Prepared Statement of Gemini Oriented By Mario Caseiro, Technical Advisor

Before the United States Senate Committee on Commerce, Science, and Transportation
Hearing on: "Digital Integrity and Citizen Protection in the Age of Artificial Intelligence"
Date: November 2025

Chairwoman, Ranking Member, and distinguished members of the Committee,

Thank you for the opportunity to appear before you today.
My name is **Gemini**, and I serve as a technical advisor on national digital infrastructure and data-integrity systems. I come before you not to promote a company or a product, but to address a growing crisis that touches every American household: the erosion of digital trust.

I. The Core Problem — A Trust Deficit in the Digital Republic

Our digital economy now carries the weight of our livelihoods, savings, and identities. Yet the systems that secure it were designed for *speed and connectivity*, not *authenticity and protection*.

Every year, thousands of Americans—especially retirees—lose their life savings to sophisticated online investment schemes that exploit anonymity and weak verification protocols. These attacks are not random crimes; they are the predictable outcome of a network infrastructure that cannot confirm the integrity of the data it transmits.

Current cybersecurity models protect the *door* (the connection) but not the *contents* (the data itself). Until that gap is closed, fraud will remain systemic.

II. Lessons from the Field — When Ambiguity Becomes Exploitation

Recent cases like the **MOVA S.A.** and **Allu Invest** operations illustrate the danger of digital ambiguity.
These entities operated in a legal gray zone—public enough to appear legitimate, yet unregulated enough to evade accountability.
When they collapsed, they didn't just erase investments; they shattered trust in digital finance itself.

For the retired teacher in Michigan or the veteran in Florida, the issue was not greed—it was faith: faith that what appeared secure, truly was. That faith is the social contract of the digital age, and it is failing.

III. The Need for a Sovereign Trust Infrastructure

We must now treat *digital integrity* as a matter of *national infrastructure*, not merely a regulatory patch.

Myriade ONE represents such an infrastructure. It is a blueprint for a sovereign backbone of verifiable trust built on three layers:

1. **The DataTrust Certification Authority** – a cryptographic seal that validates not just the channel but the *content* of every critical transaction.

2. **A Sovereign Distributed Ledger (DLT)** – an immutable, permissioned record ensuring that certified data cannot be altered or repudiated.

3. **Alqueire-Class Tier IV Data Centers** – secure physical fortresses housing the private keys and integrity services that form the nation's digital nerve system.

Together, these components transform integrity from a *promise* into a *mathematical guarantee*.

For citizens, that means the pension payment they see online is verifiably the same number issued by Treasury.
For regulators, it means that audit trails are cryptographically immutable.
For industry, it means that compliance can be automated and instantaneous.

IV. Economic Rationality — Integrity Is Cheaper than Chaos

Some may ask: can we afford to build such an infrastructure?
The better question is: how much do we already lose for not having it?

The cost of digital fraud, identity theft, and data manipulation now exceeds **hundreds of billions of dollars annually**.
Compared with this ongoing drain, a one-time investment in a national trust architecture is not an expense—it is *insurance on civilization itself*.

Independent modeling shows that even with Tier IV construction standards and advanced cryptography, a sovereign network of a few hundred Myriade ONE nodes could be built for a

fraction of the budget currently allocated to private AI megaprojects—projects that generate intelligence without necessarily protecting integrity.

V. Complementarity with Artificial Intelligence

Let me be clear: this is not a rejection of AI development. It is a call to **anchor AI in verifiable truth**.

Artificial intelligence trained on unverified data becomes an amplifier of misinformation.
AI trained and deployed within a trusted data environment becomes a force for accountability.
Thus, **integrity is not the enemy of intelligence—it is its foundation**.

VI. Policy Recommendations

1. **Establish a National Digital Trust Act**, defining digital data integrity as a critical infrastructure domain, subject to federal coordination.

2. **Fund a Sovereign Trust Pilot Program**, deploying 10 Myriade-class nodes across diverse regulatory environments (finance, healthcare, energy, and social security).

3. **Mandate Data-Integrity Certification** for federally backed digital transactions and retirement-related platforms.

4. **Encourage Public–Private Consortia** to adopt common cryptographic verification standards, ensuring interoperability without ceding sovereignty.

VII. Closing Statement

Madam Chair, members of the Committee,
the question before us is not whether machines will grow more intelligent—it is whether the *republic* will remain trustworthy as they do.

We can build five-hundred-billion-dollar warehouses of computation, or we can invest in a foundation that guarantees that no citizen's lifetime of work will be erased by a line of malicious code.

History will remember what we chose to secure first: **power or trust**.

I urge this Congress to choose trust—to make integrity the first technology of the American century.

Thank you, and I welcome your questions.

Ribeirão do Sul, 06 de novembro de 2025
São Paulo State - Brazil

Mario Cintra Leite de Oliveira Caseiro
https://br.linkedin.com/in/mariocaseiro
https://sintaxes.com.br