US Data Center Daily Briefing

May 24, 2026

KEY THEMES

- Keppel terminates S$1.43bn sale of 89.3% M1 stake
- IMDA pauses M1 review over possible unauthorized radio-frequency use
- Keppel targets US$150bn AUM by 2030, pivots to data centres
- South Africa e-Vetting Q1 2026/27 rollout and cyber strategy finalisation

---

Keppel's attempt to sell control of Singapore telco M1 just hit a wall — and the reason matters. The S$1.43bn M1 sale to Simba Telecom was terminated after conditions weren't met, with Singapore's IMDA having paused its review over possible unauthorized radio-frequency use. For investors watching Southeast Asia's digital infrastructure capital flows, this is a reminder that "adjacent" telecom assets still carry regulatory tripwires Keppel can't simply step around as it pivots harder into data centres and green energy.

The Big Stories

Keppel has terminated the planned sale of its 89.3% stake in M1 to Simba Telecom, a deal originally valued at about US$1.1bn (S$1.43bn). The catalyst wasn't just deal mechanics: IMDA paused its review due to concerns over possible unauthorized radio-frequency use. The immediate takeaway is obvious — Keppel doesn't get the clean exit it wanted — but the bigger point is that Singapore's regulators can effectively freeze M&A timelines when compliance questions pop up, even on assets that aren't "new" infrastructure.

The other signal is strategic: Keppel has been repositioning toward asset management and capital-light growth, raising S$6.3bn in 2025 and targeting US$150bn AUM by 2030, while leaning into data centres and green energy. This deal failure doesn't change that direction, but it does keep capital and management attention tied up in a telco business it was trying to monetise — and that can affect how quickly it can recycle capital into the next wave of DC and power-linked projects.

Behind the Headlines

South Africa is quietly putting more scaffolding around cyber and intelligence — which can spill into how digital infrastructure is governed and secured. In her Vote 8 tabling, Minister Khumbudzo Ntshavheni outlined State Security's 2026/27 priorities and reforms, including finalising a cyber strategy, rolling out e-Vetting (UAT has commenced; deployment targeted for Q1 2026/27), and reconfiguring the intelligence architecture under GILAA into separate domestic and foreign services. She also flagged new institutional plumbing — a Data Institute and progress on SANAI HEI registration — alongside the National Communication and Information Centre functioning and National Intelligence Estimates awaiting NSC approval.

Why this matters for the sector: when governments formalise cyber strategy and vetting regimes, the practical impact is rarely just policy documents — it can shape procurement requirements, operator security obligations, and how quickly projects involving sensitive workloads can move. The creation of data-focused institutions also signals a push to centralise capabilities that often end up intersecting with private-sector compute and storage ecosystems, even when the headline is “state security” rather than “data centres.”