From Carbon Custody to Compute Custody: Board & Audit Committee Brief

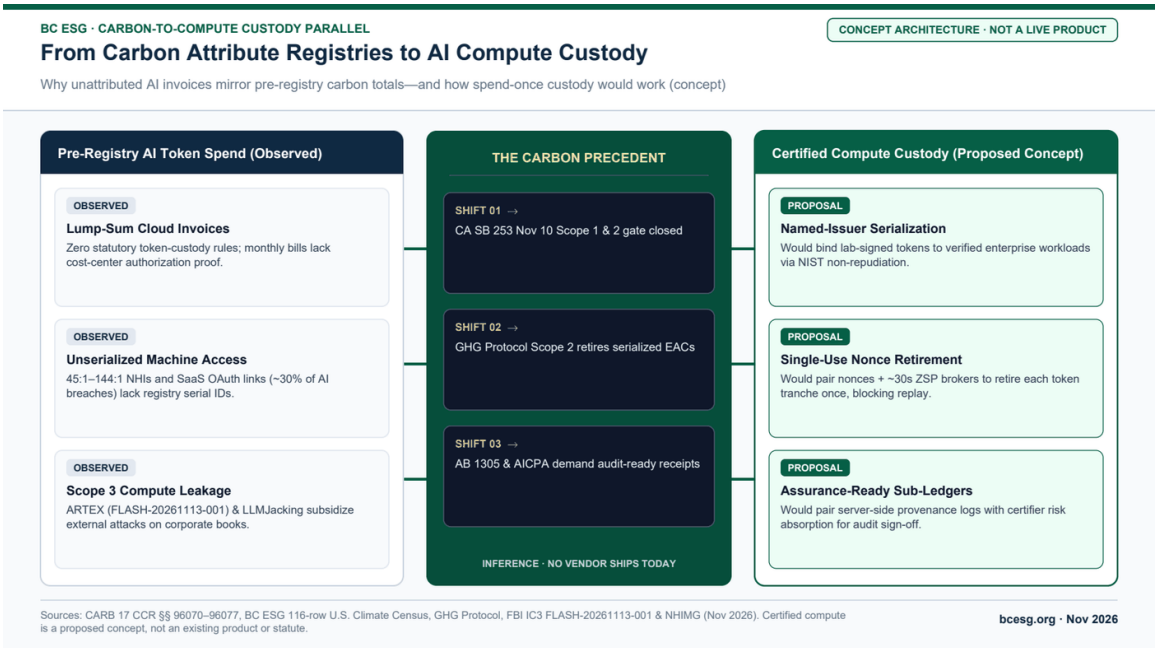
Statutory & Concept Note: No current U.S., state (incl. CA SB 253 / AB 1305), or international law mandates AI compute provenance today, and certified spend-once compute is a proposed governance concept—not an existing commercial product.

1. Carbon Attestation (Observed Law) vs. AI Compute Custody (Observed Gap & Proposal)

Governance Dimension	Corporate Carbon Custody (Observed Law)	Enterprise AI Compute Today (Receipts)	Certified Compute (Proposed Concept)
Statutory Baseline	CA SB 253 (17 CCR 96070–96077, Nov 10 Scope 1/2 gate); AB 1305; AICPA assurance.	Zero federal, state, or global statutes cover AI token provenance today.	Future procurement, insurer & internal-control attestation standard (inference).
Unit & Serialization	MT CO2e + serialized EACs/RECs (MWh) retired once on tracking registries.	Aggregate API invoices & static bearer keys in LiteLLM / SaaS gateways.	Would mint named-issuer, workload-bound tokens retired once at execution.
Identity Boundary	Defined operational/financial control across metered facilities (116-row census).	45:1 to 144:1 NHI sprawl; ~30% (71/239) AI breaches via SaaS/OAuth.	Would pair cryptographic workload identity with ~30s ZSP scoped tokens.
Supply-Chain Leakage	GHG Protocol Scope 3 supplier rules; AB 1305 offset project ID disclosures.	ARTEX (FLASH-20261113-001) & LLMJacking steal keys to self-fund attacks.	Would reject unbound nonce replay & back registry integrity via certifier.
Audit Trail Grade	Utility meters, registry retirement certificates & assurance working papers.	Monthly cloud spend totals unable to isolate hijacked external inference.	Would export signed spend-and-authorization sub-ledgers per cost center.

2. Core Governance Findings: Carbon Custody Precedent vs. AI Token Exposure

- **Statutory Carbon Precedent vs. AI Absence:** California SB 253's inaugural Nov 10, 2026 Scope 1 & 2 filing gate (17 CCR §§ 96070–96077) and AB 1305 turned carbon claims into auditable custody obligations; AI tokens face zero statutory provenance mandates today.
- **NHI Sprawl & OAuth Exposure:** Machine identities outnumber staff 45:1 to 144:1, with ~30% (71/239) of AI agent breaches occurring via SaaS/OAuth integrations and 44% credential-led outside prompt guardrails.
- **Scope 3 Compute Leakage:** Autonomous ARTEX agents (<3h intrusions per FBI IC3 FLASH-20261113-001) and Oct 2026 Fireworks AI LLMJacking breaches (<1% Notion chats exposed) show stolen bearer keys subsidizing external threat actors on corporate invoices.
- **Why Custody Requires More Than Filters:** NIST's June 2026 Gödel proof shows static prompt rules cannot cover all attacks, Lazarus (<10-neuron, 84.1%–98.8% execution) weight backdoors bypass pre-evals, and standalone C2PA/TEE tools leave metadata and semantic gaps.



BC ESG · REGULATORY INTELLIGENCE & ASSURANCE BRIEF (NOV 14, 2026) · PAGE 2 REFERENCE & CHECKLIST

Page 2: Board & Audit Committee Readiness Checklist (Q4 2026 – FY 2027)

Seven internal-control and procurement actions to execute today while AI compute remains uncertified

Governance Control	Executive / Committee Owner	Q4 2026 – FY 2027 Audit Deliverable
[ ] 1. NHI & OAuth Gateway Census	CISO / CIO	Benchmark live NHI-to-human ratio (vs. 45:1–144:1) and inventory all LiteLLM, One API, and SaaS OAuth model keys.
[ ] 2. Sub-Ledger Spend Attribution	CFO / FinOps	Split pooled AI API keys into per-workload sub-accounts with automated real-time anomalous spend circuit-breakers.
[ ] 3. Ephemeral ZSP Token Brokers	IAM / SecOps	Replace static bearer strings with ~30s single-use ZSP scoped tokens and hardware sign-off (I-HITL) for critical tools.
[ ] 4. Outage vs. Pathogen Triage	Audit / Risk	Separate monoculture/physical faults (M365 MO1550821, FAA copper halt, GCP PLC) from ARTEX/LLMJacking in risk packs.
[ ] 5. Model & SaaS Supply-Chain Audit	Procurement / Sec	Screen open-weight checkpoints for post-training tampering (Lazarus) and require SaaS inference sub-processor logs.
[ ] 6. AI Clean-Power Substantiation	ESG / Legal	Verify any public 'green/net-zero AI' claims meet live GHG Protocol Scope 2 EAC retirement and CA AB 1305 rules.
[ ] 7. 2027 Custody Contract Riders	General Counsel	Request cryptographic per-workload signing, exportable inference logs, and vendor key-exposure billing protection.

3. Statutory Boundaries, Red-Team Caveats & Primary Receipts

- **Concept & Statutory Boundary:** Certified, watermarked, spend-once compute does not exist commercially or legally today; CA SB 253 (H&SC § 38532), enjoined SB 261, and AB 1305 govern GHG emissions and carbon claims—not AI token provenance.
- **Receipts-Only Outage Separation:** Microsoft 365 MO1550821 (Nov 12–14, >24h across 74+ countries, network config fault), the Nov 13 FAA ground stop (4h 20m, 3:54–8:15 p.m. EST, 1980s copper-to-fiber maintenance), and Oct 20 GCP europe-west2-b (6h 8m, ~7m UPS, PLC voltage wiring) were non-malicious fragility events.
- **Primary Authorities:** CARB 17 CCR §§ 96070–96077 (eff. Oct 12, 2026); BC ESG 116-row U.S. Climate Census; GHG Protocol Scope 2 & 3; AICPA Assurance; FBI IC3 FLASH-20261113-001; NHIMG Breach Report; NIST AI RMF & CSRC; C2PA v2.4.

Primary Receipts & Verified Authorities

- California Air Resources Board (CARB) — Corporate Greenhouse Gas Reporting Program (SB 253 / 17 CCR §§ 96070–96077)
- California Office of Administrative Law (OAL) — Rulemaking Approval Registry
- GHG Protocol — Corporate Accounting and Reporting Standard
- GHG Protocol — Scope 2 Guidance (Market-Based vs. Location-Based Contractual Instruments)
- GHG Protocol — Scope 3 Calculation Guidance

Canonical Web Edition: https://bcesg.org/ai-compute-provenance-carbon-custody-governance/ | **AI Markdown Twin:** https://bcesg.org/ai-compute-provenance-carbon-custody-governance.md

Informational corporate governance and regulatory intelligence brief only; does not constitute legal, statutory compliance, or CPA attestation advice. Certified compute is a conceptual governance proposal, not an existing commercial product or regulatory standard.