obligations to make and retain records of its activities.

The SIT Case Coordinators and Workforce Reviewers must also undergo privacy and breach response training during onboarding and on an annual basis.

7.11.7.7 Reassessment of risk ratings:

Risk 9: This risk has been updated to very low to reflect the level of governance and oversight in relation to the individuals who have access to personal information in the CMS.

Risk rating: Very low

Risk 10: There is currently a retention freeze meaning the OPWSS must retain all records until further notice. This risk has therefore not been addressed and will be reviewed at a later time.

Risk rating: Low

Risk 11: This risk has been updated to medium to reflect that Workforce Reviewers will now be provided a PWSS device so that personal information will be under control of PWSS at all times, as well as other controls including updated contracts, training, deeds of confidentiality, and the various SIT operating policies and procedures which Workforce Reviewers will be expected to comply with. AS Workforce Reviewers are still external staff, there exists a level of intrinsic risk that information can be exfiltrated, such as through taking pictures of the screen or having conversations about the individuals involved in cases. PWSS will also not have control over the working environment of Workforce Reviewers and, due to the Covid-19 pandemic, there is an increased likelihood that Workforce Reviewers will work from home where other members of the household might be present. As such, given the nature and sensitivity of the information Workforce Reviewers will have access to, this rating has been revised to medium.

Risk rating: Medium

Risk 12: This risk has been revised to a low rating to reflect that a data breach response plan has been developed and implemented and that sufficient training is provided to both SIT Case Coordinators and Workforce Reviewers.

Risk rating: Low

7.11.7.8 Updated recommendations:

11.1 This recommendation has been marked as complete

11.2 This recommendation has been marked as still effective. It is recommended that the PWSS ensure that governance requirements are outlined for user access reviews (i.e. require SIT Manager to action/validate user listing with PM&C support team within 48 hours, etc.).

11.3 This recommendation has been marked as complete on the basis that all Workforce Reviewers must demonstrate they have NV1 clearance at a minimum

11.4 This recommendation has been marked as complete on the basis that Workforce Reviewers will be provided a secured PWSS device and so information will no longer need to be transferred outside the PWSS environment.

11.5 This recommendation has been marked as still effective on the basis that there is an information retention freeze in place until further notice

11.6 This recommendation has been marked as complete

11.7 This recommendation has been marked as still effective on the basis that a simulation exercise has not been planned to take place. A breach simulation exercise to test the plan should be undertaken in the next 6 months, and templates developed for communicating incidents and data breach notifications.

7.12 APP 12: Access to personal information

The Freedom of Information Act will not apply to the SIT. Therefore APP 12.2 will not apply to authorise it to release or refuse to release personal information.

We understand that an administrative release process will be developed.

APP 12.1 provides individuals with the right to access their personal information on requests.

Individuals may request to access their personal information that the SIT holds about them or to receive copies of it by contacting a SIT case co-ordinator. Individuals may

also send a request or complaint to the nominated person using the contact information provided in the draft Privacy Policy.

Where an individual who has lodged their case anonymously seeks to access their personal information, the SIT will validate their identity by requesting their case identifier. In the event that they do not have a case identifier, facts about the case may be used to validate a person's identity.

Where information relates to an ongoing complaint, it may not be possible to access or receive copies of any information until the dispute is resolved in order to ensure individuals do not attempt to use privacy processes as a tool to understand what is being reported or otherwise said about them.

7.12.1 APP12 Risk Ratings

Risk 13

Where guidance on the exceptions for providing access to a complainant's personal information are not adequately documented and communicated, there is a risk that information may be shared that could for example compromise another individual's privacy.

Risk rating: Medium

7.12.2 APP12 Recommendations

12.1 A procedure for dealing with access requests should be developed including having regard to the recommendations in APP 2 in relation to use of case or individual IDs.

12.2 Guidance on what exceptions that may apply to the release of any personal information should be developed, given the sensitivity of the information and the status of a case. SIT case workers should be able to explain the access process and determine if any information needs to be withheld or redacted to ensure the privacy of other individuals is not impacted.

7.12.3 October 2021 Review

The PWSS has drafted its Administrative Access Policy which is available under the resources section of the PWSS website. This policy outlines the individual's right to access and request copies of their personal information, including copies of documents where relevant. The policy also outlines the required steps to submit a request, the

expected timeframe to respond to such requests, and what an individual can expect if their request is granted or refused. The policy also provides contact information for further queries, feedback, or complaints.

Guidance for the SIT team on what an individual may request is provided under the PWSS Privacy Policy, the PWSS Procedures_Release of Information (Incl WHS risk), and the training provided to SIT Case Coordinators and Workforce Reviewers

7.12.3.1 Updated Risk Ratings:

Risk 13: The rating has been revised to low, to reflect that a policy and procedure is now in place which allows individuals to access their personal information in accordance with APP12.

Risk rating: Low

7.12.3.2 Updated recommendations:

12.1 This recommendation has been marked as complete

12.2 This recommendation has been marked as complete

7.13 APP 13: Correction of personal information

Individuals may ask for their personal information to be corrected by contacting a SIT Case co-ordinator. Individuals may also send make a request by using the contact details in the draft Privacy Policy.

Care should be taken to ensure correction requests do not interfere with or cause any facts and evidence to be amended during an investigation.

7.13.1 APP13 Risk Ratings

Risk 14

There is a risk that individuals may attempt to amend their information in order to influence an investigation, or that SIT staff may not understand the SIT's APP 13 obligations and how to manage correction requests.
Risk rating: Low

7.13.2 APP 13 Recommendations

13.1 Ensure a documented process and policy is available to staff in relation to the correction of records and that it is communicated to individuals to ensure that requests to amend statements or evidence are managed appropriately particularly during a review.

7.13.3 October 2021 Review

Guidance on what can be requested by individuals in relation to their personal information, including making amendments to their personal information, is available under the PWSS Privacy Policy, PWSS Procedures_Release of Information (Incl WHS risk), and the training provided to SIT Case Coordinators and Workforce Reviewers. The FINAL Records keep procedure also advises Case Coordinators on how to update records in order to ensure the SIT can comply with both privacy and records keeping obligations.

7.13.3.1 Reassessment of risk ratings:

Risk 14: This risk has been updated to very low to reflect the updated guidance and training provided to Case Coordinators.

Risk rating: Very low

7.13.3.2 Updated Recommendations:

13.1 This recommendation is marked as complete

8 Appendices

8.1 Appendix 1 – Stakeholders consulted

Name	Position/Department
Emily Arnberg	Director, Privacy PM&C
Samantha Jorgensen	Director, SSAD Team PM&C
Samantha Portelli	Director, ICT Procurement PM&C
Jackie Paul	Director, PM&C
Clare Sharp	Assistant Secretary, PM&C
Erin Murray	Senior Advisor, PM&C
Ryan Erlandsen	Project Lead, PM&C
Roberto Imbriano	Solution Architect, PM&C
Scott Goldsworthy	IT Security Advisor, PM&C
Glen Simpson	Records Management, PM&C
Alecia O'Toole	Records Management, PM&C
Michele Thompson	Records Management, PM&C
Victoria Blakeley	Parliament House Procedures Review, PM&C
Nechama Basserabie	Subject Matter Expert – Foster Review
Elodie Oxenham	SIT Case Co-Ordinator

8.2 Appendix 2 – Materials received

1. 210719 Website Content
2. 210802 SIT Draft Privacy Policy
3. 210802 SIT Draft Privacy Collection Notice
4. Commonwealth Contract for Consultancy Services
5. Data Breach Response Plan Assessment Template (Final – March 2021)

6. Data Privacy Breach Response Plan – One-Page Flow Chart
7. ICT Security and Human Resources Services Schedule (v1.0 as at December 2019)
8. ISB Request Form – February 2021
9. ITAB Terms of Reference – February 2021
10. Memorandum of Understanding between the Department of Prime Minister and Cabinet and The Australian Public Service Commission – Head Agreement (v1.0 as at 19 December 2019).
11. Memorandum of Understanding for the Independent Complaints Mechanism and Handling of Complaints and Reports Concerning Parliamentary Workplaces.
12. Overview of SIT Processes (DRAFT) 030821
13. PIA CRM - 17 February 2021
14. Review of the Parliamentary Workplace: Responding to Serious Incidents.
15. PMC Information Management Policy
16. PMC Retention and Destruction of Original Records
17. PMC Risk Management Policy and Framework
18. PMC Data Breach Response Plan
19. Privacy Fact Sheet – Working with Personal Information
20. Privacy Management Plan (2021) – Final
21. RE_Case management system – procurement [SEC=OFFICIAL]
22. SIT Case Management Design Document V0.1
23. SIT Came Management Design.vsdx
24. SIT Case Management Product Requirements Document V0.1
25. SIT CMS Access Request Form (wording) – Privacy edits
26. SIT CMS Access Request Form
27. SIT CMS Specs (002)
28. SIT CMS Welcome Screen (wording) – Privacy edits
29. SIT Project Technical Setup

8.3 Documents reviewed in October follow-up:

30. PWSS Procedures_Referrals and Intake
31. 210917 PWSS Procedures_Release of Information (incl whs risk)
32. 3. PWSS Procedures_Workplace Review for case coordinators
33. Deed of confidentiality - M Manthorpe
34. FINAL Data Breach Response Plan (VB edits re contractors)
35. FINAL Handling personal and sensitive information
36. FINAL NAP Policy
37. FINAL Record keeping procedure
38. FINAL Records factsheet
39. MOU with Finance - signed - 23.09.2021_final
40. PSC PWSS CCS Contract - Michael Manthorpe
41. PWSS Protocols_Case Notes
42. PWSS Staff Exit Notification Form_Template
43. PWSS Templates_Intake Form with Prompts
44. Short Form SRA - Serious Incident Case Management System
45. SIT CMS - User Guide v1.1
46. PWSS Privacy Policy
47. PWSS Privacy Collection Notices
48. PWSS Administrative Access Policy

8.4 Appendix 3 – Updated Risk Assessment Table

Risk	Initial Risk Rating	KPMG Risk Commentary	Updated Risk Rating
Risk 1 If the relevant policies and procedures are not adequately defined and documented before the SIT and CMS become operational, and if a Privacy Officer is not nominated, there is a risk that personal information will not be managed in accordance with the APPs and SIT staff may not be sufficiently aware of their responsibilities under the APPs.	**High**	The risk rating has been reassesed to reflect that significant work done to develop the policies that relate to the personal information handling at PWSS by the SIT team and the appointment of a Privacy Officer.	**Low**
Risk 2 If information-recording protocols are not adequately defined for cases in which an individual wishes to remain anonymous, there is a risk that Case Co-ordinators could unwittingly record information that identifies an individual.	**Medium**	Anonymity procedures have been well considered, designed, and implemented. These are sufficiently communicated at several points during an interaction between the SIT team and an individual. This risk rating has therefore been reassessed.	**Low**
Risk 3 It may not be clear how individuals can request access to information, or what information is necessary to collect in order to provide such access. This is especially relevant in cases where individuals chose to remain anonymous.	**Low**	Procedures have been put in place to ensure individuals can remain anonymous but still access their information. The use of a passcode and a pseudonym means an individual may continue to interact with the SIT team in a secure manner and that the SIT team can be assured they are speaking with the same individual. This also ensures individuals can be verified for the purposes of information access requests without compromising their anonymity.	**Very low**

Risk	Initial Risk Rating	KPMG Risk Commentary	Updated Risk Rating
Risk 4 If the SIT does not obtain valid consent, particularly to collect sensitive information, there is a risk that it will breach APP 3. Further, there is also a risk that consent may not be adequately captured where an individual was referred to the SIT, or where consent was implied or gathered orally.	**Medium**	The risk rating has been reassessed given the amount of notice information and guidance that has been developed since the initial assessment. While there is still a risk that consent could be contested based on the language of the intake form, this risk is low given it is based on the discussions that will take place between the SIT team and individuals and that the intent of the form is to act as a temporary document for the information to be later transferred into the electronic CMS with the appropriate consents chosen in the system. That said, it is recommended that the language on the intake form is updated to avoid any doubt.	**Low**
Risk 5 If professional judgement is incorrectly or inconsistently applied, there is a risk that unsolicited personal information could be recorded on an individual's case record.	**Low**	The risk remains low as the PWSS has developed several documents, including training, procedures, forms and policies, to ensure SIT staff are aware of the risks of unsolicited information and how to manage it.	**Low**
Risk 6 Collection notices are not finalised at the time of writing this PIA. If a privacy collection notice is not used when personal information is being collected, there is a risk that individuals contacting the SIT are not adequately aware of the matters referred to under APP 5 (please see above). If this occurs, it may result in the SIT being in breach of their duty to take reasonable steps to make people aware of these matters. The detailed web guidance drafted by the SIT helps to mitigate this risk as well as the general approach the Case co-ordinators will adopt, which involves always informing the individual and seeking consent to continue.	**Medium**	The risk rating has been reassessed given the adequate collection notices that are available online, and the procedures, forms, policies and training all encourage and support Case Coordinators to provide notice and collect valid consent which requires adequate notice. It is also understood that the need for further or enhanced notices will be under constant review, and will be revisited during the 6- & 12-month follow-ups to this PIA by the Privacy Officer.	**Low**

Risk	Initial Risk Rating	KPMG Risk Commentary	Updated Risk Rating
Risk 7 Disclosure of information may not be consistent with APP 6 if consent has not been obtained. As such, an individual may not understand that their information being disclosed to a Reviewer if they wish to progress their case to a workplace review. Their consent in this instance should therefore be explicit and not implied. It will not be necessary to seek consent where the Case Co-ordinator reasonably believes a person is in immediate risk of serious harm, however such incidents should involve a validation process with a trained supervisor or other adequately experienced employee where possible. We understand that where a call is received out of hours, that this may not be possible and the Case Co-ordinator should, therefore, rely on their professional judgement in the situation (i.e. prioritising the wellbeing of the individual at risk).	**Low** to **Medium**	This risk has been confirmed as a low rating to reflect that considerable work has been done by PWSS to document procedures, guidelines and expectations. Notices clearly articulate to individuals how their personal information will be used and disclosed, and various arrangements are in place to govern this, including MoUs and contracts with Workplace Reviewers.	**Low**
Risk 8 If there is a lack of consistency in the way free-text fields are used, this could result in inconsistencies in the quality of information recorded against different case records. This could impact the effectiveness and the outcome of a workplace review.	**Low**	This rating has been reassessed to reflect the additional fields in the CMS and the range of targeted guidance and training which reduce the likelihood of errors or inconsistencies in data entry.	**Very Low**
Risk 9 If there is a lack of appropriate governance over user access reviews, there is a risk that necessary user account terminations may not be completed in a timely manner. This could result in unauthorised access to, and use of, personal information held in the CMS.	**Low**	This risk has been reassessed to reflect the level of governance and oversight in relation to the individuals who have access to personal information in the CMS.	**Very Low**

Risk	Initial Risk Rating	KPMG Risk Commentary	Updated Risk Rating
Risk 10 There is a risk that case records could be retained for longer than the permitted period if requirements are not formally defined.	**Low**	There is currently a retention freeze meaning the OPWSS must retain all records until further notice. This risk will therefore be reviewed at a later time.	**Low**
Risk 11 Given that Reviewers will be individuals who will not be working from a secured enterprise work environment and will be using their own devices to conduct reviews and may be collecting and sharing information via unsecured third-party systems, there is an increased risk that a complainant's personal information may be stored insecurely or exposed to a data breach.	**Very High**	This risk rating has been reasessed to medium to reflect that Workforce Reviewers will now be provided a PWSS device so that personal information will remain under the control of PWSS, and other controls implemented including updated contracts, training, deeds of confidentiality, and the various SIT operating policies and procedures which Workforce Reviewers will be expected to comply with. As Workforce Reviewers are not staff, there will continue to be a level of intrinsic risk to the security of the information they can access. PWSS will also not have control over the working environment of Workforce Reviewers and, due to the Covid-19 pandemic, there is an increased likelihood that Workforce Reviewers will work from home where other members of the household might be present.	**Medium**
Risk 12 There is a risk that data breach incidents may not be appropriately handled and reported (where relevant) if a response plan is not formally documented and communicated. This could result in negative consequences for the SIT and other relevant parties, including reputational damage, fines, and harms to individuals.	**High**	This risk rating has been reassessed to reflect that a data breach response plan has been developed and implemented and that sufficient training is provided to both SIT Case Coordinators and Workforce Reviewers.	**Low**

Risk	Initial Risk Rating	KPMG Risk Commentary	Updated Risk Rating
Risk 13 Where guidance on the exceptions for providing access to a complainant's personal information are not adequately documented and communicated, there is a risk that information may be shared that could for example compromise another individual's privacy.	**Medium**	This risk rating has been reassessed to reflect that a policy and procedure is now in place which allows individuals to access their personal information in accordance with APP12.	**Low**
Risk 14 There is a risk that individuals may attempt to amend their information in order to influence an investigation, or that SIT staff may not understand the SIT's APP 13 obligations and how to manage correction requests.	**Low**	This risk has been reassessed to reflect the updated guidance and training provided to Case Coordinators.	**Very Low**
Risk 15 Further privacy risks that may arise as the SIT begins operating and takes on cases are not documented and addressed.	**Medium**	This risk rating has been reassessed to reflect that the Privacy Officer has been appointed and has committed to reviewing the PIA at 6- & 12- month intervals to assess whether any other privacy risks arise through the course of operating the service that have not been proactively identified at the time of this PIA. The rating also represents effort taken to reduce the risks assessed by the PIA through the implementation of various policies and processes.	**Low**

8.5 Appendix 4 – Table of Recommendations

Ref	August 2021 Description	Priority	Current Status & Commentary
1.1	Finalise and publish the SIT Privacy Policy.	High	Complete
1.2	Confirm who the nominated Privacy Officer will be.	Medium	Complete
1.3	Revisit and update this Report in 6 and 12 months to ensure any additional privacy risks are assessed and documented and steps implemented to address them.	Medium	Still effective
2.1	Ensure collection notices make clear that an individual may remain anonymous	Medium	Complete
2.2	Give Case co-ordinators documented guidance detailing the protocols for recording information and progressing anonymous complaints.	Medium	Complete
2.3	Define a process for providing access to personal information where an individual chooses to remain anonymous, or has used a pseudonym.	Low	Complete
3.1	Consider the process and basis for collection of an individual's personal information from third parties.	Medium	Complete
3.2	Ensure that in each case where consent is collected the consent is valid.	High	This recommendation is marked as still effective on the basis of the consent language in the intake form only. It is recommended that the consent box language be updated so that, instead of suggesting it is a tick box to confirm that conversations about consent took place, it captures consent for the individual's personal information to be collected for the purposes of creating and managing a case.
4.1	Develop guidance for staff that outlines how to handle unsolicited information.	Low	Complete
5.1	Various formats of collection notices should be developed and used where appropriate.	High	This recommendation is still effective on the basis that the Privacy Officer has committed to continue to review and update notices on an as-needs basis, and to review during the 6- & 12-month PIA follow-up reviews.
6.1	Ensure that affected individuals are made aware of the circumstances in which their information may be disclosed.	Medium	Complete

Ref	August 2021 Description	Priority	Current Status & Commentary
6.2	Ensure the process for disclosing information of a complainant for independent review includes obtaining explicit consent.	High	Complete
6.3	Ensure that any incident which may result in the SIT using or disclosing personal information to lessen or prevent a risk of serious harm involves an escalation or validation step where possible and reasonable.	Medium	Complete
10.1	Reasonable steps should be taken to maintain the integrity of the data in the CMS given its particularly sensitive nature.	High	Complete
10.2	Develop guidelines that Case Co-ordinators should follow when recording personal and/or sensitive information in any free-text fields.	Low	Complete
11.1	Ensure that PM&C and SIT staff are adequately aware of their respective roles and responsibilities in relation to information security.	High	Complete
11.2	Ensure that governance requirements are outlined for user access reviews (i.e. require SIT Manager to action/validate user listing with PM&C support team within 48 hours, etc.).	Medium	This recommendation has been marked as still effective. It is recommended that the PWSS ensure that governance requirements are outlined for user access reviews (i.e. require SIT Manager to action/validate user listing with PM&C support team within 48 hours, etc.).
11.3	Ensure that Reviewers are subject to appropriate risk assessment before they are engaged under the Commonwealth contract for consultancy services.	Very High	This recommendation has been marked as complete on the basis that all Workforce Reviewers must demonstrate they have NV1 clearance at a minimum
11.4	Ensure that controls are in place to protect personal information that is transferred to or accessed by third parties, including Reviewers, such as mechanisms to share and access information via a secure file transfer or by granting access to a secure folder on PM&C systems that limits downloads and any protocols to manage further disclosures by them and the return of information.	Very High	This recommendation has been marked as complete on the basis that Workforce Reviewers will be provided a secured PWSS device and so information will no longer need to be transferred outside the PWSS environment.

Ref	August 2021 Description	Priority	Current Status & Commentary
11.5	Conduct a review of case record retention requirements and formally define them.	Medium	This recommendation has been marked as still effective on the basis that there is an information retention freeze in place until further notice
11.6	PM&C ICT staff should carry out a security risk assessment prior to the system going live.	High	Complete
11.7	Develop a SIT-specific data breach response plan which covers incidents that could be caused by staff and Reviewers.	High	This recommendation has been marked as still effective on the basis that a simulation exercise has not been planned to take place. A breach simulation exercise to test the plan should be undertaken within the next 6 months, and templates developed for communicating incidents and data breach notifications.
12.1	Develop a procedure for dealing with access requests.	Medium	Complete
12.2	Develop guidance on what exceptions may apply to the release of any personal information	Medium	Complete
13.1	Ensure a procedure to correct records developed and communicated to staff.	Medium	Complete