TELOS Regulatory Alignment Map

Evidence Relevance, Capability Gaps, and Current Legal Status

TELOS AI Labs Inc.

August 11, 2026

Standing caveat

This map identifies obligations for which TELOS records and measurements may be relevant. It is a self-assessment by TELOS Labs, not an independent certification or legal opinion. A technical artifact can support a compliance process without satisfying the governing obligation. Legal sufficiency depends on the regulated role, system classification, jurisdiction, deployment facts, record completeness, retention, and review by qualified counsel, auditors, and regulators.

The map is current as of August 11, 2026. Laws, implementation dates, guidance, and enforcement positions can change. Each website publication should show the review date and assign an owner for updates.

Capability-to-evidence map

TELOS capability	Potential evidence contribution	Current limitation
Versioned Manifest	Declared purpose, scope, tools, sequences, boundaries, and approval requirements	Manifest identity and approval root are not bound into the opened receipt schema
Per-action measurement	A contemporaneous comparison between submitted work and a fixed external reference	Production engine and calibration are not publicly reconstructable
Drift and stability telemetry	Post-deployment monitoring and trend evidence	Coverage depends on every relevant action reaching the adapter
Graduated surfacing	Evidence that uncertainty or departure was identified for human attention	The receipt alone does not prove that a human received or resolved it
Signed per-result receipt	Detectable alteration of covered measurement and decision fields	Key identity, authorization, ordering, and trusted time require additional evidence
Public hash-linked projections	Payload and published order integrity	No public signature or authorship proof
Retention setting	Declared intended retention period	Automatic expiry is not implemented in the opened source
Documentation-to-Manifest compiler	Intended traceability from organizational documents to the runtime specification	COMING, not shipped
Signed Manifest and session chain	Intended end-to-end authority and ordering evidence	COMING in the opened implementation

European Union AI Act

Primary source: Regulation (EU) 2024/1689.

Article 72: post-market monitoring

Providers of high-risk AI systems must establish and document post-market monitoring that actively and systematically collects, documents, and analyzes relevant performance data over the system's lifetime. TELOS per-action scores, drift indicators, stability measures, and event logs are potentially relevant evidence because they observe behavior after deployment.

The contribution is conditional. The deployment must establish coverage, metric validity, record completeness, issue handling, retention, and a documented process that evaluates continued compliance. TELOS alone does not establish Article 72 satisfaction.

Articles 11 and 12: documentation and record keeping

The Manifest, configuration record, signed receipts, and telemetry can contribute to technical documentation and logging. The planned documentation-to-Manifest compiler is intended to create traceability from existing policies and procedures, but that compiler is COMING. The opened receipt does not bind Manifest version, approval root, or predecessor, and automatic retention enforcement is not implemented.

Article 14: human oversight

Graduated surfacing can route a departure to a named human through the escalate path. The clarify state is an agent-path resolution step and is not by itself evidence of human visibility. Evidence of actual oversight also requires an adapter event record, recipient, response, timing, and resolution. A score or receipt alone does not prove meaningful human oversight.

Article 15: accuracy, robustness, and cybersecurity

The adversarial and drift studies can contribute to an evidence package. The current results are primarily self-scored development evidence without a held-out split. They are not an independent demonstration that a deployed high-risk system meets Article 15.

Article 19: automatically generated logs

Article 19 sets retention requirements for certain automatically generated logs under a high-risk provider's control. TELOS exposes a retention setting, but the opened implementation does not automatically delete aged records. Deployers must implement the applicable retention period, legal holds, access controls, and deletion behavior outside or around the current component.

Article 50: transparency

Article 50 includes transparency duties for specified AI interactions and generated or manipulated content. TELOS can preserve an account of what a governed agent submitted and how it was scored. It does not itself provide every required notice, disclosure, or machine-readable marking.

Articles 6, Annex III, and 99

Classification and penalties depend on the system and regulated role. Annex III includes specified uses such as biometrics, critical infrastructure, education, employment, essential services, law enforcement, migration and border control, and administration of justice and democratic processes. A TELOS component embedded in a regulated system should be assessed within the actual system boundary. The governance layer should not be assumed to sit outside the regulated system.

EU Digital Omnibus proposal

The European Commission proposed changes to implementation timing in November 2025. The Council announced its negotiating position on March 13, 2026. The legislative process remained ongoing as of this review date. This is a timing and legislative-status issue, not a basis to reduce the substantive design controls in the AI Act.

Primary source: Council position, March 13, 2026.

California SB 53

Primary source: California SB 53 bill record.
California's Transparency in Frontier Artificial Intelligence Act took effect January 1, 2026. It applies to covered frontier developers meeting statutory conditions and includes safety-framework, transparency-report, incident-reporting, and whistleblower provisions.
TELOS is primarily positioned for deployers, so the mapping is directional. Runtime evidence may help a covered organization demonstrate that declared limitations were monitored and that adversarial behavior was evaluated. Whether TELOS is inside a covered developer's safety framework, and what evidence must be published or reported, requires analysis of the actual entity, model, role, and incident.
California SB 243
Primary source: California SB 243 bill record.
The internal SB 243 benchmark set is a research artifact, not evidence that a deployment satisfies California law. A benchmark result can contribute to product testing, but statutory duties concerning disclosures, protocols, reporting, or user protections must be implemented and evidenced directly.
Colorado SB 26-189
Primary source: Colorado SB 26-189, enacted May 14, 2026.
Colorado SB 26-189 repealed and reenacted SB 24-205 with new requirements for automated decision-making technology used to materially influence consequential decisions. Principal requirements begin January 1, 2027.
The enacted summary identifies, among other things:

- technical documentation from covered developers describing intended uses, training-data categories, known limitations, appropriate use, and human review;
- notice obligations for covered deployers;
- plain-language descriptions following specified adverse outcomes;
- consumer rights concerning data, correction, meaningful human review, and reconsideration;
- at least three years of compliance records for developers and deployers.

TELOS records may support documentation of intended purpose, measured departures, configuration, and human review. They do not provide consumer notices, perform reconsideration, correct personal data, or automatically enforce the three-year record period. The open receipt also lacks Manifest identity and human-resolution fields, so a deployer would need a broader evidence system.
FDA Quality Management System Regulation
Primary sources: FDA QMSR overview and 21 CFR Part 820.
The Quality Management System Regulation became effective February 2, 2026. It amended 21 CFR Part 820 and incorporates ISO 13485:2016 by reference.
For a regulated finished-device manufacturer, TELOS telemetry may contribute to evidence concerning validation and monitoring of production or service processes, nonconformity handling, corrective action, and records. Applicability depends on the device, the use of AI within the quality system or product lifecycle, and the manufacturer's validated procedures.
The phrase continuous per-action measurement does not establish process validation. A QMS record must also establish approved procedures, validation acceptance criteria, change control, review, investigation, corrective action, and record control. This paper does not assert a universal FDA record-retention period because retention depends on the applicable record type and governing requirements.
ISO 9001:2015 and ISO 13485:2016
Primary sources: ISO 9001 and ISO 13485.
TELOS uses the Plan-Do-Check-Act and statistical process-control analogy:

Quality phase	TELOS mapping
Plan	Approve a Manifest and measurement configuration
Do	Run the agent through an integrated observation path
Check	Measure per-action fidelity, drift, stability, and departures
Act	Surface, investigate, resolve, recalibrate, or change the specification under control

Potentially relevant areas include monitoring and measurement, the ability of processes to achieve planned results, nonconformity, and corrective action. Conformity to either standard requires an audited management system and cannot be inferred from installing a measurement component.
NAIC Model Bulletin on AI used by insurers
Primary source: NAIC model bulletin announcement and materials.
The bulletin expects an insurer's AI program to address governance, risk management, documentation, and accountability. TELOS can contribute declared purpose, continuous measurement, event records, and named human handling. It does not create the insurer's complete written program, validate input data, establish nondiscrimination, or satisfy state-specific adoption and examination expectations.
The architecture may also be relevant to insurers underwriting third-party agent deployments because receipts and monitoring can improve observability. That commercial relevance is not an insurance certification or an actuarial claim.
NIST AI Risk Management Framework
Primary sources: NIST AI RMF 1.0 and NIST AI 600-1 Generative AI Profile.

Function	Potential TELOS contribution	Gap
GOVERN	Manifest, named authority, approved thresholds, oversight process	Approval identity is not bound into the current receipt
MAP	Declared use, scope, tools, boundaries, and risk context	Coverage and impact analysis remain organizational duties
MEASURE	Per-action scores, trends, benchmark evidence, false positive measurement	Independent validation and held-out performance remain open
MANAGE	Graduated surfacing, issue records, recalibration decisions	The current default is observe/open and does not itself remediate

This is a voluntary-framework relevance map, not a NIST endorsement.
NIST NCCoE agent identity and authorization project
Primary source: NCCoE Software and AI Agent Identity and Authorization.

NCCoE capability area	TELOS relevance	Evidence boundary

Agent identification	A receipt can be verified against a deployment public key	Independent evidence must bind that key to an issuer and agent
Authorization	Manifest fields and measurement can support authorization review	Manifest identity and approval are external to the current receipt
Auditing	Signed receipts and telemetry are potential audit artifacts	Completeness, ordering, retention, and handling need deployment controls
Non-repudiation objective	A valid signature can bind covered bytes to a key	Chain-level signing, trusted time, and identity binding are not public-prototype properties

OWASP Top 10 for Agentic Applications

Primary source: OWASP agentic security release.

TELOS measurement, boundaries, tool declarations, receipts, and escalation may be relevant to multiple agentic-risk categories. The defensible claim is observability and evidence contribution, not full mitigation of all ten risks. Threats involving identity, excessive permissions, tool abuse, memory, supply chain, insecure output handling, and compromised orchestration require controls outside semantic fidelity measurement.

TELOS data protection posture

Intelligence-layer collection is off by default. When enabled, the opened telemetry record stores governance metrics and identifiers without raw request text or content embeddings. Even without raw text, identifiers and behavioral metrics can be personal data or confidential operational information.

The deployment must address:

- lawful basis and purpose limitation;
- data minimization;
- access, correction, deletion, and retention requests where applicable;
- encryption and key management;
- cleartext session headers and aggregate files;
- plaintext fallback if encryption setup fails;
- cross-border transfer and processor terms;
- security incident response;
- manual clearing behavior.

TELOS does not resolve these obligations automatically.

Publication control

Every public regulatory claim should carry one of these labels:

Label	Meaning
DIRECT	The artifact directly implements or records the identified technical function
SUPPORTING	The artifact can contribute evidence to a broader obligation
COMING	The capability is planned but not shipped
EXTERNAL	The obligation must be implemented by the deployer or another control
NOT ASSESSED	Applicability or sufficiency has not been evaluated

No mapping in this document should use the words compliant, certified, guaranteed, or meets the law without an identified external determination and its scope.

Related documents

- Core whitepaper
- Technical method
- Validation report
- Record of Trust protocol