Use and Governance of Artificial Intelligence Systems by Australian Public Sector Entities
Name of department/agency: **Commonwealth Superannuation Corporation (CSC)**

Questions

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

Currently CSC is employing basic functionalities of AI. This includes the initial implementation and utilisation of CoPilot for Microsoft 365. For example, CSC has signed up for Digital Transformation Agency (DTA) Copilot for Microsoft 365 trial. The Copilot trial is conducted in control environment where business use cases are selected carefully to mitigate any data risk. At present CSC has less than 50 users in the trial group.

CSC has identified an initial set of AI business use cases that can be beneficial for CSC operations. This work is in progress as part of the MS 365 Copilot trial. By exploring these use cases, CSC is planning to leverage Copilot to streamline existing business processes and accelerate innovation within the teams in a more control manner. Refer to Copilot trial business use case list for more details.

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

CSC's internal policies including CSC Code of Conduct, Data Privacy, Data Management Policy, Information Security Management, IT Security, ICT Architecture Governance Policy, and Acceptable Use of ICT Policy are comprehensive and designed to cover a wide range of technological applications including artificial intelligence. Our overarching policies are designed to remain flexible and adaptable to emerging technologies including AI. While a specialised AI Policy may be considered in the future, we believe that our current framework provides a strong foundation.

CSC has developed an AI guideline document which provides a comprehensive set of principles including best practices for deployment and use of AI technologies. This document serves several key purposes such as risk mitigation, regulatory compliance, innovation, education, and awareness.

CSC as an Australian Prudential Regulation Authority (APRA) regulated entity, must comply with Prudential Standard CPS 234 which requires CSC to assess risks related to AI adoption, considering security controls, vulnerabilities, and threats.

3. What 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?

Policies:

CSC Code of Conduct, Data Privacy, Data Management Policy, Information Security Management policy framework, IT Security Policy, ICT Architecture Governance Policy, and Acceptable Use of ICT Policy.

CSC supports and encourages a diverse and inclusive workforce by fostering a culture and environment of equity, respect, courtesy, honesty and integrity. These requirements are captured in the CSC Diversity and Inclusion Policy.

Other relevant documentation:

- *CSC AI Intelligence Definitions and Guideline Document*
- *CSC AI intelligence Definition and Guideline all staff training pack*
- *Technology AI working group Terms of Reference*
- *CSC Intranet AI Page extract accessible for all staff.*

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

At this stage CSC does not rely on AI tools to deliver critical operations.

Note- Currently CSC is employing basic functionalities of AI. This includes the initial implementation and utilisation of CoPilot for Microsoft 365. Similar to other third-party tools, there is always an element of supply chain risk. However, CSC mitigates this risk by implementing a supply chain risk management process aligned with APRA CPS 234 standards.

5. What additional controls been developed by your entity to manage:
   a. the broad risks associated with AI

CSC standard process involves conducting appropriate due diligence prior to onboarding any technology applications (including third party applications). The degree of due diligence is commensurate with the level of risk, the operations it supports and the third-party relationship. The same controls applicable to AI tools. In addition, current AI usage via web browsers is subject to additional controls, such as proxies and firewalls.

   b. the risks associated with the design and implementation of systems using AI

The current Co-Pilot trial aligns with CSC's existing identity architecture and has undergone assessment by the architecture governance board.

   c. the risks associated with change management policies that arise from the use of AI

Only limited use of AI, refer to response at question 3.

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

Copilot is in use in a controlled environment. CSC also have clear data ownership and stewardship roles defined to maintain accountability for data integrity, privacy, and security. Appropriate control measures, including encryption, access control, intrusion detection etc. implemented to mitigate the risk of unauthorised access and breaches.

Staff awareness training was provided prior to granting access to Copilot to educate users around effectively mitigating privacy breaches and data sprawl to safeguard data.

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

CSC has encouraged an open dialogue regarding the use of the AI tools and potential risks and mitigation strategies. Working groups (Technology level and Enterprise level) have been established to discuss legitimate use cases or suggestion on how to responsibly intergrade such technologies into our processes, security features that we should enable etc. This Working Group also facilitates collaboration between different departments ensuring that AI initiative are integrated.

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

CSC utilises AI in a limited and controlled manner. The AI Working Group serves as a committee with oversight responsibilities for ensuring compliance and control in the use of AI within CSC.

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

CSC comply APRA CPS 234 (information Security) and government specific requirements such as Information Security Manual (ISM) to ensure any AI tools meets the required security controls and protocols.

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

Cyber Security is a standing agenda item for every Risk Committee meeting and within this agenda item, the use of AI may feature. The Board received a biannual 'Digital and IT Update' which includes updates on cyber security, digital opportunities and threats etc and may include reporting on AI.

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

Due to the limited usage within CSC, the AI systems, including Microsoft Copilot, is not subject to the current audit plan.

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

Not applicable.

13. Are the AI platforms in use at your entity:
    a) off the shelf products
    b) customised from other products
    c) systems developed in-house?

Off the shelf products.

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?

Not applicable.