Policy Actions For Reliable And Robust AI Compute Governance

This policy memo proposes chip registration/chip location verification and a whistleblower incentive and protection programme as policy recommendations for the Department of Commerce. These recommendations protect U.S. national security while maintaining its international position in AI chips.

SUMMARY
As frontier AI systems pose extreme "dual-use" security risks, compute controls are an effective and realistic way to limit frontier AI systems capabilities and prevent unwanted actors from accessing those capabilities. Recent BIS actions have rescinded the Framework for Artificial Intelligence Diffusion of January 2025 and issued new guidance, including new end-use controls for advanced computing items, guidance to prevent diversion, and controls on Chinese ICs. The Foundry Due Diligence Rule additionally mandates due diligence and licensing.

ANALYSIS OF CURRENT BIS EXPORT CONTROLS

- **Safeguarding against information leaks:** As compute is a strategic, military, and economic resource, current BIS export controls aim to restrict adversary access to frontier training compute and weights through the AI chip supply-chain, particularly against China.
- **Fragile training compute thresholds**: Numeric performance thresholds (such as TPP<=4800) are easy to evade by distributing workloads across clusters, or by low-compute models like DeepSeek R1, and serve as a poor proxy for capabilities.
- **Lack of regulatory binding force**: Non-regulatory advisories, uneven due-diligence burdens, and weak enforcement create unpredictability and compliance burdens for exporters.
- **Model weight enforcement challenges**: Controlling AI weights is an extremely complex and hard to enforce process which will become more challenging as models increase in size.

RECOMMENDATIONS FOR THE DEPARTMENT OF COMMERCE

- The Department of Commerce should strengthen export control by implementing specific **chip registration and chip location tracking methods** to **secure the AI chip supply chain**. Chip location verification through attestation has been successfully prototyped, does not pose a privacy risk, and does not contain any security backdoors. The BIS could create a feasible and well-enforced chip registration policy consisting of manufacturing registration requirements and transfer reporting requirements.
- **Chip smuggling into China** is a major enforcement issue that BIS can tackle with a low-cost **whistleblowing incentive and protection programme**. This programme would incentivise whistleblowers to report chip smuggling by providing monetary support for penalties and offering protection and confidentiality.