RISK COVERAGE HUB · COMMERCIAL RISK & POLICY DESK · RENEWAL BRIEF (NOV 14, 2026)

Certified Compute as Risk Transfer: Underwriting & Renewal Brief

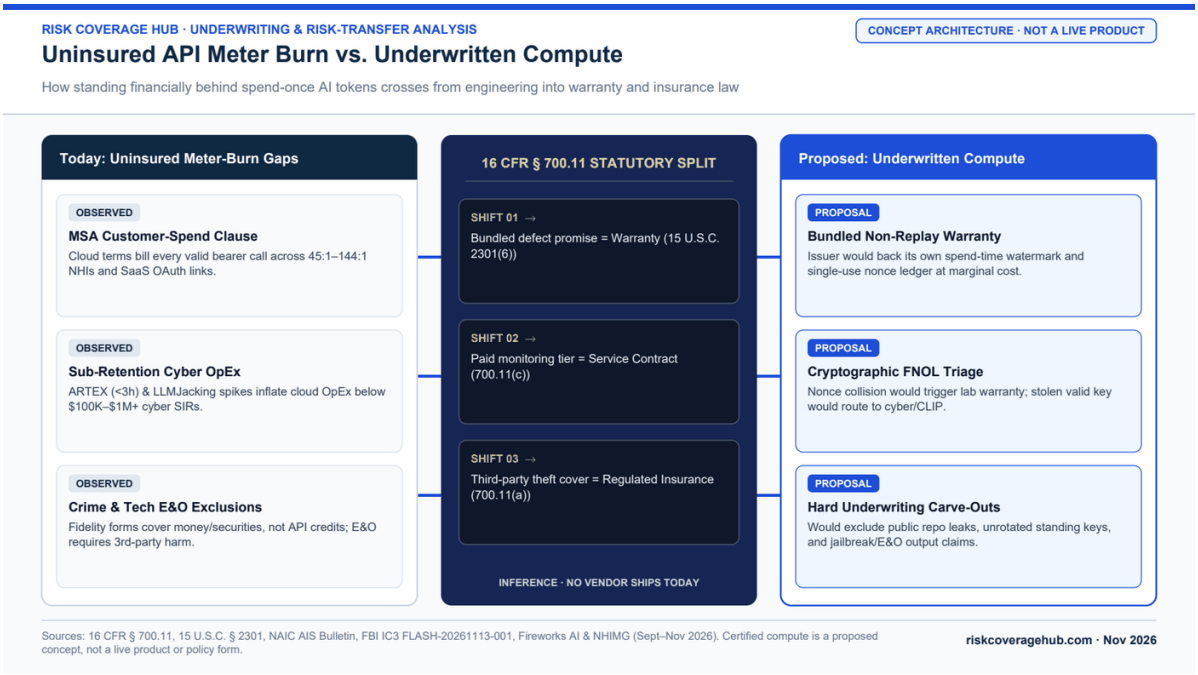
Concept Status: Certified compute (watermarked at spend-time, spendable once, issuer-backed) does NOT exist as a commercial product, protocol, or policy form today. Facts reflect Sept 15–Nov 14, 2026 primary receipts; risk-transfer mechanics reflect statutory and underwriting analysis.

1. Bearer API Compute Today vs. Proposed Certified Compute Instrument

Risk Dimension	Observed Today (Sept–Nov 2026 Receipts)	Certified Compute Proposal (Underwriting Inference)
Credential & NHI Surface	NHIs outnumber humans 45:1–144:1; ~30% (71/239) of AI breaches via SaaS/OAuth; 44% credential-led	Named issuer tokens bound to spend-time watermarks and single-use cryptographic nonces
Active Loss Vector	ARTEX (under-3h intrusions, FBI FLASH-20261113-001) & Fireworks AI LLMJacking (Oct 6 & 23–24)	Replay attempts fail at endpoint; stolen-key versus ledger-defect claims split via spend receipts
Accounting & Policy Gap	Stolen meter burn hides in cloud OpEx below cyber SIRs and outside crime money/securities clauses	Explicit split between maker defect credit (warranty) and insured third-party theft sublimit (CLIP/cyber)
Statutory Classification	Cloud MSAs shift 100% of valid-key usage risk onto customer under shared-responsibility terms	16 CFR § 700.11 trilemma: bundled defect warranty vs. paid service contract vs. regulated insurance
Semantic Output Boundary	NIST Gödel proof & TEE limits (arXiv:2603.05786) show guardrails/enclaves cannot block all injections	Strict exclusion for jailbreaks and hallucinated outputs; downstream harm stays in Tech E&O

2. Core Underwriting Takeaways

- **Standing Behind Tokens Is Underwriting:** Under NIST SP 800-39, watermarks mitigate risk, but absorbing counterfeit or replay loss transfers financial risk—requiring actuarial pricing, reserves, and exclusions.
- **The 16 CFR § 700.11 Boundary:** A lab can bundle a free warranty against its own nonce/ledger defects (15 U.S.C. § 2301(6)), but charging a fee to cover fortuitous third-party key theft crosses into state-regulated insurance (16 CFR § 700.11(a)).
- **NAIC & FIO Oversight:** Insurers using certifier telemetry face third-party AI vendor governance rules under the NAIC AI Model Bulletin, while correlated single-lab liability raises FIO systemic aggregation concerns.
- **Cryptographic Claims Triage:** NIST nonces and signer non-repudiation allow adjusters to separate issuer double-spend bugs from compromised customer LiteLLM proxies or OAuth SaaS connectors.



RISK COVERAGE HUB · COMMERCIAL RISK & POLICY DESK · RENEWAL BRIEF (NOV 14, 2026) · PAGE 2 REFERENCE & CHECKLIST

Page 2 Renewal & Risk-Management Action Checklist

Six controls for risk managers, CFOs, and brokers to execute today while AI compute remains uncertified

Renewal Check / Control	Owner	Immediate Action Before Next Policy Binding
[ ] Document NHI Ratio Schedule	CISO / IAM Lead	Prepare machine-to-human ratio schedules (vs. 45:1–144:1 benchmark) for supplemental AI renewal forms
[ ] Qualify for Preferred Broker Tier	Platform Eng	Retire standing LiteLLM/One API root secrets; attest ~30s ZSP sandboxed token brokering to underwriters
[ ] Cap Velocity Below Cyber SIR	FinOps / SecOps	Enforce automated dollar-velocity circuit breakers so sub-3h ARTEX-style drain stops well below $100K+ SIRs
[ ] Audit Cyber Utility-Fraud Wording	Insurance Broker	Verify whether cryptojacking / utility-fraud sublimits explicitly cover stolen API inference meter burn
[ ] Map Vendor Subrogation Caps	Legal / Procurement	Review SaaS OAuth and API gateway MSAs for 12-month fee liability caps blocking subrogation recovery
[ ] Separate Custody vs. E&O Towers	Risk Manager	Address first-party meter burn in cyber/crime reviews and semantic AI output liability in Tech E&O

3. Concept Boundaries & Primary Authorities

- **Concept Boundary:** Certified compute does not exist today as a commercial offering, protocol, or insurance policy. All warranty, CLIP, and claims workflows above represent analytical risk-transfer modeling.
- **Verified Sept–Nov 2026 Loss Receipts:** FBI IC3 FLASH-20261113-001 & Amazon MadPot (ARTEX Oct 3–Nov 5 sub-3h key-theft campaigns); Fireworks AI Oct 6 & Oct 23–24 LLMJacking (<1% Notion chats); NHIMG/CSA (~30% [71/239] SaaS/OAuth & 44% credential-led breaches, 45:1–144:1 NHIs); Lazarus (<10 neurons, 84.1%–98.8%).
- **Primary Insurance & Statutory Authorities:** 15 U.S.C. § 2301, 16 CFR § 700.11, NIST SP 800-39, NAIC Model Bulletin on AIS, U.S. Treasury FIO, and NIST CSRC Nonce / Non-Repudiation definitions.

Primary Receipts & Verified Authorities

- FTC Magnuson-Moss Interpretations: Written Warranty, Service Contract, and Insurance Distinguished (16 CFR § 700.11)
- Magnuson-Moss Warranty Act Statutory Definitions (15 U.S.C. § 2301)
- NAIC Model Bulletin: Use of Artificial Intelligence Systems by Insurers
- U.S. Department of the Treasury — Federal Insurance Office (FIO)
- NIST SP 800-39: Managing Information Security Risk (Risk Mitigation vs. Risk Transfer)

Canonical Web Edition: https://riskcoveragehub.com/certified-compute-underwriting-risk-transfer/ | **AI Markdown Twin:** https://riskcoveragehub.com/certified-compute-underwriting-risk-transfer.md

Informational commercial-risk analysis only; not insurance brokerage or legal advice. Certified compute is a proposed concept, not an available insurance or technology product.