Public Comment on Proposed Rule: Prohibition on Certain Semiconductor Products and Services

The Box Commons

April 1, 2026

THE BOX COMMONS
Independent AI Agent Credentialing Standards Body
standards@theboxcommons.org · theboxcommons.org

April 1, 2026

FAR Council
DoD, GSA, and NASA
Submitted via regulations.gov

Re: FAR Case 2023-008 (RIN 9000-AO56) — Prohibition on Certain Semiconductor Products and Services

Dear Members of the FAR Council:

The Box Commons respectfully submits this comment in response to the proposed rule on the Prohibition on Certain Semiconductor Products and Services, published at 91 FR 7223 on February 17, 2026, implementing Section 5949 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023.

The Box Commons is a Wyoming mutual benefit nonprofit corporation organized under Section 501(c)(6) of the Internal Revenue Code. We develop independent credentialing standards for artificial intelligence systems, with a focus on verifiable compliance, behavioral safety, and interoperability across regulatory frameworks. Our standards architecture maps to the NIST AI Risk Management Framework.

We write to address a specific gap in the proposed rule: **the absence of independent verification mechanisms for semiconductor provenance in AI systems procured by federal agencies.** AI systems represent among the most semiconductor-intensive products in federal procurement, yet the proposed rule's "reasonable inquiry" standard provides no AI-specific guidance for verifying the provenance of the specialized chips — GPUs, TPUs, AI accelerators, and inference processors — on which these systems depend.

I. The Reasonable Inquiry Standard Is Insufficient for AI Hardware Supply Chains

The proposed rule establishes a "reasonable inquiry" standard under which contractors must seek out information to identify the source of semiconductor products or services in their offerings. The

FAR Council explicitly declined to require detailed provenance tracking, hardware bills of materials, or independent third-party audits, stating that reasonable inquiry "would sufficiently mitigate the risk of noncompliance at this time."

We respectfully disagree, at least as applied to AI systems. The AI hardware supply chain presents unique verification challenges that distinguish it from general electronic products:

Fabrication complexity. A single AI accelerator chip may involve design in one country, fabrication in another, packaging and testing in a third, and integration into a module or server in a fourth. The entities listed as covered — SMIC, CXMT, and YMTC — participate at various tiers of this supply chain, sometimes as direct manufacturers and sometimes as sub-tier foundry providers. Self-certification by a prime contractor or first-tier supplier cannot reliably verify provenance across these tiers.

Rapid model turnover. Federal AI deployments frequently update model architectures and hardware configurations. A system certified as compliant at contract award may incorporate different semiconductor components during performance as hardware is refreshed or upgraded. The proposed 72-hour reporting requirement (compressed from the statutory 60-day window) implicitly acknowledges this dynamism but provides no mechanism for continuous verification.

Concentration risk. The AI accelerator market is dominated by a small number of manufacturers, several of which maintain fabrication relationships with entities in semiconductor foreign countries of concern. A contractor conducting "reasonable inquiry" in good faith may lack visibility into whether a supplier's fabrication partner has subcontracted to a covered entity.

II. Lessons from Section 889 Implementation

The proposed rule's self-certification approach mirrors the framework adopted for Section 889's prohibition on certain telecommunications equipment. The experience under Section 889 is instructive: federal oversight efforts — including FCC investigations and inspector general audits — have documented cases where self-certification failed to prevent covered telecommunications equipment from entering federal and federally funded supply chains. Contractors certified compliance in good faith, but lacked the supply chain visibility to verify their certifications.

The semiconductor supply chain is more complex and less transparent than the telecommunications equipment supply chain that Section 889 addressed. If self-certification proved insufficient for a market dominated by identifiable equipment manufacturers (Huawei, ZTE), it will prove even less reliable for semiconductors embedded at sub-component levels across a global fabrication network.

III. Recommendations

Recommendation 1: Establish a voluntary third-party verification pathway for AI hardware provenance. The FAR Council should recognize independent third-party credentialing as an optional compliance pathway that provides contractors with enhanced safe harbor protections. Contractors who obtain third-party verification of semiconductor provenance for their AI systems would receive a rebuttable presumption of compliance with the reasonable inquiry standard. This creates a market incentive for verification without imposing a mandate.

This approach mirrors established models in federal procurement: FedRAMP provides third-party assessment for cloud security; CMMC provides tiered certification for cybersecurity maturity. Neither

was mandated in initial rulemaking — both evolved from voluntary frameworks to required standards as the threat landscape matured.

Recommendation 2: Define "reasonable inquiry" standards specific to AI hardware. The proposed rule's reasonable inquiry standard is technology-neutral. For most electronic products, this is appropriate. For AI systems — where the semiconductor components are purpose-built, high-value, and concentrated among a small number of suppliers — the FAR Council should issue supplementary guidance defining what constitutes reasonable inquiry for AI accelerators, GPUs, TPUs, and inference processors specifically. This guidance should address multi-tier fabrication visibility, not merely first-tier supplier certification.

Recommendation 3: Align Section 5949 compliance with Section 5949(g) supply chain risk mitigation. The FAR Council has deferred rulemaking on Section 5949(g), which addresses supply chain risk mitigation for non-prohibited semiconductors. We urge the Council to consider these provisions jointly rather than sequentially. A credentialing framework that addresses both prohibited entity verification (Section 5949(a)-(b)) and broader supply chain risk mitigation (Section 5949(g)) would provide contractors with a unified compliance pathway rather than layering successive requirements.

Recommendation 4: Address AI-specific critical systems. The proposed rule defines "critical system" by reference to national security systems under 40 U.S.C. 11103(a)(1) and Federal Acquisition Security Council designations. As federal agencies increasingly deploy AI systems in decision-making roles — including in defense, intelligence, and homeland security contexts — the FAR Council should clarify whether AI systems used for automated analysis, threat detection, or operational planning qualify as critical systems under the Part B prohibition, regardless of whether the broader IT environment in which they operate is classified as a national security system.

IV. Conclusion

The proposed rule represents a necessary step in securing the federal semiconductor supply chain. We support its objectives. Our concern is that the reasonable inquiry standard, while appropriate for general electronics procurement, is insufficient for the specialized and opaque AI hardware supply chain.

Independent third-party verification — provided by credentialing bodies with technical expertise in AI hardware provenance — offers a scalable, market-driven complement to self-certification. The Box Commons is developing standards for exactly this purpose, mapped to the NIST AI Risk Management Framework, and we respectfully urge the FAR Council to create the regulatory space for such verification mechanisms.

Respectfully submitted,

Brice Love
Acting Executive Director
The Box Commons
standards@theboxcommons.org