DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Joint Public Accounts and Audit

Subject: Use and Governance of Artificial Intelligence Systems by Australian Public sector Entities

Asked by: Julian Hill

Question 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 of Home Affairs (the Department) uses AI for advanced analytics and to increase productivity across a number of diverse missions, operational domains, and mandated functions.

The Department defines **advanced analytics** as Machine-Learning analysis systems. The Department currently uses advanced analytics for a range of functions, including in supplementing efforts to: predict risk in visa programs, detect and disrupt the flow of illicit goods in the international mail and cargo domain; identify fraudulent documents using computer vision techniques; and to extract entity information from unstructured text using Natural Language Processing.

The Department defines **productivity AI** as simple process automation and office productivity tools. The Department is currently using some rules-based robotic process automation tools, which are sometimes complemented with simple machine learning such as natural language processing, noting none of these systems produce decisions. The Department is also assessing and trialing Gen AI tools for office productivity purposes across a small range of functions, including participation in the DTA-led Microsoft Copilot trail, for which the Department has a standalone instance of Copilot to maintain security and privacy, and to ensure no Departmental data leaves our tenancy or control.

The Department is also **exploring** the appropriateness and viability of incorporating AI elements into additional Departmental functions for potential future usage, where we are confident that the potential risks of using AI can be mitigated.

Question 2:

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

Answer:

The Department of Home Affairs' (the Department) use of AI is undertaken in accordance with relevant APS policy frameworks, including the Australian AI Ethics principles; Australia's Cyber Security Strategy; the Data and Digital Government Strategy; and the Guidelines for Secure AI System Development; the Protective Security Policy Framework (PSPF); Information Security Manual (ISM); and the Department's Security Risk Management Framework. Every individual AI system is also built in compliance with relevant domain specific legislation/regulation, for instance anything built for border management is done in compliance with the Customs Act and Australian Border Force Act.

In addition, the Department has contributed to and is preparing to implement the Australian Public Service (APS) Policy for the responsible use of AI in Government and the APS AI Assurance Framework currently being developed by the Digital Transformation Agency (DTA) and the Department of Industry, Science and Resources (DISR). The Department also remains engaged with national and international best practice, frameworks and standards, such as the soon to be launched National AI Centre (NAIC) AI Safety Framework.

Question 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:

In addition to ensuring the use of AI is undertaken in accordance with relevant legislation and regulations, the Department has various internal frameworks and policies to ensure the responsible use of AI. These include: the Data Science Lifecycle Procedural Instruction; the Department's Data Product Lifecycle Framework; the AI Risk Management Plan; the AI Ethics Policy; Privacy Impact Assessments; the Data Security and Access Management Policy Statement and Procedural Instruction; Critical Technology Supply Chain Principles; and the Acceptable use of Departmental ICT Resources Procedural Instruction. These internal frameworks and policies complement the Australian Government's regulatory requirements for information security under the Protective Security Policy Framework (PSPF), the Information Security Manual (ISM) and the Department's Security Risk Management Framework – Policy Statement.

The Department's internal frameworks and policies are informed by international and whole-of-government best practice, standards and frameworks, such as the Datasheets for Datasets, Model Cards for Model Reporting, and the National AI Centre AI Safety Framework.

Question 4:

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

Answer:

The Department of Home Affairs (the Department) is cognisant of potential supply chain risks when using existing AI solutions or software and takes active steps to monitor and mitigate these risks. Supply chain risks are particularly acute where users become dependent on commercial providers for applications that require training on data to build effective capabilities.

In 2021, the Department published Critical Technology Supply Chain Principles (the Principles), which are publically available on the Department's website at https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/critical-technology-supply-chain-principles.

The Principles identifies ten principles grouped under the pillars of 'security-by-design', 'transparency', and 'autonomy and integrity', and aims to assist government and businesses to make informed decisions regarding suppliers and the transparency of their own products. While this forms a basis for the Department's understanding of supply chain risks in relation to AI, the Department is committed to constantly reviewing its policies against international and whole-of-government standards to ensure they remain fit for purpose.

Question 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:
The Department of Home Affairs' (the Department) Enterprise Risk Management Policy sets the framework for establishing and maintaining appropriate systems of risk oversight and management including:

- The Department's approach to managing risk and how this supports the Department's objectives
- The Department's risk appetite and tolerances
- Key roles and responsibilities for managing risk.

The Department has developed an AI Risk Framework which requires approval by the Chief Information Security Officer and Chief Data Officer. This risk based approach is complemented by policies, frameworks, and controls, informed by relevant legislation, regulations and internationally accepted standards to manage the broad risks associated with AI.

The Department has a number of mechanisms to manage the risks arising from AI including:

- The Department's Data Science Life Cycle Procedural Instrument
- Software controls
- Architectural Review Board (ARB)
- Internal assessments.

The Department's Data Science Life Cycle Procedural Instrument is used to govern internally developed Machine Learning systems used by the Department and contains governance requirements that ensure compliance before systems can be triggered to advance beyond these checkpoints.

Question 6:

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

Answer:

The Department of Home Affairs (the Department) has developed a Data Science Lifecycle Procedural Instrument that outlines how to manage regular updates to AI and supporting data. In alignment with this Procedural Instrument, Production AI and Machine Learning models are periodically retrained at intervals appropriate to the application. Models that become obsolete or ineffective or requiring incorporation of new datasets are retired, and a new updated version is built. The Department is also committed to providing regular training to ensure staff have the relevant skills and experience needed to manage these issues.

Question 7:

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

Answer:

The Department of Home Affairs (the Department) takes a variety of factors into consideration when planning for the additional capability required to implement AI. This includes the guidance provided in the draft APS AI Policy and Assurance Framework, as well as the need to build AI requirements into our data architecture: the technical guardrails, capability mapping, and the training required to ensure AI systems used by the Department are compliant with our legislative, policy and ethical obligations.

Question 8:

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

Answer:

The Department has internal policies and frameworks to manage the risks of bias and discrimination in the use of AI. These include: the Data Science Lifecycle Procedural Instruction; the Department's Data Product Lifecycle Framework; the AI Risk Management Plan; the AI Ethics Policy; the Data Security and Access Management Policy Statement and Procedural Instruction; Critical Technology Supply Chain Principles; and the Acceptable use of Departmental ICT Resources Procedural Instruction.

The Department continues to leverage and evolve accepted international and whole-of-government guidance on the ways to manage the risks of bias and discrimination in the use of AI, including as outlined in the Datasheets for Datasets, Model Cards, and the soon to be released National AI Centre AI Safety Framework.

Question 9:

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

Answer:

All production systems in the Department of Home Affairs (the Department) are robustly managed with formal ICT, data, privacy, legal and security assurance and governance. The Department manages production systems through its Security Risk Management Plan (SRMP), the Data Operating Model, Privacy Impact Assessments, legal review, and providing either an "Interim Authority to Operate" (for proof of concept projects) or "Authority to Operate" (for production systems).

Machine Learning systems are additionally governed in alignment with Australia's AI Ethics framework and our Data Science Lifecycle Procedural Instrument (DSLC). All data products including robotic process automation or other productivity tools are governed by the Department's Data Product Lifecycle (DPL) Framework. These frameworks assure a rigid set of steps to ensure ethical, code, security and privacy assessments are undertaken before a product is developed and released. The DSLC incorporates the Australian Government's regulatory requirements for information security under the Protective Security Policy Framework (PSPF), the Information Security Manual (ISM) and the Department's Security Risk Management Framework – Policy Statement.

The Department's staff and systems are also governed by the Acceptable use of Departmental ICT Systems and Information Procedural Instruction.

Both the DSLC and DPL Framework are aligned to the Department of Industry Science and Resources AI Ethics Principles, and the Guidelines for Secure AI System Development, which are publically available.

Question 10:

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

Answer:

The Department of Home Affairs' (the Department) Senior Leadership Committee has been briefed about AI usage in the Department.

Question 11:

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

Answer:

The Department's internal audit program considers the Department's major investment programs, projects and systems as well as the risks and controls in place in respect of those items. This includes in respect of the Department's use of AI.

The Department also has a range of separate assurance controls. These include ICT, security, access management and data governance and assurance frameworks, and the Data Science Lifecycle Procedural Instruction. Generative AI tools are also not available broadly to staff, unless there is a formal application, risk assessment and mandatory Generative AI training and assessment is undertaken.

These internal frameworks and policies complement the Australian Government's regulatory requirements for information security under the Protective Security Policy Framework (PSPF), the Information Security Manual (ISM) and the Department's Security Risk Management Framework – Policy Statement.

The Department continues to contribute to whole-of-government efforts to uplift and uphold AI standards, controls, and architectural approaches, to complement policy, governance and assurance frameworks. The APS AI Policy and Assurance Framework is also in the process of being implemented which will provide another layer of controls, risk management and assurance for AI systems.

Question 12:

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

Answer:

No Machine Learning AI systems used by the Department produce decisions.

Question 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:

Yes, the Department uses AI platforms that are off the shelf products, customised from other products, and AI systems developed in-house.

Question 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:

All algorithms, code and bespoke AI systems generated by the Department of Home Affairs are owned by the Department. Source code is documented and undergoes code reviews by specialist technology and cyber security staff.

The code of third party AI systems are owned by the vendors. The Department tests and reviews the functionality of third party AI products and in some instances works with technology vendors to improve the effectiveness of the product.