Australian Government

Services Australia

Services Australia submission to the Joint Committee of Public Accountants and Audit in response to the request for information to an Inquiry into Commonwealth Financial Statements 2022-23: Use and Governance of Artificial Intelligence Systems in the Australian Public Sector

 7 June 2024

Questions

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

   Services Australia (the Agency) uses Artificial Intelligence (AI), or technology supported by AI to support the delivery of services for our customers and staff.

   For the purposes of this response, the Agency uses the following definition of AI:
   Artificial intelligence refers to an engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation[1].

   The Agency currently uses AI technologies for the following purposes:
   - **Optical Character Recognition (OCR)**: This technology is used to extract data from forms and letters that are received and scanned. Digital content from the form is sent to staff to manually to compare the OCR output to the source document, and make corrections as required.
   - **Interactive Voice Response (IVR)**: IVR technology is used in our call centre environment to help route calls in a smarter way. There is also the use of speech to text capability which can transcribe customer calls.
   - **ChatBots**: Digital Assistants (**DAs**) help to respond to millions of customer enquiries each year and provide customers with key information on how to access government services. Supporting our DAs is an ecosystem of tools such as text analytics tool which gives staff visibility of customer enquiries and enables them to create and adjust content that DAs can use.
   - **Website content editing**: The Agency is trialling a generative AI tool to assess its capability in website content revisions.
   - **Microsoft Copilot for M365**

   The Agency is exploring further ways in which AI can be used ethically in alignment with the Agency's **Interim AI Strategy** and governance processes, with guidance and feedback provided by the Interim Independent Advisory Board, Digital Transformation Agency (DTA), Department of Industry, Science and Resources (DISR), Department of Social Services (DSS), and the Attorney-General's Department (AGD).

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

   The Agency acknowledges and is ensuring alignment with the current cross-Government policies and frameworks:
   - Data and Digital Government Strategy

---

[1] ISO definitions (ISO/IEC 22989:2022) as outlined in the Agency's Interim AI Strategy

- Australia's AI Ethics Framework
- Australian Government Architecture
- NSW Government AI Strategy
- Agency involvement in the AI Taskforce *(led by DTA and DISR)*
- Commonwealth Ombudsman Automated Decision-making Better Practice Guide.

In addition, the Agency continues to ensure compliance with the *Public Governance, Performance and Accountability Act 2013* (and Commonwealth Procurement Rules) when procuring AI technologies. The Agency is also continuing to work closely with other government agencies to ensure alignment with AI policies and frameworks that are under development.

In addition to the above, the Agency's internal policies and frameworks aligned to AI include:
- Interim AI Strategy
- Master Plan
- People Strategy
- Technology Plan
- Automation Operating Model
- Data Trust and Ethics Framework
- Data and Analytics Strategic Plan
- Cyber Security Sub-Strategy, and
- Cloud Strategy.

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?**

   The Agency's interim AI Strategy and associated AI assurance process includes data ethical assurance covering the Agency's **8 Data Trust and Ethics Principles**. These principles span the areas of security, privacy, ethics, bias, discrimination, transparency, and accountability, as well as additional areas including legality and human-centered design.

   A range of processes, artefacts and authorities help assure the Agency against these principles. The questionnaire-based **Data Trust and Ethics Satisfaction Tool (DataTEST)** is available to projects or initiatives using data, including projects or initiatives using AI. A dedicated team administers the DataTEST, and the Agency's **Data Trust and Ethics Committee** is available for escalation.

   We also have the following frameworks and governance mechanisms in place to assist with assessing risks:
   - Automation Operating Model (incorporating Risk Assessment and Design Principles)
   - Data Trust and Ethics Framework
   - Digital Capability and Automation Committee
   - Automation Working Group
   - Portfolio Management Investment Committee.

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

   The Agency's interim AI Strategy and governance process ensure we adhere to the AI Ethics Principle of 'Contestability' when assessing and monitoring all AI systems. To complement this, we review AI systems to identify supply chain risks including:

- Strategic sourcing
- Media disinformation
- Cyber security including phishing and distributed denial of service (DDOS)
- Privacy by design to safeguard against exposure of sensitive data
- Onshore and offshore cloud hosting, and
- A vendor's reliability and safety record.

The Agency is developing a standard clause for inclusion in vendor contracts that may leverage AI technologies. The clause will require vendor compliance with the Agency's AI and related frameworks and require vendors to inform the Agency if an update or new release uses AI technologies.

5. **What additional controls have been developed by your entity to manage:**
   a. the broad risks associated with AI
   b. the risks associated with the design and implementation of systems using AI
   c. the risks associated with change management policies that arise from the use of AI

The Agency has comprehensive and robust governance, assurance, risk, and change management practices, frameworks, and policies in place to manage enterprise risks. As the technology landscape continues to evolve, the Agency's internal governance processes are iteratively refined.

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

The Agency manages its use of AI, including updates to AI and supporting data, in accordance with the Interim AI Strategy.

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

The Agency follows the process set out in the Interim AI Strategy when considering implementing AI technologies.

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

The Agency's Interim AI Strategy sets out the Agency's approach to managing bias and discrimination in the Agency's use of AI.

In addition, the Agency's **Data Trust and Ethics Framework (DTEF)** outlines **eight principles** to enable the Agency to deliver trusted and ethical use of data. These include human-centred design, adherence to relevant legislation and codes of practice, mitigation of bias and discrimination, retaining human oversight and testing reliability. **Australia's Artificial Intelligence Ethics Framework principles** has been used to guide the development and iterative revision of the Agency's data trust and ethics principles. The Data Trust and Ethics Committee is also available for escalation.

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

The Agency ensures all AI systems undergo a privacy, ethics and IRAP assessment prior to use. Systems developed in-house are created and deployed on platforms that have been vetted by cyber-security and comply with government security requirements.

The Agency will continue to mature frameworks that will help us engage responsibly, ethically, and safely with AI.

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

The Agency has been briefed on AI through a range of its internal governance committees and forums including an Executive Committee briefing and endorsement of the Agency's Interim AI strategy that outlines the AI governance process. Executive Committee also received an onsite briefing on AI and emerging technology at the Agency's Technology Innovation Centre. Whilst the Audit and Risk Committee has received briefings on technology more broadly, it has not been specifically briefed on the Agency's use of AI.

The Agency has established an "AI adoption risk" on the enterprise watchlist. This will be revisited regularly to ensure ongoing awareness and compliance with agreed governance and frameworks.

In addition, the Agency is conducting AI Short Courses for all SES staff delivered by world-leading experts at the Australian National University. The courses are designed to uplift AI literacy across the Agency SES and improve AI design and decision making.

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

The Agency's internal audit program helps the Agency to accomplish its objectives by bringing a systemic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes. The Agency's internal audit program has not, to date, specifically considered the robustness of controls for AI to provide assurance around mitigation or risks, noting the Agency's very limited use of AI technologies.

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

The Agency does not use AI to make decisions.

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?

The AI technologies currently in use in the Agency are off the shelf products that are customised / configured to meet Agency requirements.

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?**

To date, developers of the limited AI technologies used in the Agency have retained ownership and possession of the source code.