Use and Governance of Artificial Intelligence Systems by Australian Public Sector Entities

Name of department/agency: **Department of the Prime Minister and Cabinet (PM&C)**

Questions

1. **For what purposes do you currently use AI in your entity, and do you have planned or likely future uses? Please summarise.**

   PM&C uses AI tools and services for Proof of Concept/Trial purposes. With the fast-paced evolution and growing need for AI solutions, PM&C will continue to reassess and evolve its position in line with the Digital Transformation Agency's (DTA) guidance as the lead agency.

2. **Which legislative, regulatory and policy frameworks (including cross-Government policies) are relevant to your entity's use of AI?**

   PM&C will continue to follow DTA's, Department of Industry, Science and Resources (Industry) and Australian Cyber Security Centre (ACSC) interim guidance on the relevant use of AI and also adhere to National Archives of Australia (NAA) on managing information and data for government.

3. **That are your internal framework/policies for assessing the risks associated with the use of emerging technologies such as AI, specifically in the areas of security, privacy, ethics, bias, discrimination, transparency and accountability?**

   PM&C has established governance forums to assess risks associated with adoption of emerging technologies such as AI. These forums evaluate the use of technologies under various guidance and guardrails provided by government agencies such as DTA, Industry and ACSC.

4. **What are the supply chain risks when using existing AI solutions or software?**

   Following are some of the supply chain risks that may require consideration when utilising AI solutions:

   1. Third-Party Vulnerabilities: AI solutions often involve third-party providers whose security measures might not be as robust, increasing the risk of data breaches.
   2. Data Privacy and Compliance: There is a risk that third-party vendors may not adhere to strict data privacy and compliance regulations, potentially leading to data misuse or violations of laws such as GDPR or the *Privacy Act 1988.*
   3. Ethical and Bias Concerns: Pre-existing biases in third-party AI algorithms can lead to discriminatory outcomes, which can damage reputation and lead to legal challenges. Vendors may not fully disclose how their AI algorithms function, making it difficult to assess and mitigate biases or ensure ethical use.

5. **What additional controls have been developed by your entity to manage:**
   a. **the broad risks associated with AI:**
   Conduct thorough due diligence on third-party vendors to assess their security practices, compliance with regulations, and overall reliability. This is done through established governance forums and security assessments.
   b. **the risks associated with the design and implementation of systems using AI:**
   PM&C does a thorough analysis of risks associated with the adoption of emerging technologies such as AI through its established governance forums in consultation with our cybersecurity team. The department does not have any bespoke AI applications and does not undertake any design or development of AI.
   c. **the risks associated with change management policies that arise from the use of AI:**
   Any updates to change management policies is through consultation with the broader ICT delivery teams and through relevant forums.

6. **How do you manage regular updates to AI and supporting data?**

PM&C uses commercial off the shelf AI Services provided by third party vendors, such as ChatGPT. Updates to such commercial AI offerings and supporting data is sole responsibility of the vendor including adherence to WoAG policies and framework.

7. **What considerations or planning do you undertake for any additional capability required to implement AI?**

At PM&C, we undertake thorough considerations and strategic planning when evaluating the need for additional capability. This includes conducting comprehensive requirement and risk assessment, compliance considerations, and potential disruptions to existing operations.

8. **What frameworks have you established to manage bias and discrimination in any of your systems that use AI?**

PM&C adheres to the framework established by departments such as DTA, Home Affairs, and Industry.

9. **How do you ensure that that the use of AI meets government security and privacy requirements?**

To ensure that the use of AI meets government security and privacy requirements, PM&C undertakes the following steps:

a. Adherence to Government Standards and Regulations:
   - Following guidelines from DTA and ACSC to comply with relevant Australian laws and regulations, including the *Privacy Act 1988*, the Australian Government Information Security Manual (ISM), and the Protective Security Policy Framework (PSPF).

b. Access Controls:
   - We have implemented strict access control mechanisms to ensure that only authorised personnel can access AI systems.

c. Staff Training and awareness:
    - Conduct trainings and awareness sessions to keep all stakeholders informed about the importance of security and privacy in AI systems.

d. Monitoring and Logging:
    - Have guidelines for the user to log the use of AI systems to detect and monitor on ad hoc need basis.

e. Third Party Vendor engagement:
    - Due Diligence: Perform thorough due diligence on vendors and third-party providers to ensure they adhere to government security and privacy standards.
    - Contracts and SLAs: Include stringent security and privacy clauses in contracts and Service Level Agreements (SLAs) with third-party vendors.

10. What briefings are given to your audit and risk committees, or boards, on the use of AI?

PM&C provides regular briefings to key departmental governance committees when required.

11. How does your internal audit program consider the robustness of controls for AI to provide assurance around mitigation or risks?

PM&C has a risk-based internal audit work program that provides assurance on the department's financial, operation and IT controls. The 2024-25 Internal Audit Work Program is currently being developed, and will consider the merits of including an audit topic on AI in the context of PM&C's overall risk profile.

12. As part of your system design process, how do you audit and trace the output of, and decisions made through AI?

As per DTA interim guidance, PM&C business areas approved to test AI services are encouraged to keep a register of their AI use.

13. Are the AI platforms in use at your entity:

Yes

14. Who has ownership and possession of the source code for your AI, and can you understand this code, including its capacity to learn and innovate? How?

PM&C does not develop bespoke AI applications.