The Hyperscaler Vulnerability

United States Cloud Infrastructure as a Structural National Security Risk to India

BOTTOM LINE

India's strategic and citizen data now sits, at scale, on infrastructure operated by United States companies: Amazon Web Services, Microsoft and Google. This is **a structural sovereign vulnerability, not a compliance problem**, because it arises from who controls the infrastructure, not where the disks are. India has begun to respond: MeitY's March 2026 cloud selection framework and a sovereign cloud framework now in preparation point in the right direction. **The decision that matters is whether that framework will test control and jurisdiction rather than location, bind rather than advise, and have a single owner.** Its design over the next six to twelve months will fix India's posture for a decade.

THREE DISTINCT THREATS: EACH NEEDS ITS OWN REMEDY

	A · The United States as state	B · Adversarial actors	C · Withdrawal of service
Mechanism	CLOUD Act, FISA §702 and EO 12333 reach data held by US providers wherever it is stored. Jurisdiction follows the provider, not the server.	Hostile services compromise the provider's global identity plane, aggregate dispersed metadata, or use insiders.	A provider suspends an Indian user under foreign sanctions, export controls, a court order or its own terms.
Evidence	Microsoft France told the French Senate under oath (June 2025) it could not guarantee French public data would never reach US authorities. §702 lapsed in statute on 12 June 2026, yet collection continues to March 2027.	Storm-0558 (2023): PRC-linked actors forged Microsoft tokens and read mail of 22 organisations and 500+ individuals, including the US Commerce Secretary. Midnight Blizzard breached Microsoft itself months later.	July 2025: Microsoft cut Nayara Energy off from email and data after EU sanctions, until a Delhi High Court hearing loomed. June 2026: a US export directive barred all foreign nationals from two frontier AI models for nearly three weeks.
Remedy	**Narrowable.** Host sensitive data with operators outside US jurisdiction. A CLOUD Act agreement helps only on the law-enforcement channel.	**Not negotiable.** Shrink and segment the attack surface; keep the most sensitive data off shared platforms.	**Contract and prepare.** Continuity clauses, tested exit, and an Indian-controlled fallback for core services.

FOUR FINDINGS REQUIRING ATTENTION

- **Localisation is not sovereignty.** CERT-In, RBI and SEBI rules fix where data sits. None protects it from US legal process while the operator is under US jurisdiction. France, the EU (June 2026 proposal) and Germany (April 2026 catalogue) now test ownership and control.
- **Core public systems already run on US platforms.** GeM moved from a domestic government cloud to AWS in 2024; the National Health Authority uses AWS; the e-Shram registry of some 31 crore workers runs on Azure.
- **India has a live denial-of-service precedent.** Nayara's week without email showed that a foreign measure can switch off an Indian enterprise. Its switch to an Indian provider within days shows that fallback is feasible if prepared.
- **The State's own exposure is unmeasured.** Restraining orders in Jammu and Kashmir (2024, 2025), the Army's December 2025 messaging policy and a March 2025 leak traced to a former official's personal device indicate significant consumer-platform use. No audit has measured it.

WHERE INDIA STANDS: RIGHT STRUCTURE, WITHOUT FORCE

Instrument	What it does	What it lacks
MeitY cloud selection OM (Mar 2026)	Classify under NISPG; Top Secret and Secret off cloud; Category A to government or notified sovereign cloud.	Advisory by its own terms; no sovereign providers notified; no check on classification.
Sovereign cloud framework (draft, Sep 2026)	About 46 safeguards across legal, technical, operational and Make in India requirements.	Not yet final or binding; strength of the control test and continuity terms undecided.
Email to Zoho; Bhashini to Yotta	16.68 lakh official accounts on an Indian platform; language AI on Indian cloud and GPUs.	States, PSUs and the defence supply chain still on consumer cloud. The test must apply to Indian vendors too.

PROPOSED RESPONSE: BUILD ON WHAT EXISTS

Calibrated sovereignty, not autarky. Use the existing NISPG categories as tiers: **Tier 1** (Top Secret and Secret) stays off cloud; **Tier 2** (Category A) moves, under a binding rule, to government or certified sovereign cloud within 36 months; **Tier 3** (Category B) may use any empanelled provider, with continuity and exit clauses.

Track	Horizon	Actions
A · Immediate	0 to 18 months	Shape the sovereign cloud framework before it is final: a control-and-jurisdiction test for every applicant, Indian or foreign; continuity of service as a qualifying condition; binding force for Category A. Commission a twelve-month dependency audit of MoD, DRDO, ISRO, DPSUs, MEA, MHA, regulators and PSBs. Issue a personal-account directive. Insert continuity and exit terms in all cloud contracts. Open exploratory CLOUD Act talks.
B · Medium term	18 to 48 months	Enact a Data Sovereignty and National Security Act giving statutory force to classification and certification. Place the owning authority on a statutory footing with a capital budget of the order of ₹50,000 crore over five years, subject to costing. Regulate AI processing of government data.
C · Structural	48 months +	Build Indian-controlled sovereign cloud capacity; government operation for Tier 1, qualifying domestically controlled ventures permitted for Tier 2. Expand the IndiaAI Mission to provide domestic fallback for AI services. Pursue mutual recognition with France, the EU, Japan and the UAE.

Ownership. Separate the owner of the risk from the owner of the standard. The **National Security Council Secretariat**, through the National Cyber Security Coordinator, owns sovereign-cloud risk for Tiers 1 and 2 and enforces across ministries, the armed forces and regulators. **MeitY** owns the standard, runs certification through STQC and notifies qualifying providers.

NET ASSESSMENT

COST OF ACTION VERSUS COST OF INACTION

The cost of action is bounded and schedulable: eighteen to thirty-six months of transition friction, about ₹50,000 crore over five years (roughly 0.2 per cent of Union spending over the period), and trade friction France has absorbed and the EU now invites. Its own risks, namely domestic lock-in, capability lag and relabelling of foreign offerings as "sovereign", can be designed against. The cost of inaction compounds: two identity-plane breaches of one provider within a year, US collection that survived a statutory lapse, and foreign measures that have already reached an Indian company and AI services used in India. **A bounded cost incurred deliberately is preferable to an unbounded one incurred by default.**

WHAT THE ANALYSIS POINTS TO

(i) One owner for the risk: the National Security Council Secretariat for the most sensitive tiers, with MeitY owning the technical standard. **(ii)** A sovereign cloud framework that tests control and jurisdiction, treats continuity of service as a qualifying condition, and binds for Category A workloads. **(iii)** A twelve-month audit of how much defence, space and regulatory data actually sits on foreign-controlled cloud and personal accounts.

COMMENTS INVITED

This note is an independent analysis, offered to start a discussion. I would value the views of practitioners in government, the armed forces, industry, law and research, particularly on these questions:

- **The test.** Should India's sovereign cloud qualification rest on control and jurisdiction, as France and the EU now propose? How should it treat Indian providers with foreign subsidiaries, code or support functions?
- **Threat C.** Is withdrawal of service by foreign decision serious enough to make continuity of service a qualifying condition? Which contract terms are realistic?
- **Ownership.** Is the NSCS the right owner of the risk, with MeitY owning the standard, or is there a better institutional home?
- **Scale and pace.** Are an indicative ₹50,000 crore over five years and a 36-month migration for Category A workloads realistic?
- **Evidence.** What have I missed or got wrong? Open-source evidence on defence, PSU and regulator cloud use is especially welcome.

Views are welcome by email at iqbalsingh.grewal@gmail.com. Prepared from open sources reviewed to 23 October 2026. The views expressed are personal.