40° South Guard

Guard alongside NVIDIA NeMo Guardrails

Different problems, different products

Version 1.0 | May 2026

Why this comes up

NVIDIA NeMo Guardrails is an open-source toolkit that lets developers add programmable guardrails to LLM applications. It runs in-process, embedded directly in the application code, and uses Colang (a modelling language) to define conversational boundaries.

The question we hear is: "Our engineering team is already building guardrails with NeMo. Why would we also need Guard?"

The short answer: NeMo is a developer toolkit for building custom guardrails. Guard is a turnkey compliance product. NeMo helps your engineers control LLM behaviour. Guard helps your compliance team prove to APRA that controls are active on every AI call.

Side by side

Capability	40 South Guard	NVIDIA NeMo Guardrails
Primary purpose	Per-call compliance evidence and attestation for all AI providers	Open-source toolkit for building programmable LLM guardrails
Architecture	Inline API proxy. One API change, every provider covered.	In-process library embedded in the application. Requires application-level integration.
Australian PII	Purpose-built detection with checksum validation for TFN, Medicare, ABN, and ACN	No built-in Australian PII detection. Customer builds custom detectors.
Regulatory mapping	Every call mapped to CPS 234, the AI Safety Standard, and the Privacy Act	No regulatory mapping. Developer defines custom rules in Colang.
Per-call attestation	Cryptographically signed attestation per API call with tamper-evident 7-year audit trail	No attestation. No evidence vault. Logging is application responsibility.

AI-specific controls	Prompt injection detection, model inventory, shadow AI blocking, policy enforcement	Topical guardrails, jailbreak detection, hallucination reduction, custom flows via Colang
Data residency	Australian-hosted infrastructure. Data never leaves AU jurisdiction.	Runs wherever the application runs. No managed infrastructure. Customer manages deployment.

Could you run them together?

Yes, though they serve quite different layers of the stack. NeMo Guardrails is excellent for controlling LLM conversation behaviour at the application level. Guard sits at the infrastructure level, generating compliance evidence regardless of what application guardrails are in place.

A practical deployment would use NeMo Guardrails within your application to enforce conversational boundaries, and Guard as the inline proxy to generate regulatory evidence and attestation for every AI call. Guard deploys with one API change. NeMo requires application-level integration.

Suggested next step

We can run a 30-minute proof of value showing Guard generating compliance evidence on the same AI calls your NeMo guardrails are already processing. You will see per-call attestation and regulatory mapping working at the infrastructure level, complementing your application-level controls.

Contact

hello@40south.au

40south.au

Sources

1. APRA Prudential Standard CPS 234 Information Security, July 2019. www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
2. NVIDIA, "NeMo Guardrails documentation." docs.nvidia.com/nemo/guardrails/
3. Australian Government, "Voluntary AI Safety Standard," August 2024. www.industry.gov.au/publications/voluntary-ai-safety-standard
4. OAIC, "Chapter 8: APP 8 — Cross-border disclosure of personal information." www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information

5. 40 South Guard technical documentation. 40south.au