Public Accounts and Audit

Answers to questions on notice

Agriculture, Fisheries and Forestry Portfolio

Inquiry:	Inquiry into Commonwealth Financial Statements 2022-23: Use and Governance of Artificial Intelligence Systems in the Australian Public Sector
Question No:	Inquiry QoNs 1 - 14
Hearing Date:	n/a
Division/Agency:	Digital Business Division
Hansard Page:	n/a
Question Date:	20 May 2024
Question Type:	Written

Mr Julian Hill MP asked:

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

Answer:

The department's use of AI include:

- Natural language processing to detect specific biosecurity risks from a limited set of imported cargo goods descriptions.
- Natural language processing to analyse Officer free text comments as part of the business quality assurance process.
    - AI techniques in the department's data warehouse are used for business insights. Outputs are not directly applied through software integration to regulatory services; they are provided to inform regulatory officers of any potential biosecurity risk.
    - AI is used to produce land use maps, undertake pattern recognition, preform predictive modelling to characterise farm performance and identify biosecurity risk. Predictive modelling techniques are expected to support commodity forecasting.
    - Microsoft 365 Copilot is being trialled as a productivity tool for a limited number of staff (~300); it acts as a digital assistant by drafting content, finding information on the department's intranet, rewriting content for style and clarity, and summarising Microsoft Teams meetings.
    - Departmental staff, primarily our ICT teams, use Chat GPT periodically to seek answers for consideration to inform ICT technical problems.
    - The department’s responses to this question are based on AI capabilities currently in use. There are, however, some AI initiatives being trialled and tested by the department. These will require review and authorisation prior to deployment, based on current and expected whole-of-government security, privacy, transparency, and accountability frameworks and guidelines.
    - The department's data maturity project will lay the foundations for AI to ensure appropriate gateways are in place for future adoption.
    - The department understands these Questions on Notice to be about generative AI and have responded on this basis.

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

Answer:

- The department has a range of legislative obligations included under the *Privacy Act 1988, Public Service Act 1999, Archives Act 1983, Copyright Act 1968 and Freedom of Information Act 1982* in relation to the way it manages information. These obligations extend to any use of AI by the department.

- The Commonwealth Risk Management Policy, Interim guidance on government use of public generative AI tools (November 2023), Australia's AI Ethics Principles, Adoption of Artificial Intelligence in the Public Sector, Protective Security Policy Framework (PSPF) and Australian Government Information Security Manual (ISM) determine the basis of cybersecurity considerations of all IT systems and software in the department.

- The department has published guidance to staff on Artificial Intelligence on the department's intranet. This guidance also includes links to the Digital Transformation Agency (DTA) and Department of Industry, Science and Resources (DISR) websites for information on Australia's AI Ethics Principles and Adoption of Artificial Intelligence in the Public Sector.

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?***

Answer:

- The department has published guidance to staff on Artificial Intelligence on the department's intranet. This guidance also includes links to the Digital Transformation Agency (DTA) and Department of Industry, Science and Resources (DISR) websites for information on Australia's AI policies, frameworks, and information.

- DAFF's Enterprise Risk Management Framework and Policy are in place to establish robust and fit-for-purpose systems of risk oversight, management, and internal control.

- All systems are assessed using the ICT Risk Management and Authorisation Framework and AI components are given particular attention. This also aligns with our Enterprise Risk Management Framework and Policy.

- The department has a Data Science Guideline, used to align to the Australian Government Architecture AI Ethics Principles.

- The department also follows the Five Safes (security) framework along with other whole-of-government security, privacy, discrimination, transparency and accountability guidelines and practices.

- Our Information Security Policy Management Lifecycle management plan governs our process for determining when updates are needed to policies, frameworks, and standards. These updates may result from new legislation, whole-of-government advice, or guidelines. This means any new government policies, advice, legislation, or guidelines on AI will be incorporated into our DAFF policies and processes on a regular basis.

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

Answer:

- Guidelines on the use of ChatGPT and other generative AI tools are published on the department’s intranet. The Commonwealth Risk Management Policy, Interim guidance on government use of public generative AI tools (November 2023), Australia’s AI Ethics Principles, Adoption of Artificial Intelligence in the Public Sector, Protective Security Policy Framework (PSPF) and Australian Government Information Security Manual (ISM) determine the basis of cybersecurity considerations and guidance of all IT systems and software in the department which includes the development and use of AI.

5. ***What additional controls 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

Answer:

- Our use of AI is limited, and emergent with the application of existing risk assessment controls.

- Augmentation of these controls will identify and isolate specific processes for management of risks and controls – whether adopted from mandated WofG standards or developed internally.

- In the meantime, guidelines for the use of AI exist (noted elsewhere), and declarations are sought for any external use of AI. These guidelines outline the responsibilities to be adhered to, and links to the department's privacy and security policies.

- To remain abreast of whole of government direction on AI and emerging or agreed positions on AI risk and relevant means to address them, the department is:

  - Actively participating as a member of the WofG AI Policy Taskforce for the Australian Government.

  - Actively participating as a member of the WofG Chief Data Officer network.

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

Answer:

- The department defines and applies a Data Science Development Management Life Cycle for bespoke AI products.

- Machine learning models are manually code reviewed by internal teams.

- Microsoft implements updates to Microsoft 365 Copilot, in accordance with their product roadmap.

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

Answer:

- The department has recently (May 24) established a small team focused on AI within its new operating structure to understand the AI context in broader government, opportunities, risks, and governance.
- All departmental staff who have participated in the Microsoft 365 Copilot trial have completed mandatory training on the responsible and appropriate use of AI. Training includes awareness of the risks of bias and hallucinations from generative AI systems.

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

Answer:

- The department's data science blueprint includes a feedback cycle, random, unbiased validation, and well-defined machine learning guidelines.
- All departmental staff who have participated in the Microsoft 365 Copilot trial have completed mandatory training on the responsible and appropriate use of AI. Training includes awareness of the risks of bias and hallucinations from generative AI systems.

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

Answer:

- We operate strictly under the Digital Services Division security policies, which enforce requirements for systems security to be managed in accordance with legislation, regulation, and government standards, including the Privacy Act, Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) requirements.
- The department has privacy obligations to ensure that any new projects including those involving AI comply with the Privacy Act 1988. The department’s privacy obligations extend to the use of AI.
- The department also follows the Five Safes (security) framework along with other whole-of-government security, privacy, discrimination, transparency and accountability guidelines and practices.
- All departmental systems must be assessed under our ICT Risk Management and Authorisation Framework. This aligns to the department’s Enterprise Risk Management Framework and Policy and is based on the requirements of the Protective Security Policy Framework and Australian Government Information Security Manual.
- As a part of this standard assessment process, any use of AI will be examined from a cyber and information security perspective to ensure the government security and privacy requirements are met.

- The department has undertaken a security assessment of Microsoft 365 Copilot, with the subsequent implementation undertaken in accordance with both the security assessment and guidance from the Digital Transformation Agency.

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

Answer:

- The Chief Information Officer (CIO) provides a regular briefing to the department's Audit and Risk Committee on the overall ICT landscape, with a focus on cyber security risk. In recent briefings the CIO has discussed the department's participation in the whole-of-government trial of Microsoft 365 Copilot, however, there has not been a broader discussion or briefing specifically on the topic of AI use.
- The Data and Analytics Transformation Committee (DATC) comprises of First Assistant Secretaries from divisions that manage and store data. DATC is chaired by the Chief Data Officer (CDO).
- The Data Governance Management Committee (DGMC), comprising of Assistant Secretaries, is chaired by the CDO or his delegate. Both DATC and DGMC committees meet to discuss data initiatives and AI and the department’s approach will be overseen in these fora and the Data and Digital Steering Committee.
- A trial of Microsoft 365 Copilot is underway and any extension of this has been discussed, with more work being done to understand financial implications.

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

Answer:

- To date, the department's internal audit program has not undertaken an audit on the controls for AI.

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

Answer:

- The department's internal AI product development lifecycle (bespoke) includes:
    - Defining Clear Objectives and Metrics
    - Data Logging
    - Version Control
    - Explainability and Interpretability
    - Performance Audits against the defined objectives and metrics.
    - Stakeholder Engagement
    - Continuous Monitoring and Improvement

  - We document where AI is used within the department.

- Microsoft 365 Copilot is a digital assistant that does not make decisions. It requires user input to accept/action any output that is provided by the tool.

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?

Answer:

- The AI platforms used by the Department comprises Commercial Off the Shelf (COTS) and bespoke (systems developed in-house).

- Microsoft 365 Copilot is a COTS product.

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?

Answer:

- AI development teams within the department have ownership and responsibility for understanding their bespoke code, including training code models to learn and innovate. Code is reviewed as part of the development lifecycle.

- The source code for Microsoft 365 Copilot is owned by Microsoft and is used under license agreement.