# Ensuring a sovereign and secure AI cloud

nst.com.my/opinion/letters/2026/11/1575349/ensuring-sovereign-and-secure-ai-cloud

November 11, 2026




FILE PIC, FOR ILLUSTRATION PURPOSES ONLY

LETTERS: Cybersecurity policy should be driven by what Malaysia is building and how well those systems are prepared for emerging threats.

In this regard, one project deserves particular attention - the Sovereign AI Cloud announced in the 2027 Budget.

The government states that the cloud is being planned to ensure that the rakyat's data and the nation's strategic information remain under Malaysian control. That is a vital objective.

However, that is only one part of digital sovereignty. A system can be sovereign and still be highly vulnerable.

As critical sectors, industries, public systems and infrastructure increasingly explore and integrate AI, the digital environment we need to protect will become increasingly complex.

AI introduces security risks that go beyond those associated with traditional information systems.

The National Cyber Security Agency (Nacsa) recognises this in its 2026 AI Systems Cyber Security Framework. The framework identifies risks including data poisoning,

prompt injection, model theft, unauthorised access and attacks on the AI supply chain.

Some of these threats do not simply attempt to break into a system; they actively interfere with the data an AI system relies on, the instructions it receives, or the outputs it produces.

That is why one principle within Nacsa's framework is particularly important: Secure-by-Design. Cybersecurity must be engineered into an AI system from its inception, rather than patched on as an afterthought once it has already been developed or deployed.

For the Sovereign AI Cloud, that principle should drive decisions over data protection, access controls, third-party components, continuous monitoring, testing and incident response right from the design stage. The same rigorous thinking should guide AI systems used across our critical infrastructure and public services.

Malaysia is not starting from zero. We already have the Cyber Security Act 2024, Nacsa and now an AI-specific cybersecurity framework.

The task now is to ensure these laws, institutions and frameworks are consistently translated into the very systems we are building today and those we will rely on in the future.

Before the Sovereign AI Cloud advances from a policy announcement to implementation, the government must clarify exactly how Nacsa's Secure-by-Design principles will be embedded into its architecture, procurement requirements, and arrangements with technology partners.

Security testing, continuous monitoring, third-party risk management, and incident response are not secondary considerations to be settled only after deployment.

Nacsa has already provided the framework. What matters now is whether it actively shapes the systems we actually build. If the purpose of the Sovereign AI Cloud is to keep the rakyat's data and the nation's strategic information under our control, sovereignty cannot stop at ownership or control alone.

A sovereign cloud must also be one whose infrastructure is designed, tested and defended to remain secure.

**THULASY SUPPIAH**

Kuala Lumpur