OFFICIAL

SUBMISSION - INQUIRY INTO THE USE AND GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS BY PUBLIC SECTOR ENTITIES

Reference Period (October 2024)

For further information on making a submission to a Committee inquiry, please see the [APH website](#).

AGENCY APPROACH TO AI

In accordance with government guidance and policy, the ABS carefully manages the risks associate with exploring the potential benefits of Artificial Intelligence (AI). The ABS approach is backed by the strong internal controls and security culture of the ABS, developed over many years of protecting the sensitive information it collects, processes and disseminates.

The ABS approach to AI is informed by engagement with consumers, industry, government and the research sector. The ABS tracks AI developments through monitoring of publications and guidelines in Australia and overseas. To ensure it following best practice, it works closely with other agencies, particularly the Digital Transformation Agency (DTA), Department of Industry Science and Resources (DISR) and the Australian Cyber Security Centre (ACSC).

The ABS is also part of the *Generative AI for Official Statistics* project under the High-Level Group for the Modernisation of Official Statistics (HLG-MOS) established by the Conference of European Statisticians. This project is exploring potential applications for AI within national statistical organisations and the management of associated risks and issues.

INQUIRY INTO THE USE AND GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS BY PUBLIC SECTOR ENTITIES
Submission – Australian Bureau of Statistics
October 2024

Governance controls

The use of technology within the ABS is governed by the Chief Information Officer (CIO) with support from the Chief Technology Officer (CTO) and Chief Information Security Officer (CISO). New technologies, including AI, must be assessed and approved prior to introduction into the ABS ICT environment or use for official business purposes.

ABS staff are educated on appropriate use of AI productivity tools and are permitted to use Microsoft Copilot in Edge (formerly known as Bing Chat Enterprise). This AI web chat platform from Microsoft provides enterprise data protections which have been assessed by an independent (IRAP) accredited security assessor as suitable for work purposes at the Official level.

ABS staff are reminded by all staff bulletins and direct emails of the risks associated with the use of public AI platforms (e.g. ChatGPT). ABS staff have been directed not to use public AI platforms for official business use. This means that internal or potentially sensitive ABS information must not be used with public AI platforms, and staff may only experiment with public AI platforms outside the ABS IT environment, using publicly available information.

To limit security and privacy risks, the ABS has implemented controls to block access to public AI services (e.g. ChatGPT) from the ABS IT environment.

Policy controls

The use of AI within the ABS is currently covered by the ABS Cyber Security Policy and Cloud Services Security Policy. These policies ensure that official information, sensitive information, and information protected under the Census and Statistics Act (1905) is appropriately secured against unauthorised access, modification or deletion. To protect sensitive information and information protected under the Census and Statistics Act, these security policy directives have been issued:

- Cloud services must reside within Australia to ensure data sovereignty
- Strong encryption must be applied to protect data
- Cloud service providers must not have access to unprotected ABS data
- Only cloud services that have been subject to independent (IRAP) security assessment should be used.

In accordance with the recently released *Policy for the responsible use of AI in government,* the ABS is developing an AI strategy and policy to more formally govern its use of AI and related technologies (planned for completion March 2025). In the interim, the ABS will continue its directives, guidance and communications to all staff on the appropriate use of AI. At the ABS Security Week (21-25 October 2024) security and risks relating to AI are a key theme throughout staff education and awareness events.

AI USE CASES

The ABS has explored several applications of AI to better its understanding of the technology and associated risks. The AI use cases being explored by the ABS focus on productivity and reduction of effort, and do not involve decisions on service delivery.

ANZSCO coding service

As part of the ANZSCO (Australian and New Zealand Standard Classification of Occupations) Review project, a system to automate the coding of occupations has been developed using Machine Learning (ML) technology.

This system has been developed on the Amazon Web Services (AWS) cloud platform using services that have been subjected to an independent (IRAP) security assessment. The ABS has commissioned its own security risk assessments throughout the development of this system.

Significant testing has been conducted and controls are in place to ensure the quality of outputs. Quality controls include automated checking of ML coded responses against other ABS coding services, establishing measures of accuracy and monitoring for changes in accuracy over time, and human oversight of coding outputs. The Hierarchical Support Vector Machine (HSVM) machine learning technology used for this service enables direct traceability of input to output.

This service is currently being prepared for release which will see broad use both within the ABS and by other government agencies.

ANZSCO job descriptions

In 2023 as part of the ANZSCO review, the ABS conducted a trial outside of its IT environment using generative AI (ChatGPT) to suggest occupation tasks. This low-risk trial used information already in the public domain and helped the ABS explore the potential risks of generative AI for security, privacy, ethics, technology and legal compliance.

The successful trial met its primary business objective of improving efficiency, while also improving the ABS's understanding of AI solutions and risks.

AI assisted code conversion

Following discussions with other national statistical organisations who are using AI to modernise their statistical codebase and operations, the ABS is trialling the use of AI to translate SAS code into R, and AI coding assistants to support application developers.

Solutions being tested have been investigated to ensure that any ABS source code shared with the AI platform remains secured and is not incorporated back into the AI model. Furthermore, the ABS has verified with the vendors that any source code provided by the AI platform remains the intellectual property of the ABS. Staff trialling these platforms have been advised that they must review and verify all code (AI and human developed source code), and all code is subjected to security scanning for defects and vulnerabilities.

INQUIRY INTO THE USE AND GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS BY PUBLIC SECTOR ENTITIES
Submission – Australian Bureau of Statistics
October 2024

Copilot for Microsoft 365

ABS is currently conducting a limited trial of Copilot for Microsoft 365 (AI assistant for Microsoft Office). This trial will help the ABS better understand how to harvest the benefits of AI, while effectively managing the risks.

The ABS understands that information management and access is a key enabler for the success of AI. Given the ABS is only in the early stages of migrating its information holdings from HCL Notes (formerly IBM Lotus Notes) to Microsoft SharePoint, there are less potential benefits from a broader scale trial. Therefore, the ABS has not opted into the broader Australian Public Service trial of Copilot which is being led by the DTA.

Other AI technologies

ABS continues to monitor the progression of AI with its technology vendors. Many vendors who supply technologies to the ABS have plans to integrate some form of AI into their products. ABS will thoroughly scrutinise all new AI technologies to ensure they provide appropriate protection against AI related risks, and that sensitive data is held within Australia and protected in accordance with ABS security policies.