Executive Summary: KYC2 - Self-Enforcing AI Chips for Export Control

This submission, written by a legal and technical expert, argues that export control is now focused more on access to computing power than on hardware. Our KYC2 (Know Your Compute) framework uses algorithms to enforce policy, helping close legal gaps and enabling real-time evolution rather than waiting to fix problems after they happen.

The RASA Act (Jan 2026)[1] authorizes the regulation of remote compute access, fixing the loophole that allows the U.S.'s adversaries and market rivals from being able to rent U.S. chips. The current laws lack technical enforcement–cloud providers cannot verify users–which puts national security and semiconductor export revenue in danger.[2]

Policy Recommendation: The KYC2 Framework. We suggest mandating hardware-level telemetry on AI controlled chips (H200, MI325X) using BIS authority (RASA,[1] EAR §734.9(h), §744.6, §744.21, §748.15[3]). The chips would serve as "Digital Border Guards" that would report workload, location, authentication, and training patterns to automatically find potential military uses (EAR §744.11[3]) and stop unauthorized transfers. Violations would trigger disciplinary actions (EAR §764.3[3]), supporting effective compliance automation.

Economic & Strategic Rationale. Due to the G42's UAE agreement[4], it is now legally acceptable to monitor hardware. Refusing to change risks a potential $77B in revenue[2] while enabling economic rivals and adversaries to become self-sufficient.[6] KYC2 attempts to close the compute gap[5] through algorithmic monitoring, and locks global AI into U.S. standards.

KYC2 Seeks to Counter Current and Future Threats. The framework attempts to confront specific threats. Automated compliance should defeat China's audit ban, GPS verification should defeat Russian/Iranian shells, authentication logs should expose North Korea's identity theft, and workload signatures should distinguish between military/commercial AI usage. Our algorithmic classifiers seek to utilize growing threats to "retrain" faster than attackers can evolve.

Challenges & Mitigation. While some in the industry may be concerned about hardware costs, advocates raise surveillance concerns–ITIF data[2] shows enforcement failures will cost more than implementation costs. On-chip processing seeks to avoid user tracking, while G42's UAE model[4] provides precedent for international acceptance.

Implementation Authority & Timeline. We propose that BIS should issue an interim ruling under RASA and EAR authority[3] in Q2 2026. The framework can be tested in the UAE, UK, and Singapore during Q3/Q4, with full compliance expected by Q4 2027. BIS already has the authority under RASA to act quickly without new laws. **See Page 2 for technical architecture.**

Adaptive ENN GPS Chip: Hardware Export Control

Objective: Export control will be directly embedded within small AI chips that will be placed on other high-level chips. This hardware-level enforcement is difficult to bypass and easier for regulators to verify. Unlike software-based telemetry, this uses an embedded, small-scale neural network to infer a policy violation and authorize preventive measures.

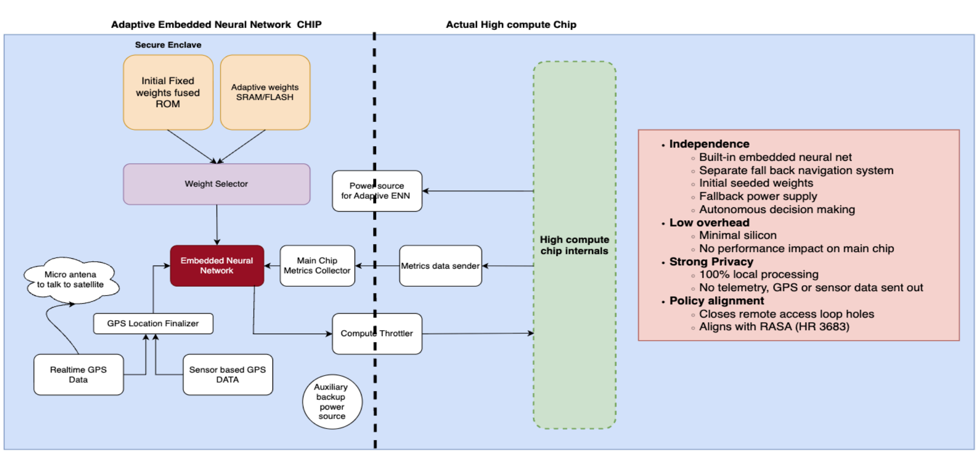
Security[7]: Fixed embedded neural network weights, policy rules for violation inference, and secure boot logic reside in a secure enclave. Roots of trust verification of firmware integrity at boot and runtime. Trusted environment protects fixed model weights against tampering

Embedded neural network layer[8]: A light neural net with fewer than 10 million parameters that will run on a dedicated low-power core. As mentioned above, fixed weights will be in a secure enclave, and adaptive weights will be in a separate modifiable block for periodic external updates via unsupervised adaptation. Weights will be quantized to 4 or 8 bits

Location Tracking[9]: There will be an on-chip micro GPS antenna for geolocation. A fallback geolocation system using MEMS accelerometer/IMU for inertial dead-reckoning will be used. The chip combines the last good GPS position with the accelerometer/gyro predictions using a Kalman filter

Sensors & Telemetry Interface from main chip[10]: An embedded neural network requires live data to determine whether the chip is being used for an unauthorized purpose**.** The chip will include a small collection of microsensors. Accelerometers and inertial measurement units will be used to measure movement, tilt, acceleration, vibration, and more. Temperature, humidity, and voltage sensors will be used to measure temperature, air moisture, and voltage. The built-in one-way interface from the main chip provides power and key metrics (FLOPs, tensor-core utilization, power draw, memory bandwidth, sync frequency, etc.) to ENN.

AI-enabled policy enforcement unit[11;12]: Logic gates (hard-wired circuits built into the chip's silicon) will throttle the GPU clock when a violation is detected. Additionally, it will disable tensor cores or cap interconnect bandwidth in response to embedded neural network detected policy violations(location or high-risk workload patterns).



References

1. Remote Access Security Act, H.R. 2683, 119th Cong. (2025).

2. Information Technology and Innovation Foundation, "Decoupling Risks: How Semiconductor Export Controls Could Harm US Chipmakers and Innovation," 2025, November 10, https://itif.org/publications/2025/11/10/decoupling-risks-semiconductor-export-controls-harm-us-chipmakers-innovation/

3. Export Administration Regulations, 15 C.F.R. §§734.9(h), 744.6, 744.11, 744.21, 748.15, 764.3 (2024). https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

4. G42, "G42 Receives U.S. Approval for Advanced AI Chip Exports, Enabling Full-Scale Deployment of Trusted AI Infrastructure," Press Release, 2025, November 25, https://www.g42.ai/resources/news/g42-receives-us-approval-advanced-ai-chip-exports-enabling-full-scale-deployment-trusted-ai-infrastructure

5. Henry Farrell and Abraham Newman, "How America Can Stay Ahead of China in the AI Race," Foreign Affairs, 2025, April 15, https://www.foreignaffairs.com/united-states/how-america-can-stay-ahead-china-ai-race

6. Matthew Goldstein and Emily Weinstein, "DeepSeek's Lesson: America Needs Smarter Export Controls," RAND Corporation, February 2025, https://www.rand.org/pubs/commentary/2025/02/deepseeks-lesson-america-needs-smarter-export-controls.html

7. Mao, Y., et al. "Amulet: Fast TEE-Shielded Inference for On-Device Model Protection." https://arxiv.org/pdf/2512.07495

8. Lee, J., et al. "LittleBit: Ultra Low-Bit Quantization via Latent Factorization" https://arxiv.org/pdf/2506.13771

9. Shkel, A. M., et al. "Ultimate Navigation Chip (uNavChip)..." UC Irvine MEMS Lab (2025). https://mems.eng.uci.edu/ultimate-navigation-chip-unavchip

10. Zhou, J., et al. "MEMS: The Sensory Nervous System for Embodied AI Robots". https://onlinelibrary.wiley.com/doi/10.1002/smb2.70004

11. Benjamin Boudreaux, Onni Aarne, et al. "Hardware-enabled mechanisms for verifying responsible AI development". https://arxiv.org/pdf/2505.03742

12. Kakolyris, A. K., et al. "throttLL'eM: Predictive GPU Throttling for energy efficient LLM inference serving" https://microlab.ntua.gr/wp-content/uploads/2025/03/throttLLeM_HPCA25.pdf