Joint Committee of Public Accounts and Audit
Inquiry into the use and governance of artificial intelligence systems by public sector entities
ANSWERS TO WRITTEN QUESTIONS ON NOTICE
Commonwealth Scientific and Industrial Research Organisation (CSIRO)
15 November 2024

Questions

1. Does the CSIRO's position as a corporate Commonwealth entity change how it approaches the adoption of AI, in comparison to non-corporate Commonwealth entities? Has the CSIRO made any findings or tried any approaches that could be adopted by other corporate Commonwealth entities?
2. In your submission to this inquiry, you advised that CSIRO has established an internal Responsible AI Working Group.
    a. Is the working group expected to remain in operation after its deliverables have been completed?
    b. Which departmental position chairs the working group? Does it have decision-making authority?
3. Your submission states that the working group is developing a risk assessment process.
    a. Does CSIRO have any views on whether existing frameworks (such as the Commonwealth Risk Management Policy) provide appropriate guidance for corporate Commonwealth entities to refer to?
4. Please provide more information on the work of the National AI Centre before it transitioned to the Department of Industry, Science and Resources on 1 July 2024.
5. In your response to the 14 AI questions, you advised that CSIRO researchers have access to generative AI test beds 'to enable innovation and experimentation with third party tools within a secure environment.'
    a. Please provide more detail on the test beds, including any examples of results from experiments.
    b. What supporting arrangements, such as access controls or policies, are in place to support use of the test beds?

Answers

1. As Australia's national science agency, and consistent with its functions under the *Science and Industry Act* 1949, CSIRO engages with AI in ways that may differ from some corporate and non-corporate Commonwealth entities (CCEs). This requires us to take a tailored approach to managing the use of AI that considers its use in a research context. A tailored approach may be advisable for other CCE's, to ensure management of AI is relevant to each CCE's usage.

CSIRO considers it good practice to align with the DTA's *Policy for the responsible use of AI in government,* even where it is not mandatory for CCEs. CSIRO intends to align our policies and procedures with this policy, while also considering where additional management may be required to suit CSIRO's use of AI in research.

2.

a. CSIRO's internal responsible AI working group is a temporary group responsible for establishing a responsible use of AI procedure, AI risk assessment, and AI governance committee. Following completion of these deliverables, the working group will be dissolved, and the AI governance committee will have ongoing oversight of responsible AI use.

b. CSIRO's Chief Digital Officer chairs the internal responsible AI working group. Once established, the responsible use of AI procedure will define roles and responsibilities for AI governance, including formalising decision-making authority.

3. CSIRO is unable to comment on whether existing government frameworks provide appropriate guidance to other Commonwealth entities.

The Commonwealth Risk Management Policy (CRMP) informs CSIRO's own Risk Management Framework (RMF), which our AI risk assessment tool will be aligned with. The CRMP provides broad guidance and principles for managing risks. It also recommended that 'entities should tailor their risk management arrangements to suit the nature of their operations and the risks they face.'

Considering our use of AI across science and enterprise, CSIRO is developing a tailored AI risk assessment tool that will help our people identify and make informed decisions about the risks specific to our use of AI.

In addition, as outlined in our submission (TOR2), risks to CSIRO technology environments are considered in line with the Protective Security Policy Framework and Hosting Certification Framework, provided by the Department of Home Affairs; and the Information Security Manual, published by Australian Signals Directorate. Whilst this guidance is not specific to AI technology, CSIRO considers that these are still highly relevant and applicable to managing a number of the risks inherent with the use of AI technologies.

4. Before transitioning to the Department of Industry, Science and Resources, the National AI Centre was hosted by CSIRO to help grow an AI industry in Australia and help Australian industry to responsibly adopt AI.

The National AI Centre's activities included engagements with industry through events, focus groups and networks, and the development of advice and frameworks on the use of AI by industry, which it did in close collaboration with CSIRO's Data61.

Examples of these activities include:

- Establishing the Responsible AI Network (RAIN), a world-first cross-ecosystem program to support Australian companies to use and create AI responsibly through events, webinars and publications.
- Delivery of Australia's AI Safety Standard, a single source of guidance, best practice and tools for Australia's AI industry to implement AI safely and responsibly.
- Launching the inaugural Australia AI Month in November/December 2023, with over 70 events delivered nationwide.

5.

a. CSIRO currently provides application programming interface (API) access for research teams to several OpenAI GPT models (GPT3.5 turbo, and GPT 4.0) via the Microsoft Azure cloud. Access is also provided to the Amazon Web Services Bedrock foundational model service, which provides access to additional models from Anthropic, Facebook Llama, and Mistral.

The majority of Generative AI test bed users are researchers who use interactive chatbots for specific research use cases. Other uses include projects that process large amounts of data such as scientific literature or papers, large numbers of source code files, or even images. These use cases are largely explorative and aren't of sufficient maturity to share the results of research.

b. Access to the test beds is managed through CSIRO's cloud accounts and inherits the existing security controls and protections in place for CSIRO's use of cloud accounts. This includes centrally managed access control, monitoring and logging, security alerts, and financial cost controls. Internal guidance on the use of Generative AI has been published, that aligns with the DTA's interim guidance published in 2023. All technology tools, including AI test beds, must be used in accordance with existing CSIRO policies and procedures such as Responsible Use of ICT and Internet Services, Software Acquisition and Management, Record Keeping, Cyber Security, and Privacy.