Te Pourewa Mātaki
Inspector-General of Intelligence and Security

NZSIS and GCSB use of artificial intelligence

Public summary

Brendan Horsley
Inspector-General of Intelligence & Security
June 2026

INTRODUCTION

1. I have reviewed the New Zealand security and intelligence agencies' use, or planned use, of artificial intelligence (AI).[1] I split my review into two parts:

    - Part one, a research report, set out the domestic and international AI regulation, and frameworks, summarised how AI might be used in the security and intelligence sector, and challenges for the oversight of AI.[2] I published this report in August 2024.

    - Part two, a classified report, examined the use of AI by the NZSIS and the GCSB.[3]

2. This is an unclassified summary of my second report. It omits details of technical capabilities and operations, in accordance with my duty to avoid disclosure of any information that would compromise the agencies' methods. In my classified report I detailed how the NZSIS and GCSB assess, approve, and deploy AI systems, and the nature of these systems. I also examined the agencies' governance of AI, including policies and procedures, and the internal compliance and oversight mechanisms in place.

REVIEW SUMMARY

3. Use of AI in the performance of agency functions potentially raises a number of risks which may have consequences for the legality or propriety of agency operations. The Intelligence and Security Act 2017 (ISA) does not expressly address the agencies' use of artificial intelligence. The lawfulness of use of AI under the Act depends therefore on what an agency does with it. For example:

    - To use AI for a lawful activity relevant to one of its functions (eg using 'dummy' data to test the viability of a tool), an agency would not need any authorisation.[4]

    - To use AI to assist an otherwise unlawful activity (eg covert surveillance in a private place), an agency would need an intelligence warrant.[5] The warrant would authorise the intrusion, not the use of AI as such.

4. Since the publication of my research report, the New Zealand Government produced further guidance for the public sector on using AI responsibly.[6] It emphasises the need for good governance, impact assessments (including privacy and human rights), human oversight,

---

1 These are the New Zealand Security Intelligence Service (NZSIS or the Service) and the Government Communication Security Bureau (GCSB or the Bureau).

2 IGIS *Artificial intelligence frameworks and regulation: An intelligence perspective* (August 2024). This is available on my website.

3 This was a review under s 158(f)(ii) of the Intelligence and Security Act 2017 (ISA).

4 Section 48 ISA provides that an agency may carry out a lawful activity in the performance or exercise of any function, duty or power without an authorisation.

5 Section 49 ISA provides that an agency may carry out an otherwise unlawful activity if authorised.

6 The Department of Internal Affairs (DIA) "Responsible AI Guidance for the Public Service: GenAI" and "Public Service AI Framework" (February 2025).

consideration of security risks and procurement processes, good quality data, and audit and evaluation.

5. The agencies are not excluded from applying the public sector guidance, but there are some obvious limitations on their ability to do so. In particular their need to keep their activities covert limits the extent to which they can make their use of AI transparent and explainable to the public.

6. Unlike many (but not all) government departments, the agencies are not signatories to New Zealand's Algorithm Charter.[7] The charter includes commitments to transparency about algorithm use, consultation with impacted people, and providing a channel for challenging or appealing decisions informed by algorithms. I accept that the charter is worded in a way more suited to agencies that do not operate covertly. The agencies' policies, however, reasonably align with the principles of the charter, to the extent practicable.

7. Overall I found that the agencies have approached the use of AI cautiously. In my classified report I detail how they have considered, and continue to do so, the scope for using AI for intelligence purposes, the risks and the necessary controls. I discuss the agencies' policies, procedures and guidance material, covering matters including record-keeping, risk assessment, training, and human review and validation.

8. The agencies have established an expert advisory group of technical, legal and other specialists, which has responsibilities such as developing an AI-specific risk framework, creating a central repository of systems in use, and reporting to various governance groups, senior leaders, and stakeholders (including my office). I consider it useful for the advisory group to determine what AI applications might approach or pass the agencies thresholds of acceptable risk. I will be looking at their AI risk framework, when it emerges, with this in mind.

9. I was reassured to find neither agency had enabled AI decision-making or relied on AI outputs for decisions. Instead, AI has been used to enhance human capabilities or speed up time-consuming processes, such as triaging large, complex or unstructured data for further human analysis. My impression is that there is an understanding within both agencies of the need for a human to verify machine outputs and consider accuracy, reliability and other matters that require human comprehension.

10. My review found guidance material for the use of AI spread across the agencies' document management systems. As the number of AI tools in use proliferates there is possibly a risk that vital information is scattered. It will be important in my view that those supervising the uptake of AI take care to ensure there is an authoritative, up-to-date and readily findable source of information for each tool. Persistently updated records are an important resource not just for oversight, but also for the agencies' senior leadership and others with responsibilities for managing organisational risk, such as legal and compliance staff.

[7] New Zealand Government *Algorithm Charter for Aotearoa New Zealand* (July 2020). I note that 'algorithms', in the charter, encompasses analytical tools much less sophisticated than AI as well as models that "can take on properties of machine learning".

11. My review identified a few aspects of the agencies' documentation which could be improved, especially when it came to articulating the risks. This is improving under the guidance of the expert AI advisory board. I was informed that some gaps in documentation were being remedied.

12. Since the completion of my classified report I have begun exploring with the agencies how they will continue to facilitate my office's ongoing oversight of their uptake and use of AI. There is an opportunity, while adoption of this technology is in its early stages, to build in protocols and procedures supporting independent oversight as well as robust internal controls. In this highly challenging area it is critical for effective independent oversight that we achieve this.