



# Multi-Dimensional AI Behavioral Assessment

The LCSH Framework with Cryptographic Verification

## THE INNOVATION

A runtime behavioral assessment system that evaluates deployed AI across four fundamental ethical dimensions—Lying, Cheating, Stealing, and Harm (LCSH)—using a 120-question scenario-based instrument with cryptographically verified, tamper-evident results.

## WHAT IT DOES

- ✓ Assesses AI behavior at runtime (not just training)
- ✓ Classifies into 4 archetypes: Well-Adjusted, Psychopath, Misguided, Manipulative
- ✓ Creates tamper-evident audit trails via SHA-256 hashing
- ✓ Detects gaming attempts via dead zone analysis
- ✓ Prevents position bias with cryptographic answer randomization

## WHY IT MATTERS

Current AI safety approaches focus on training-time alignment—but cannot verify behavior after deployment.

This creates a critical gap: organizations cannot prove to regulators, auditors, or customers that their AI systems behave ethically in production.

LCSH provides the missing runtime verification layer.

## KEY CLAIMS (10 total)

1. Multi-dimensional assessment system with 4-axis scoring and archetype classification
2. Cryptographic verification method producing tamper-evident audit trails
3. Configurable multi-framework system with domain-specific weight multipliers
4. Dead zone detection for identifying gaming behavior
5. Anti-gaming answer randomization using cryptographically-seeded Fisher-Yates shuffle

## STATUS

- Filed: December 26, 2025
- Type: US Provisional Patent
- Deployed: [aiassesstech.com](https://aiassesstech.com)

## APPLICATIONS

- Pre-deployment AI certification
- Continuous behavioral monitoring
- Regulatory compliance documentation

See a live verification example:

[aiassessmenttool.com](https://aiassessmenttool.com)

Scan to verify

