Artificial Intelligence (AI) and ChatGPT

KEY NARRATIVE

- PM&C has used Artificial Intelligence (AI) in the past.
- PM&C does not currently use ChatGPT.
- There is scope for PM&C to expand its use of AI (including ChatGPT) in future projects.

KEY QUESTIONS AND ANSWERS

Does PM&C currently use Artificial Intelligence (AI) or ChatGPT?

- No.
- PM&C has undertaken some small scale AI testing in the past.
- PM&C has not utilised ChatGPT at this time, however PM&C would consider its use if a business requirement existed.
- A cyber security review of ChatGPT has not been undertaken.
- ChatGPT, like all systems that are used on PM&C's IT network, would have to be secure and stable in order to be compatible for use on PM&C's classified networks.
- Any evaluation of ChatGPT, or other similar systems, would be done in line with PM&C's standard system authorisation review processes, and would typically involve the Australian Cyber Security Centre due to the unique nature of the service.
- *If pressed* – The primary use of AI within PM&C was a simple chatbot that provided users with basic information about the PM&C Enterprise Agreement.
    - This testing was undertaken as a proof of concept only and is no longer active.
- ACSC have not provided any guidance to PM&C on the use of AI or ChatGPT specifically.

Is there potential for the department to use AI or ChatGPT? Is it cleared for use?

- Yes, there is potential for future use.
    - AI can be used for data analytics, particularly for categorising and sorting unstructured datasets.
- No, this has not yet been cleared for use.
    - As is the case with the potential procurement and implementation of any new technology, PM&C would need to consider skilled resources, funding and the suitability of any AI program or service used to ensure it meets privacy, security and value-for-money criteria.
- PM&C has no current projects involving AI on our networks, including ChatGPT, at this time.

FACTS AND TIMELINE

What is AI?

In general use, the term "artificial intelligence" means a programme which mimics human cognition. At least some of the things we associate with other minds, such as learning and problem solving can be done by computers, though not in the same way as we do. AI is loosely defined as a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation.

What is ChatGPT?

ChatGPT (short for Chat Generative Pre-trained Transformer) is a chatbot. It was launched by OpenAI, a US company, in November 2022. The program is built on top of OpenAI's GPT-3.5 family of large language models. It is fine-tuned with both supervised and reinforcement learning techniques.

ChatGPT was launched as a prototype on November 30, 2022. The website had more than one million users after five days. It got attention for its responses and answers in many areas of knowledge. Its uneven accuracy was said to be a major drawback.

While the chatbot is free to use, there have been announcements and rumours over a paid version called ChatGPT Professional. OpenAI warns users that the bot may give wrong information or have biased content.

Artificial Intelligence (AI) and ChatGPT

KEY NARRATIVE

- PM&C has used Artificial Intelligence (AI) in the past.
- PM&C does not currently use ChatGPT.
- There is scope for PM&C to expand its use of AI (including ChatGPT) in future projects.

KEY QUESTIONS AND ANSWERS

Does PM&C currently use Artificial Intelligence (AI) or ChatGPT?

- No.
- PM&C has undertaken some small scale AI testing in the past.
- PM&C has not utilised ChatGPT at this time, however PM&C would consider its use if a business requirement existed.
- A cyber security review of ChatGPT has not been undertaken.
- ChatGPT, like all systems that are used on PM&C's IT network, would have to be secure and stable in order to be compatible for use on PM&C's classified networks.
- Any evaluation of ChatGPT, or other similar systems, would be done in line with PM&C's standard system authorisation review processes, and would typically involve the Australian Cyber Security Centre due to the unique nature of the service.
- *If pressed* – The primary use of AI within PM&C was a simple chatbot that provided users with basic information about the PM&C Enterprise Agreement.
    - This testing was undertaken as a proof of concept only and is no longer active.
- ACSC have not provided any guidance to PM&C on the use of AI or ChatGPT specifically.

Is there potential for the department to use AI or ChatGPT? Is it cleared for use?

- Yes, there is potential for future use.
    - AI can be used for data analytics, particularly for categorising and sorting unstructured datasets.
- No, this has not yet been cleared for use.
    - As is the case with the potential procurement and implementation of any new technology, PM&C would need to consider skilled resources, funding and the suitability of any AI program or service used to ensure it meets privacy, security and value-for-money criteria.
- PM&C has no current projects involving AI on our networks, including ChatGPT, at this time.

FACTS AND TIMELINE

What is AI?

In general use, the term "artificial intelligence" means a programme which mimics human cognition. At least some of the things we associate with other minds, such as learning and problem solving can be done by computers, though not in the same way as we do. AI is loosely defined as a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation.

What is ChatGPT?

ChatGPT (short for Chat Generative Pre-trained Transformer) is a chatbot. It was launched by OpenAI, a US company, in November 2022. The program is built on top of OpenAI's GPT-3.5 family of large language models. It is fine-tuned with both supervised and reinforcement learning techniques.

ChatGPT was launched as a prototype on November 30, 2022. The website had more than one million users after five days. It got attention for its responses and answers in many areas of knowledge. Its uneven accuracy was said to be a major drawback.

While the chatbot is free to use, there have been announcements and rumours over a paid version called ChatGPT Professional. OpenAI warns users that the bot may give wrong information or have biased content.

Artificial Intelligence Policy and Large Language Models

Handling note

- First Assistant Secretary National Security, Lachlan Colquhoun, to lead.
    - First Assistant Secretary Corporate and Technology, Hugh Cameron, to lead on use of ChatGPT in the Department of the Prime Minister and Cabinet (PM&C).
- Questions relating to critical technology policy development and the digital economy should be directed to the Department of Industry, Science and Resources.
- Questions on cyber security policy should be directed to the Department of Home Affairs.
- Questions on government's use of information and communications technology should be directed to the Digital Transformation Agency.
- Questions on the Protective Security Policy Framework and privacy policy should be directed to the Attorney-General's Department.

Framing points

- The Government has identified Artificial Intelligence (AI) as a critical technology in the national interest.
- AI and large language models (LLMs), including OpenAI's ChatGPT, pose unique challenges that Government is still working to understand and respond to.
- The Government will continue to make security decisions based on our national interests, informed by relevant agencies.

PM&C role

- PM&C provides advice to the Prime Minister on technology matters including AI, in consultation with lead agencies.

- PM&C works with the Department of Industry, Science and Resources, the Digital Transformation Agency, the Australian Cyber Security Centre, the Department of Home Affairs and other agencies to ensure a coordinated approach to Australia's emerging technology issues.

Key issues

Security concerns with artificial intelligence and large language models

- The speed of innovation in new AI models poses new risks and creates uncertainty about their full implications, including to personal and national security.

- The Government is working to understand the scope and implications of security concerns arising from AI and LLMs, and how the Government can and should respond.

If asked: Who is the Government lead on AI policy issues?

- No single agency leads AI policy issues. Understanding, managing and responding to any risks from AI and LLM technologies involves a range of agencies.

    - This includes the Department of Industry, Science and Resources, Department of Home Affairs, Digital Transformation Agency, the Australian Cyber Security Centre, Department of Foreign Affairs and Trade and Department of Education.

- AI policy in the context of critical technologies policy is led by the Critical Technologies Hub within the Department of Industry, Science and Resources.

- Further questions on the Critical Technologies Hub should be directed to the Department of Industry, Science and Resources.

If asked: what is the Government's **policy toward AI**?

- The Government is aware that AI has the potential to bring enormous benefits as well as pose unique security challenges. The Government is actively monitoring the developments in AI technologies and continues to shape its policy in line with our national interest.

- AI has been identified as one of seven priority technologies on the List of Critical Technologies.

- Further questions on the List of Critical Technologies Statement, including AI should be directed to the Department of Industry, Science and Resources.

If asked: about **security risks** posed by AI

- AI and LLM technologies have the capacity to significantly enhance or pose risk to our national interests (economic prosperity, social cohesion and/or national security).

- AI systems can also be used against Australia, and to harm our interests, such as through the use of AI in deepfake videos, or by powering large-scale malicious cyber activity.

    - LLMs, such as ChatGPT, may enable sophisticated and large-scale threats to security systems.

    - Open source reporting has indicated that ChatGPT can, and is, being used to generate malicious code.

- Easily accessible AI technologies, such as ChatGPT, are increasing the scale and speed of these security risks.

If pressed: about **security risks** posed by AI

- There are a number of security risks posed by AI.

- AI developed from poorly written or applied algorithms and biases can result in faulty decision-making that could harm people, machinery or critical infrastructure.

- AI may also be used to enable cybercrime, including scams, and malicious cyber-attacks.

- AI can erode social cohesion and trust in our democracies via the use of deepfakes and mis/dis-information at unprecedented scale.

- Vulnerabilities in AI-based systems can also be exploited to undermine public confidence in AI-based tools and services.

    - There are concerns AI can clone voices to bypass voiceprint security systems.

    - Voiceprint security systems are used by Services Australia and Australian Taxation Office.

- There are concerns that systems like ChatGPT can be used to promote violent, racist or hateful ideologies.
    - While some digital platforms have included content filters to address AI and LLM systems like ChatGPT promoting criminal behaviour or hateful ideologies, we understand that, in some instances, users are able to craft requests to evade restrictions.

If asked: about what **regulatory and/or policy settings** Government has to respond to AI security concerns

- AI regulation is an emerging policy area that cuts across many areas of Government.
- The Australian Government is currently exploring what is needed to respond to the issues posed by AI technologies. This will be informed by views across relevant agencies, experts, and international examples.
- Existing work on AI policy across government includes:

Department	Work underway
Department of Industry, Science and Resources	• Progressing work on AI regulation [and on XX XX 2023 released a consultation paper on responsible AI.] • Developed Australia's Artificial Intelligence Ethics Principles [*under the previous government]*. o There are eight principles designed to ensure artificial intelligence is safe, secure and reliable.
Department of Home Affairs	• Developed the Critical Technology Supply Chain Principles (the Principles). o These Principles are non-binding and voluntary, and are intended to act as a tool to assist governments and businesses in making decisions about their suppliers and transparency of their own products.
Australian Signals Directorate	• Developed the 'Ethical Artificial Intelligence in the Australian Signals Directorate Framework'. o The Framework outlines how the Australian Signals Directorate manages complex systems that have a direct impact on the privacy and security of Australians.

Digital Transformation Agency	• Issued guidance to help public sector adoption of AI as part of its Australian Government Architecture.
CSIRO	• Coordinates the National AI Centre, funded by the Australian Government. o The National AI Centre established the Responsible AI Network to support Australian industries with responsible AI practices.
Department of Education	• Education Ministers have agreed to establish a taskforce to develop an evidence-based, best practice framework on harnessing AI for the schools sector. The taskforce will report back to Ministers in 2023.

- Further questions should be directed to the relevant agencies.

If pressed: why isn't the Government doing more on AI?

- Government is working to understand both the potential benefits and challenges presented by AI technologies.
- There are significant potential benefits to AI for our economy and society. A considered approach is needed to ensure policy addresses potential harms and avoids unintended consequences.

If asked: about the Government's policy on **ChatGPT**

- The Government is working to understand the implications of ChatGPT, including any security concerns.
- PM&C has blocked access to ChatGPT on the departmental network. Further questions on the use of ChatGPT in PM&C should be directed to First Assistant Secretary Corporate and Technology Division, Hugh Cameron.
    - Questions on the use of ChatGPT by other government agencies should be directed to the Attorney-General's Department as controllers of the Protective Security Policy Framework (PSPF).
- Questions on critical technologies policy should be directed to the Department of Industry, Science and Resources.
- Questions on domestic security issues should be directed to the Department of Home Affairs.

Background

International approaches to AI regulation

Other nations are grappling with policy and regulatory responses to AI. The European Union (EU) and US are most advanced in regulatory developments, however a number of countries are progressing risk-based approaches to AI governance.

The EU considering new legislation (the *EU AI Act*) which would adopt a risk-based approach to AI regulation, with differing regulatory requirements based on the risk of the AI (unacceptable risk, of the high risk and unregulated). The European Commission has also proposed adapting existing civil liability rules to better support victims of AI-enabled products/services in liability claims. EU regulatory frameworks also include the *Digital Services Act* which creates obligations for online platforms to reduce harms and counter risks online.

In January 2023, **the US** released an AI Risk Management Framework which is intended for voluntary use by organisations to address risks in the design, development, use and evaluation of AI products, services and systems. The Trump Administration also released an Executive Order to guide federal agencies to ensure they use AI in a way that fosters public trust and confidence and protects privacy and other civil rights (still in effect). The White House recently released the *Blueprint for an AI Bill of Rights* which sets out principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public. A number of US states have passed bills limiting the use of AI.

The UK Science and Technology Framework sets out government's strategic vision and identifies AI as one of 5 critical technologies. The UK has also commenced consultation on an AI regulation white paper, intended to inform future legislation, which sets out a framework for responsible development and use of AI in the economy. This complements other AI transparency efforts through its National Data Strategy. **Canada** is considering its first AI legislation, the *Artificial Intelligence and Data Act*, which would establish national requirements for the design, development, use and provision of AI systems and prohibits certain conduct in relation to these systems that may result in serious harms or biased outputs.

ChatGPT

ChatGPT (short for Chat Generative Pre-trained Transformer) is a chatbot built using LLMs. LLMs are a type of artificial intelligence trained on a massive amount of articles, books, or internet-based resources to produce human-like natural language outputs.

There has been media coverage of security and social risks posed by ChatGPT, including (but not limited to) risks for cyber security, social cohesion, and the education sector.

The Government is working to understand security challenges posed by new iterations of AI, including generative language models (e.g. ChatGPT).

The Government will carefully balance the security risks with the economic and social opportunities when considering policy decisions.

Governments around the world are struggling with similar issues as they explore new policy challenges. Media has reported on other countries' approaches to ChatGPT.

On 31 March 2023, the Italian data privacy regulator ordered an immediate ban on ChatGPT over alleged privacy violations of laws such as the European Union's General Data Protection Regulation (GDPR).

On 12 April 2023, the Italian data privacy regulator gave OpenGPT until 30 April 2023 to comply with specific privacy requirements, including but not limited to, verifying users' age and consent to using personal data.

ChatGPT is banned or blocked by a number of other countries including China, Russia, North Korea, Cuba, Iran, and Syria.

Media reporting has revealed that China is concerned with the ChatGPT's non-compliance with the country's firewall, citing a risk of political interference.

Agency responsibilities for critical technologies policy

AI and LLM technologies affect a broad range of government portfolios. Relevant agencies are undertaking work to understand how these technologies interact with their broader policy responsibilities. There are varying levels of AI policy maturity across government. PM&C is working with agencies to ensure consistency as government iteratively understands the full implications of new technologies.

The Critical Technologies Hub is responsible for leading and coordinating policy advice to government on critical technologies that reflects whole-of-government equities and balances the national interest. The hub is supported by three nodes:

- The economic node, led by the Department of Industry, Science and Resources, supported by the Treasury.
- The scientific node, led by Australia's Chief Scientist, supported by the Chief Defence Scientist.
- The national security node, led by the Department of Home Affairs, supported by the Office of National Intelligence.
- The hub and nodes are supported by the Department of Foreign Affairs and Trade to provide international engagement on critical technologies.

Timeline
(Blue entries = PM&C action)

Date	Action
17 April 2023	PM&C's Division Heads' Cascade Note informed staff that access to ChatGPT has been blocked on the departmental network.
11 April 2023	Senator David Shoebridge asked a question on notice to the Minister representing the Prime Minister (no.1915) and to the Minister representing the Minister for Government Services (no.1921) regarding ChatGPT and its use by departments, agencies or ministerial officers. The question to the Minister representing the Prime Minister is unanswered.

Lachlan Colquhoun First Assistant Secretary	National Security Division	s 22(1)(a)(ii)	s 22(1)(a)(ii)
s 22(1)(a)(ii)	Critical Infrastructure and Counter Foreign Interference / Cyber Policy	s 22(1)(a)(ii)	s 22(1)(a)(ii)
Consultation	PM&C: International; QANS; II&E; SPD; Legal; GTD; Corporate; Eco External: Department of Industry, Science and Resources		

Attachment A Parliamentary Question on Notice 1915 – Senator David Shoebridge to Minister representing the Prime Minister.

ATTACHMENT A

Parliamentary Question on Notice no. 1915
Senator David Shoebridge: asked the Minister representing the Minister for Government Services on 11 April 2023—

With reference to ChatGPT:

1. Are the departments, agencies or ministerial office/s under the Minister's direction using ChatGPT; if yes, in what circumstances and for what purposes is ChatGPT used.
2. Which area of the departments/agencies/offices are using ChatGPT.
3. Does the Minister's departments, agencies or ministerial office/s prohibit employees from using ChatGPT;
    a. if yes, what was the rationale for this decision; and
    b. if no, are your departments, agencies or ministerial office/s aware of any employees who are using ChatGPT as part of their jobs.

Key points

- Artificial Intelligence (AI) has the potential to bring enormous benefits, but also poses unique security challenges.
- The Government is actively monitoring developments in AI technologies, including generative language models such as ChatGPT, and will shape its policy response in line with our national interest.
    - The Department of Industry, Science and Resources (DISR) has been undertaking a review to ensure regulatory settings reflect community expectations of trustworthy and responsible AI.
    - Further information on this work can be provided by DISR.
- AI has been identified as one of seven priority technologies for the List of Critical Technologies in the National Interest.
- The Budget provides funding to accelerate critical technologies industries, including AI, to increase local capacity and capability, and support the adoption of critical technologies such as AI in safe and responsible ways.
- AI policy issues cut across a number of agencies' portfolio responsibilities. DISR coordinates whole-of-Government advice on critical technologies policy, including AI.

Key facts and figures

- The Budget provides $86.5 million for AI initiatives aimed at embedding artificial intelligence technology in the broader economy in a responsible way today, while training the workforce of tomorrow. This includes:
    - extending the National AI Centre and its role in supporting responsible AI usage through developing governance and industry capabilities
    - supporting small and medium enterprises' adoption of AI technologies to improve business processes and increase trade competitiveness
- Previous government funding of $124.2 million for initiatives to enhance Australia's Artificial Intelligence Capability, announced as part of the Digital Economy Strategy measure, has been redirected to new expenditure measures in the 2023-24 Budget.
- Questions on AI policy should be directed to DISR in its role coordinating whole-of-Government advice on critical technologies policy, including AI.
    - But questions on the impact of AI on specific industries, or in specific contexts (ie. defence and national security) can be directed to relevant departments.